GALATASARAY UNIVERSITY
INSTITUTE OF SOCIAL SCIENCES
DEPARTMENT OF INTERNATIONAL RELATIONS

CYBER TOOLS AS FOREIGN POLICY INSTRUMENTS IN TRILATERAL RELATIONS: ANALYSING CYBER-ATTACKS TARGETING THE UNITED KINGDOM

Ph.D. THESIS

Atakan YILMAZ

Thesis Advisor: Assoc. Prof. Menent SAVAŞ CAZALA

JULY 2024

GALATASARAY UNIVERSITY
INSTITUTE OF SOCIAL SCIENCES
DEPARTMENT OF INTERNATIONAL RELATIONS

CYBER TOOLS AS FOREIGN POLICY INSTRUMENTS IN TRILATERAL RELATIONS: ANALYSING CYBER-ATTACKS TARGETING THE UNITED KINGDOM

Ph.D. THESIS

Atakan YILMAZ

Thesis Advisor: Assoc. Prof. Menent SAVAŞ CAZALA

JULY 2024

ACKNOWLEDGEMENTS

The cover page of this dissertation lists only one name as the author; however, this study would not have been possible without the contribution of many valuable names. First and foremost, I would like to express my sincerest gratitude to my thesis advisor, Assoc. Prof. Menent SAVAŞ CAZALA, who provided guidance and support not only during the thesis but throughout my entire doctoral education. Without her guidance, this thesis could never have been completed. I also extend my deep gratitude to Prof. Ebru CANAN-SOKULLU, who has always been a mentor to me, not only as a member of thesis jury but also in my academic and professional life. Her continuous support has played a crucial role in becoming a better person in every aspect of my life. I am also grateful for the insightful contributions Assoc. Prof. Ali Faik DEMİR. With his profound knowledge, he enlightened me on many topics throughout my doctoral education and offered valuable suggestions that significantly enhanced the quality of this thesis. Also, I am indebted to the faculty members of the Department of International Relations at Galatasaray University for their invaluable contributions to my academic development.

Conducting fieldwork in the United Kingdom was crucial for this thesis. I am deeply thankful to The Scientific and Technological Research Council of Turkey (TÜBİTAK) for providing me with a scholarship under the 2214-A – International Research Fellowship Programme for PhD Students. This scholarship enabled me to conduct essential fieldwork in the United Kingdom between August 2023 and February 2024, which significantly contributed to the advancement of this thesis. I would also like to thank Prof. Christian KAUNERT, who was my advisor during my fieldwork in the United Kingdom. He not only directed and guided my research but also facilitated access to important resources by introducing me to esteemed experts and academics. All these experts and academics have made significant contributions to this study, and I am thankful to all of them. However, among them, Dr. Ethem İLBİZ, in particular, played a crucial role. He provided both theoretical and methodological assistance in developing the models that form the backbone of this study. Therefore, his contribution to the advancement of this thesis was invaluable.

I finally express my special thanks to my family: my mother, Aygün YILMAZ; my father, Kerim YILMAZ; and my sisters, Sibel Emel YILMAZ and Saadet Pelin YILMAZ, who have provided me with all kinds of support throughout my education and have always stood by my side with their unwavering support. Their presence, love and support have made this challenging journey more bearable. And, of course, I am profoundly grateful to my wife, Gizem SOLMAZ YILMAZ, who patiently supported me at every stage of my doctoral journey, stood by me through many difficult moments, constantly motivated me, and never withheld her love and support.

TABLE OF CONTENT

ABBREVIATIONS

AI	: Artificial Intelligence
AIIB	: Asian Infrastructure Investment Bank
ARPANET	: Advanced Research Projects Agency Network
AUC	: Area Under Curve
BN(O)	: British Nationals (Overseas) Status
BP	: British Petroleum Company
BTC	: Baku-Tbilisi-Ceyhan Pipeline
CAMEO	: Conflict and Mediation Incident Observations
CENTO	: Central Treaty Organization
CER	: Centre for European Reform
CHW	: Countering Hybrid Warfare
CIA	: Central Intelligence Agency
CIA Triad	: Confidentiality, Integrity and Availability
CPT	: Cyber Persistence Theory
DDoS	: Distributed Denial of Service
DARPA	: US Defense Advanced Research Projects Agency
DOD	: US Department of Defence
ENISA	: The European Union Agency for Cybersecurity
EU	: European Union
FCOC	: UK Ministry of Defence Future Character of Conflict Report
FVEY	: The Five Eyes Alliance
GAO	: US Government Accountability Office
GDELT	: Global Data on Events, Location and Tone
HMG	: His/Her Majesty's Government
IAEA	: International Atomic Energy Agency
ICEWS	: Integrated Conflict Early Warning System
ICJ	: International Court of Justice
ICT(s)	: Information and Communication Technologies
IP	: Intellectual property
IR	: International Relations
IoT(s)	: Internet of Things
JCPOA	: Joint Comprehensive Plan of Action
KEDS	: Kansas Event Data System
MANPADS	: Man-Portable Air Defence Missiles
MCDC	: Multinational Capability Development Campaign
MEK	: People's Mujahedeen of Iran (Mujahedeen-e-Khalq)
MI6	: British Secret Intelligence Service
MoU	: Memorandum of Understanding
MPs	: Members of Parliament
NATO	: North Atlantic Treaty Organization
NCSC	: UK National Cyber Security Centre

NLP	: Natural Language Processing
OSCE	: Organisation for Security and Cooperation in Europe
PETRARCH-2	: Python Engine for Text Resolution and Related Coding Hierarchy-2
PKK	: Kurdistan Workers' Party
PLA	: Chinese People's Liberation Army
PLOVER	: Political Language Ontology for Verifiable Event Records
PRC	: People's Republic of China
RF	: Random Forest
RMA	: Revolution in Military Affairs
RMSE	: Root Mean Square Error
SML	: Supervised Machine Learning
SVM	: Support Vector Machines
SAR	: Special Administrative Region
TABARI	: Textual Analysis By Augmented Replacement Instructions
UN	: United Nations
UNSC	: United Nations Security Council
UNGGE	: United Nations Group of Governmental Experts
UK	: United Kingdom
US	: United States
USSR	: The Union of Soviet Socialist Republics
WEIS	: World Event/Interaction Survey

LIST OF FIGURES

Page Number

LIST OF TABLES

Page Number

RÉSUMÉ

Cette étude examine le rôle des cyber-attaques en tant qu'instruments de politique étrangère dans les relations trilatérales, en se concentrant sur les relations du Royaume-Uni avec la "Russie-Ukraine", la "Chine-Hong Kong" et " Iran-Israël", ainsi que sur les opérations de cyber-perturbation visant le Royaume-Uni entre 2014 et 2023. Selon les données de NETSCOUT, le Royaume-Uni a été le pays européen le plus visé par les attaques DDoS au cours de la dernière décennie. Il existe une corrélation entre le niveau de développement technologique d'un pays et la probabilité qu'il soit la cible de cyberattaques. En effet, si un pays dispose d'un niveau de développement technologique limité et d'un nombre restreint d'utilisateurs de ces technologies, cela signifie que les attaquants disposent également d'un nombre limité d'alternatives pour attaquer. Toutefois, le Royaume-Uni a été beaucoup plus visé que d'autres pays européens ayant un niveau de développement technologique similaire, tels que l'Allemagne et la France. Cela suggère que la situation du Royaume-Uni ne peut s'expliquer uniquement par son niveau de développement technologique. À cet égard, cette étude soutient que la politique étrangère plus active et plus affirmée du Royaume-Uni, tant au niveau systémique que régional, en particulier dans le cadre de la doctrine « Global Britain », est un facteur causal significatif de la fréquence plus élevée des cyberattaques dont il est la cible par rapport à d'autres pays européens. À cet égard, cette étude vise tout d'abord à explorer "les circonstances dans lesquelles les États utilisent les cyber-attaques comme instruments de politique étrangère". En outre, pour approfondir cette question de recherche, l'étude examine également « dans quels cas, quels États utilisent quel type d'outils cybernétiques contre quels États ».

Depuis que Carl von Clausewitz a écrit son célèbre passage, « La guerre n'est que la continuation de la politique par d'autres moyens », les principaux objectifs politiques sont restés inchangés, mais les méthodes de guerre permettant d'atteindre ces objectifs politiques se sont considérablement développées. Tout au long de l'histoire, les États ont utilisé les nouvelles technologies comme un nouvel instrument de puissance, parallèlement à d'autres instruments, de manière adaptée pour atteindre des objectifs politiques sans recourir aux moyens traditionnels. Toutefois, il existe une différence fondamentale entre les cyber technologies et les autres avancées technologiques. Le cyberespace a une structure et une logique uniques : Il est créé par les hommes et privilégie le secret à la sécurité. Par conséquent, le cyberespace offre aux États l'avantage d'un déni plausible, ce qui permet l'ambiguïté et la visibilité tout en permettant aux États d'opérer facilement dans la zone grise, où la frontière entre la paix et la guerre est très floue. Cette situation rend difficile la prévention et la dissuasion des cyber-attaques, soulignant la nécessité d'accroître la résilience des États et des sociétés dans la lutte contre les outils hybrides tels que les cyber-attaques. Dans ce contexte, cette étude examine en second lieu une autre question: « Comment les États peuvent-ils améliorer leurs capacités de détection et d'identification des cyberattaques à motivation politique en tant que menaces hybrides majeures ? » Pour approfondir cette question de recherche, l'étude aborde également la question suivante

: « Comment peut-on développer des systèmes d'alerte précoce pour analyser des indicateurs politiques complexes et alerter les États de la possibilité croissante d'opérations de cyber-perturbation parrainées par des États sur la base de ces indicateurs politiques ? »

En se basant sur ces questions de recherche, cette étude aborde tout d'abord dans un premier chapitre l'approche de la guerre hybride et sa nature changeante au cours des deux dernières décennies. La doctrine dite de Gerasimov, qui souligne l'importance croissante des méthodes non militaires pour atteindre les objectifs politiques et stratégiques, et la conviction largement répandue que la Russie a adopté la guerre hybride dans le cadre de sa politique étrangère, ont contribué à la popularité croissante du concept. Toutefois, d'aucuns critiquent le fait que le concept se soit écarté de sa définition initiale et soit devenu un mot à la mode et ambigu, réduisant ainsi la clarté conceptuelle. En outre, comme l'accent est mis de plus en plus sur les outils non cinétiques, certains affirment que la guerre hybride diffère de la guerre dans la zone grise/la guerre politique et que les deux concepts ne devraient pas être utilisés de manière interchangeable. Cette étude compare les deux approches en soulignant leurs différences et leurs similitudes. En conséquence, elle affirme que la principale différence réside dans l'accent mis sur l'utilisation d'outils non cinétiques. Néanmoins, cette étude soutient que ce n'est pas parce que les outils non cinétiques sont non militaires qu'ils sont nécessairement inoffensifs et non violents, comme on l'a vu dans l'affaire Stuxnet, qui cause des dommages physiques comme les outils conventionnels. En outre, avec les progrès technologiques (par exemple, l'intelligence artificielle), les capacités offensives augmenteront également de manière significative, ce qui rendra la classification de ces outils plus difficile que jamais. C'est pourquoi cette étude suggère de se concentrer sur le rôle des outils eux-mêmes plutôt que de s'engager dans de nouveaux débats théoriques sur l'inclusion ou l'exclusion des outils.

À cet égard, dans le deuxième chapitre, les différents rôles des outils cybernétiques dans les relations interétatiques sont abordés par « trois groupes de chercheurs ». Un premier groupe affirme que les cyber-attaques ont changé la nature de la guerre et entraîné une révolution dans les affaires militaires. Par conséquent, la cyberguerre serait un substitut à la guerre conventionnelle et les cyber outils pourraient modifier l'équilibre des puissances dans le système international. Le second groupe s'oppose au concept de cyberguerre et affirme que les cyber outils sont des outils plutôt limités en termes d'escalade et de coercition, et que les cyber outils deviennent efficaces lorsqu'ils sont combinés à d'autres outils traditionnels. En outre, certains universitaires du deuxième groupe affirment même que la principale motivation des États pour choisir une cyber-attaque à effet limité plutôt qu'une arme conventionnelle est d'utiliser les cyber-outils pour la gestion des conflits. Le dernier groupe part du principe que les cyber-outils sont de nouveaux outils autonomes qui peuvent modifier l'équilibre des forces sans recourir aux outils conventionnels. Ils affirment que les États limitent intentionnellement l'impact des outils cybernétiques afin de mettre en place des « faits accomplis » et d'exploiter progressivement les vulnérabilités. Ils mettent donc l'accent sur les effets cumulatifs à long terme des cyber-attaques plutôt que sur l'analyse de leur efficacité individuelle. Sur la base de ces approches, la présente étude adopte principalement les hypothèses du deuxième groupe et évalue les cyber outils comme des instruments de politique étrangère complémentaires dans le cadre de la diplomatie coercitive afin d'obtenir un avantage stratégique sur les rivaux. Néanmoins, à l'instar du troisième groupe, au lieu d'analyser les cyber-attaques individuellement, cette étude met l'accent sur l'utilisation à long terme des cyber-outils parce que les

États rivaux utilisent ces outils pour façonner la rivalité à long terme d'une manière plus indirecte au lieu d'obtenir des concessions immédiates. De cette manière, la façon dont les États utilisent les cyber-instruments comme outils de politique étrangère peut être évaluée d'un point de vue plus holistique.

Outre ces discussions dans la littérature, cette étude élargit également la compréhension du rôle des cyber-attaques en se concentrant sur les relations trilatérales. En général, les cyber-attaques sont examinées dans le cadre de relations bilatérales. Or, les relations entre les États s'inscrivent dans des réseaux complexes. En particulier, lorsqu'un État qui revêt une importance stratégique pour deux États rivaux accroît sa coopération avec l'un d'entre eux, l'autre rival est considérablement affecté par cette collaboration. Toutefois, dans de tels cas de rapprochement, les États disposent d'un ensemble limité d'outils de politique étrangère par rapport aux circonstances comparées à la détérioration des relations. Cette étude part du principe que les cyber-attaques offrent des options viables dans de tels cas. Par conséquent, pour les États qui ne sont pas disposés à utiliser d'autres outils mais qui veulent faire « quelque chose » « plutôt que de ne rien faire », les cyber-attaques offrent une utilité stratégique pour transmettre des signaux sans déclencher de réponse significative. À cet égard, la présente étude émet l'hypothèse que « lorsque l'un des deux États rivaux accroît son niveau de coopération avec un pays tiers stratégiquement important pour les deux États rivaux, la probabilité que l'autre État rival lance des opérations de cyber-perturbation contre son rival augmente ».

Pour vérifier cette hypothèse, la relation entre les relations trilatérales du Royaume-Uni avec la "Russie-Ukraine," "Chine-Hong Kong" et "Iran-Israël" et les opérations de perturbation cybernétique visant le Royaume-Uni entre 2014 et 2023 est examinée. Selon les rapports officiels britanniques, l'objectif premier du Royaume-Uni est de « contrer les menaces étatiques », en particulier celles provenant de la Chine (menace systémique), de la Russie (menace la plus aiguë) et de l'Iran (menace déstabilisatrice). En outre, la Chine, la Russie et l'Iran sont considérés comme les principaux acteurs de la cybermenace ciblant le Royaume-Uni. Dans ce contexte, cette étude examine comment les opérations de cyber-perturbation sont utilisées par ces « suspects habituels » comme instrument de politique étrangère en réponse à la collaboration accrue du Royaume- Uni avec des acteurs stratégiques - l'Ukraine, Hong Kong et Israël, respectivement. Des méthodes de recherche quantitatives sont employées pour cette enquête. Plus précisément, parmi les différents types de cyber-attaques, seules les attaques DDoS ont été retenues en raison de leur facilité d'exécution, de leur occurrence lors de crises et d'événements géopolitiques, de leur rôle complémentaire par rapport aux événements politiques et militaires et de la disponibilité de données permettant une recherche quantitative. Deuxièmement, pour analyser quantitativement les relations du Royaume-Uni sur une période donnée, cette étude utilise des données événementielles, qui codent divers événements politiques entre États par le biais d'une analyse textuelle. Ces événements codés sont ensuite notés sur l'échelle de Goldstein, qui va de -10 à 10. Après avoir créé des ensembles de données sur les cyberattaques et les événements et examiné les aspects historiques de ces trois relations trilatérales, cette étude a effectué trois analyses de *Régression Logistique Binaire* pour tester la relation de cause à effet entre les trois relations trilatérales du Royaume-Uni et les opérations de cyber perturbation qui le ciblent.

En conséquence, ces analyses révèlent qu'il y a une probabilité accrue d'opérations de cyber-perturbation graves à l'encontre du Royaume-Uni lorsque le

niveau de coopération du Royaume-Uni augmente avec Israël, l'Ukraine et Hong Kong, alors que le niveau de conflit du Royaume-Uni augmente avec la Chine et la Russie. En outre, même si les relations entre le Royaume-Uni et l'Iran n'ont aucune relation statistique, cette étude souligne que les relations du Royaume-Uni avec Israël - l'ennemi juré de l'Iran dans la région - pourraient inciter davantage l'Iran à utiliser des opérations de cyber-perturbation contre le Royaume-Uni. Avec les attaques DDoS, ces États ciblent des institutions/entreprises largement utilisées par la population plutôt que des cibles militaires ou gouvernementales. En menant des cyberattaques fréquentes, leur objectif est d'augmenter le nombre de personnes touchées par ces attaques. Même si les attaques elles-mêmes ne sont pas trop destructrices, leur objectif est de mener des attaques DDoS fréquentes et limitées et de les rendre publiques afin d'accroître la perception de l'insécurité et de réduire la confiance dans les gouvernements. En conséquence, les opérations de cyber-perturbation sont utilisées comme des « opérations d'influence » pour influencer la société et créer des perturbations à des fins politiques. En ce sens, cette étude soutient qu'au lieu d'utiliser la diplomatie formelle/informelle (négociation explicite) pour influencer la décision du Royaume-Uni lorsqu'il est directement impliqué dans les affaires régionales/internes en s'engageant dans des relations avec l'Ukraine, Hong Kong et Israël, ces suspects habituels mènent des opérations de cyber-perturbation en tant qu'instruments de négociation tacite contre le Royaume-Uni dans le cadre de la diplomatie coercitive.

En outre, une analyse de corrélation de Pearson est également réalisée pour examiner l'utilisation des cyberattaques contre des alliés dans la même région et pour vérifier s'il existe une corrélation entre la fréquence des cyberattaques ciblant le Royaume-Uni et d'autres pays d'Europe. Cette analyse révèle une corrélation positive significative entre le Royaume-Uni et l'Allemagne, la Belgique, l'Italie et l'Espagne en ce qui concerne la fréquence des cyberattaques entre 2015 et 2022. Ces résultats fournissent des indices importants sur les acteurs possibles de la menace en Europe, l'utilisation des cyberattaques dans la dynamique régionale, la dynamique de la sécurité européenne après le Brexit, la politique étrangère du Royaume-Uni au cours de la dernière décennie et la perception des suspects habituels à son égard.

Sur la base de tous ces résultats, un « modèle d'alerte précoce basé sur l'IA » est développé pour détecter/prédire les opérations de cyber-perturbation à motivation politique importantes en analysant simultanément les relations dyadiques du Royaume-Uni et les cyberattaques qui le ciblent. Pour élaborer ce modèle, quatre algorithmes d'apprentissage automatique sont formés à partir des relations dyadiques du Royaume-Uni avec 14 pays et des cyber-attaques ciblant le Royaume-Uni entre 2014 et 2023. D'après les performances de validation et de test de ces modèles, on observe que le modèle K-Nearest Neighbors (KNN) présente les mesures de performance d'IA les plus élevées (exactitude, précision, rappel et F1-Score) à la fois dans les phases de validation et de test. Ces résultats suggèrent que le modèle KNN peut être utilisé efficacement pour prédire les cyberattaques potentielles de perturbation à caractère politique ciblant le Royaume-Uni. En outre, le modèle KNN fournit également une fonctionnalité qui montre l'importance de chaque relation dyadique sur les performances du modèle. Cette caractéristique offre ainsi des indications précieuses sur l'importance relative des relations bilatérales pour prédire les cyberattaques importantes à motivation politique et propose un moyen d'améliorer les performances du modèle. En résumé, ces résultats sont significatifs car le modèle KNN pourrait servir de modèle pionnier pour le développement d'une version plus

complexe et avancée, telle qu'un modèle prédictif automatisé en temps réel. De cette façon, ce modèle pourrait contribuer à rendre les États et les sociétés plus résilients en mettant en place les mécanismes nécessaires pour réagir/répondre plus tôt à d'éventuelles cyberattaques importantes commanditées par des États.

ABSTRACT

This study examines the roles of cyber-attacks as foreign policy instruments in trilateral relations, focusing on the United Kingdom's (UK) relations with "Russia-Ukraine", "China-Hong Kong" and "Iran-Israel" as well as cyber-disruption operations targeting the UK between 2014 and 2023. Over the past decade, the UK has been the most targeted European country for Distributed Denial of Service (DDoS) attacks, according to data from NETSCOUT. There is a correlation between a country's level of technological development and its likelihood of being the target of cyber-attacks. This is because if a country has a limited level of technological development and a limited number of users of these technologies, it means that attackers also have limited alternatives to attack. However, the UK has been targeted much more than other European countries at a similar level of technological development, such as Germany and France. This suggests that the UK's situation cannot be explained solely by its level of technological development. In this respect, this study argues that the UK's more active and assertive foreign policy, both systemic and regional levels, particularly in line with the Global Britain doctrine, is a significant causal factor for its higher frequency of being targeted to cyber-attacks compared to other European countries. In this respect, this study firstly aims to explore "under what circumstances do states resort to cyber-attacks as instruments of foreign policy". Additionally, to elaborate on this research question, the study also investigates "in which cases, which states utilize which type of cyber tools against which states".

Ever since Carl von Clausewitz wrote his famous passage, "*War is merely the continuation of politics by other means*" the primary political objectives have remained unchanged; however, the methods of warfare for achieving these political goals have significantly expanded. Throughout history, states have utilized new technologies as a new power instrument alongside other instruments in tailored ways to achieve political goals without resorting to traditional means. However, there is a fundamental difference between cyber technologies and other technological advancements. Cyberspace has a unique structure and logic: It is human-made and prioritizes secrecy over security. As a result, cyberspace provides states with the advantage of plausible deniability, allowing for ambiguity and visibility while enabling states to operate easily in the grey area, where the line between peace and war is significantly blurred. This situation makes it challenging to prevent and deter cyber-attacks, highlighting the necessity of increasing the resilience of states and societies in combating hybrid tools such as cyber-attacks. In this context, this study secondly examines another question: "How can states enhance their detection and identification capabilities of politically motivated cyber-attacks as major hybrid threats?" To further explore this research question, the study also addresses "How can early warning systems be developed to analyse complex political indicators and alert states to the increasing possibility of state-sponsored cyber disruption operations based on these political indicators?"

Based on these research questions, in the first chapter, this study addresses the hybrid warfare approach and its changing nature in the last two decades. The so-called Gerasimov doctrine, which highlights the increasing significance of non-military methods for achieving political and strategic objectives, and the widespread belief that Russia has adopted hybrid warfare as part of its foreign policy, have contributed to the rising popularity of the concept. However, there is criticism that the concept has deviated from its original definition and has become a buzzword and ambiguous, reducing conceptual clarity. Furthermore, as the emphasis on non-kinetic tools increases, some argue that hybrid warfare differs from grey zone warfare/political warfare and two concepts should not be used interchangeably. This study compares two approaches by highlighting their differences and similarities. Accordingly, this study asserts that the main difference lies in their emphasis on the use of non-kinetic tools. Nevertheless, this study contends that just because non-kinetic tools are non-military does not mean that they are necessarily harmless and non-violent and harmless as seen in the Stuxnet case, which causes physical damage as conventional tools. Moreover, with further technological developments (e.g., artificial intelligence), offensive capabilities will also increase significantly, and this will make it difficult to classify these tools more than ever. Hence, this study suggests focusing on the role of the tools themselves rather than engaging in further theoretical debates on the inclusion/exclusion of tools.

In this respect, in the second chapter, the different roles of cyber tools in interstate relations are addressed via "*three groups of scholars*". The first group argues that cyber-attacks have been changing the nature of war and led to a revolution in military affairs. Hence, cyber war would be a substitute for conventional war, and cyber tools could change the balance of power in the international system. The second group opposes the concept of cyber war, and they argue that cyber tools are rather limited tools in terms of escalation and coercion, and cyber tools become effective when combined with other traditional tools. Moreover, some of the scholars in the second group even argue that the main motivation for states to choose a limited-effect cyber-attack instead of a conventional weapon is to use cyber tools for conflict management. The last group assumes that cyber tools are new standalone tools that can change the balance of power without resorting to conventional tools. They argue that states intentionally limit the impact of cyber tools to conduct "fait accompli" and exploit vulnerabilities gradually. Hence, they emphasize the long-term cumulative impacts of cyber-attacks instead of analysing their individual effectiveness. Based on these approaches, this study mainly adopts the second group's assumptions and evaluates cyber tools as complementary foreign policy instruments within the framework of coercive diplomacy to gain a strategic advantage over rivals. Nevertheless, similar to the third group, instead of analysing cyber-attacks individually, this study emphasizes the long-term use of cyber tools because rival states employ these tools to shape long-term rivalry in a more indirect manner instead of obtaining immediate concessions. In this way, how states use cyber instruments as foreign policy tools can be evaluated from a more holistic perspective.

In addition to these discussions in the literature, this study also expands the understanding of cyber-attacks' role by focusing on trilateral relations. In general, cyber-attacks are examined through bilateral relations. Nevertheless, states' relations take place in complex networks. In particular, when a state that holds strategic importance for two rival states increases its cooperation with one of the rivals, the other rival is significantly impacted by this collaboration. However, in such

rapprochement cases, states have a limited set of foreign policy tools than in the circumstances compared to deteriorating relations. This study posits that cyber-attacks offer viable options in such cases. Therefore, for states who are unwilling to use other tools but want to do “something” “rather than doing nothing”; cyber-attacks offer strategic utility to convey signals without triggering a significant response. In this regard, this study hypothesizes that “*when one of two rival states increases its cooperation level with a strategically important third country for both rival states, the likelihood of the other rival state launching cyber-disruption operations against its rival increases*”.

To test this hypothesis, the relationship between the UK's trilateral relations with "Russia-Ukraine", "China-Hong Kong" and "Iran-Israel" and cyber disruption operations targeting the UK between 2014 and 2023 is examined. According to official UK reports, the UK’s primary objective is to "*counter state threats*", particularly those originating from China (systemic threat), Russia (most acute threat), and Iran (destabilizing threat). Furthermore, China, Russia and Iran are identified as the top cyber threat actors targeting the UK. In this context, this study investigates how cyber disruption operations are utilized by these 'usual suspects' as a foreign policy instrument in response to the UK's increased collaboration with strategic actors – Ukraine, Hong Kong, and Israel, respectively. Quantitative research methods are employed for this investigation. Specifically, among the various types of cyber-attacks, only DDoS attacks are selected due to their ease of conduct, their occurrence during crises and geopolitical events, their complementary role to political and military events, and the availability of data that allow for quantitative research. Secondly, to quantitatively analyse the UK's relations over a specific period, this study employs event data, which codes various political events between states through text-based analysis. These coded events are then scored by the Goldstein scale, ranging from -10 to 10. After creating datasets of cyber-attack and event data and examining these three trilateral relations from a historical perspective, this study conducted three Binary Logistic Regression analyses to test the causal relationship between the UK's trilateral relationships and cyber-disruption operations targeting it.

Accordingly, these analyses reveal that there is an increased likelihood of serious cyber-disruption operations towards the UK when the UK's cooperation level increases with Israel, Ukraine, and Hong Kong, whereas the UK’s conflict level increases with China and Russia. Moreover, even though the UK-Iran relations have no statistical relations, this study stresses that the UK's relations with Israel - the archenemy of Iran in the region - could be more urging for Iran to use cyber disruption operations against the UK. With DDoS attacks, these states target institutions/businesses that are widely used by the people rather than military or governmental targets. Through frequent cyber-attacks, their goal is to increase the number of people impacted by these attacks. Even if the attacks themselves are not overly destructive, their aim is to conduct frequent, limited DDoS attacks and publicize them to heighten the perception of insecurity and reduce trust in governments. As a result, cyber disruption operations are used as "influence operations" to influence society and create disruption for political purposes. In this sense, this study contends that rather than using formal/informal diplomacy (explicit bargaining) to influence the UK’s decision when directly involved in regional/internal affairs by engaging in relations with Ukraine, Hong Kong, and Israel, these usual suspects conduct cyber disruption operations as instruments of tacit bargaining against the UK in the framework of coercive diplomacy.

Furthermore, Pearson Correlation analysis is also conducted to examine the use of cyber-attacks against allies in the same region and to test whether there is a correlation between the frequency of cyber-attacks targeting the UK and other countries in Europe. Accordingly, this analysis indicates a significant positive correlation between the UK and Germany, Belgium, Italy, and Spain regarding the frequency of cyber-attacks between 2015 and 2022. These findings provide important clues about the possible threat actors in Europe, usage of cyber-attacks in regional dynamics, the European security dynamics after Brexit, the foreign policy of the UK in the last decade, and the usual suspects' perception toward it.

Based on all these findings, as a final step, an "AI-based early warning model" is developed to detect/predict significant politically motivated cyber disruption operations by simultaneously analysing dyadic relations of the UK and cyber-attacks targeting it. To develop this model, four machine learning algorithms are trained by the UK's dyadic relations with 14 countries along with cyber disruption operations targeting the UK between 2014-2023. According to the validation and test performance of these models, it is observed that K-Nearest Neighbors (KNN) has the highest AI performance metrics (accuracy, precision, recall and F1-Score) in both the validation and test phases. These results suggest that KNN can be effectively used to predict potential politically motivated cyber disruption attacks targeting the UK. Additionally, the KNN model also provides a feature that shows the importance of each dyadic relationship on the model's performance. Thus, this feature presents valuable insights into the relative importance of bilateral relations for predicting significant politically motivated cyber-attacks and offers a way of enhancing the model's performance. To sum up, these findings are significant because the KNN model could serve as a pioneering model for the development of a more complex and advanced version, such as a real-time automated predictive model. In this way, this model could contribute to making states and societies more resilient by enabling necessary mechanisms to react/respond earlier to possible significant state-sponsored cyber-attacks.

ÖZET

Bu çalışma, siber saldırıların üçlü ilişkilerde bir dış politika aracı olarak rolünü, 2014-2023 yılları arasında Birleşik Krallık'ı hedef alan siber saldırılar ve Birleşik Krallık'ın "Rusya-Ukrayna", "Çin-Hong Kong" ve "İran-İsrail" ile üçlü ilişkilerine odaklanarak incelemektedir. Açık kaynaklardan elde edilen verilere göre Birleşik Krallık son on yılda Dağıtık Hizmet Engelleme (Distributed Denial of Service – DDoS) saldırılarının en çok hedefi olan Avrupa ülkesi olmuştur. Bir ülkenin teknolojik gelişmişlik düzeyi ile siber saldırılara uğraması arasında güçlü bir korelasyon vardır. Zira bir ülkenin teknolojik gelişmişlik düzeyi ve bu teknolojileri kullanan kullanıcı sayısı ne kadar sınırlıysa saldırganların da benzer oranda saldırmak için sınırlı alternatifleri vardır. Buna karşın Birleşik Krallık, Almanya ve Fransa gibi benzer teknolojik gelişmişlik düzeyindeki diğer Avrupa ülkelerinden çok daha fazla siber saldırının hedefi olmaktadır. Bu durum, Birleşik Krallık'ı hedef alan siber saldırıları sadece teknolojik gelişmişlik düzeyi ile açıklamanın yetersiz olduğunu göstermektedir. Bu çalışmada Birleşik Krallık'ın özellikle Küresel Britanya (Global Britain) doktrini doğrultusunda hem sistemik hem de bölgesel düzeyde daha aktif ve iddialı bir dış politika izlemesinin, diğer Avrupa ülkelerine kıyasla daha fazla siber saldırının hedefi olmasında önemli bir faktör olduğunu savunmaktadır. Bu doğrultuda çalışmada ilk olarak "devletler hangi koşullar altında dış politika aracı olarak siber saldırılara başvurmaktadır" sorusuna yanıt arayacaktır. Bu araştırma sorusuna ilaveten "hangi durumlarda, hangi devletler hangi devletlere karşı hangi tür siber araçları kullanmaktadır" sorusuna da yanıt aranarak siber saldırıların dış politikadaki araçsallaştırılması aydınlatılmaya çalışılacaktır.

Carl von Clausewitz'in "*Savaş, siyasetin başka araçlarla devamıdır*" şeklindeki ünlü pasajını yazmasından bu yana devletlerin başlıca siyasi hedefleri değişmese de siyasi hedeflere ulaşmak için kullandıkları savaş yöntemleri önemli ölçüde çeşitlenmiştir. Tarih boyunca devletler, geleneksel araçlara başvurmadan siyasi hedeflere ulaşmak için mevcut araçların yanı sıra yeni teknolojileri de yeni bir güç aracı olarak kullanmışlardır. Ancak siber teknolojiler ile diğer teknolojik gelişmeler arasında temel bir fark vardır. Siber saldırıların gerçekleştiği boyut olan siber uzay diğer boyutların aksine "*insan yapımıdır"* ve güvenlikten ziyade "*gizliliğe"* öncelik vermektedir. Bu özellikler, siber uzayda devletlere "*makul inkar edilebilirlik*" (plausible deniability) imkanı sağlayarak barış ve savaş arasındaki çizginin önemli ölçüde bulanıklaştığı gri bölgede kolaylıkla faaliyet yürütmelerine imkan tanımaktadır. Devletlerin bu faaliyetleri, siber saldırıların önlenmesini ve caydırılmasını zorlaştırırken diğer taraftan devletlerin siber saldırılar gibi hibrit araçlara karşı mücadelede neden direncin (resilience) artırılması gerektiğinin önemini göstermektedir. Bu bağlamda bu çalışma ikinci olarak "*devletler, bir hibrit tehdit olarak siyasi amaçlı siber saldırıları tespit etme ve tanımlama yeteneklerini nasıl geliştirebilir?"* sorusuna da yanıt aramaktadır. Bu araştırma sorusu kapsamında ise bu çalışma, "*Karmaşık siyasi gelişmeleri analiz etmek ve devletleri bu siyasi gelişmelere dayalı devlet destekli siber bozma operasyonlarına karşı uyarmak için erken uyarı sisteminin nasıl geliştirilebileceğini"* de araştırmaktadır.

Bu araştırma soruları doğrultusunda ilk bölümde, hibrit savaş yaklaşımı ve hibrit savaşın son yirmi yılda değişen doğası ele alınmıştır. Siyasi ve stratejik hedeflere ulaşmak için askeri olmayan yöntemlerin artan önemini vurgulayan Gerasimov Doktrini ve Rusya'nın hibrit savaşı dış politikasının bir parçası olarak benimsediğine dair özellikle Batı dünyasında kabul gören yaygın inanç, hibrit savaş kavramın literatürde yaygın kullanılmasına yol açmıştır. Bu geniş çaplı kullanımıyla birlikte, Hibrit Savaş kavramının başta geleneksel olmayan araçlar olmak üzere çok sayıda aracı kapsar hale gelmesi, kavramın orijinal yaklaşımından saparak belirsizleştiği yönünde eleştirilmesine neden olmuştur.

Dahası, kinetik olmayan araçlara yapılan vurgu arttıkça, literatürde hibrit savaşın gri bölge savaşı/politik harp'ten farklı olduğuna ve iki kavramın birbirinin yerine kullanılmaması gerektiğine dair eleştiriler artmaktadır. Bu doğrultuda iki yaklaşımın farklılıkları ve benzerlikleri vurgulanarak iki yaklaşım arasındaki temel farkın geleneksel olmayan araçların kullanımına yaptıkları vurgu olduğu belirtilmiştir. Buna karşın bu çalışma bu ayrımın giderek zorlaştığını iddia etmektedir. Stuxnet siber saldırısının geleneksel güç araçları gibi fiziksel hasara yol açması, geleneksel olmayan araçların da zarar ve şiddet içerebileceğini göstermektedir. Dahası, yapay zekâ gibi teknolojik gelişmelerle birlikte özellikle siber saldırı kabiliyetleri de önemli ölçüde artacak ve bu durum geleneksel olmayan araçların sınıflandırılmasını her zamankinden daha zor hale getirecektir. Dolayısıyla bu çalışma, geleneksel olmayan araçların ve yöntemlerin konseptlere dahil edilmesi/çıkarılması konusunda daha fazla teorik tartışmaya girmek yerine bu araçların doğrudan kendilerine odaklanmayı önermektedir.

Bu doğrultuda ikinci bölümde siber araçların devletlerarası ilişkilerdeki farklı rolleri "*üç grup*" çerçevesinde ele alınmaktadır. İlk grup, siber saldırıların savaşın doğasını değiştirdiğini ve askeri ilişkilerde bir devrime yol açtığını savunmaktadır. Dolasıyla siber savaşın konvansiyonel savaşın yerine geçebileceğini ve siber araçların uluslararası sistemdeki güç dengesini değiştirebileceğini iddia etmektedir. İkinci grup ise siber savaş kavramına karşı çıkmakta ve siber araçların "*tırmanma*" (escalation) ve "*baskı*" (coercion) kapsamında oldukça sınırlı araçlar olduğunu, siber araçların diğer geleneksel araçlarla birlikte kullanıldığında etkili hale geldiğini savunmaktadır. Ayrıca ikinci gruptaki bazı akademisyenler, devletlerin konvansiyonel bir silah yerine sınırlı etkiye sahip bir siber saldırıyı tercih etmelerindeki temel motivasyonun çatışma yönetimi için siber araçları kullanmak olduğunu savunmaktadır. Üçüncü grup ise siber araçların konvansiyonel araçlara başvurmadan güç dengesini değiştirebilecek yeni bağımsız araçlar olduğunu belirtmektedir. Devletlerin siber araçların etkisini zafiyetlerden kademeli olarak yararlanmak için kasıtlı olarak sınırladığını belirten üçüncü grup, siber saldırıları tek tek analiz etmek yerine uzun vadeli kümülatif etkilerine odaklanılması gerektiğini vurgulamaktadır. Bu üç yaklaşım doğrultusunda bu çalışma çoğunlukla ikinci grubun varsayımlarını benimsemekte ve siber araçları rakiplere karşı stratejik avantaj elde etmek için zorlayıcı diplomasi çerçevesinde tamamlayıcı dış politika araçları olarak değerlendirmektedir. Bununla birlikte, üçüncü grubun önermeleri doğrultusunda siber saldırıları tek tek analiz etmek yerine uzun vadeli kullanımlarına ve etkilerine vurgu yapmaktadır çünkü devletler bu araçları anlık tavizler elde etmek yerine daha uzun vadeli rekabetlerini şekillendirmek için kullanmaktadır. Böylece devletlerin siber araçları dış politika aracı olarak nasıl kullandıkları daha bütüncül bir bakış açısıyla değerlendirilebilecektir.

Literatürdeki bu tartışmalara ek olarak ise bu çalışma, üçlü ilişkilere odaklanarak siber saldırıların dış politikadaki kullanımına dair bakış açısını genişletmeyi amaçlamaktadır. Genel olarak siber saldırılar ikili ilişkiler üzerinden incelenmektedir. Buna karşın devletlerin ilişkileri karmaşık ağlar içerisinde gerçekleşmektedir. Özellikle iki rakip devlet için stratejik öneme sahip bir devlet, rakiplerinden biriyle iş birliğini artırdığında, diğer rakip bu iş birliğinden önemli ölçüde etkilenmektedir. Ancak bu tür yakınlaşma durumlarında devletler, ilişkilerin kötüleştiği durumlara kıyasla daha sınırlı dış politika araçlarına sahiptir. Bu çalışma, siber saldırıların bu tür durumlarda devletler için kullanışlı birer stratejik araç haline geldiğini öne sürmektedir. Dolayısıyla, diğer araçları (özellikle konvansiyonel araçları) kullanamayan yahut kullanmak istemeyen fakat bir yandan da tepkisiz kalmak istemeyen devletler; yakınlaşmadan duydukları rahatsızlığı siber araçlara başvurarak göstermektedir. Bu sayede devletler bir yandan tepkilerini gösterebilirlerken diğer taraftan siber araçların makul inkâr edilebilirlik avantajından yararlanarak krizi kontrol altına alabilmektedir. Bu bağlamda, bu çalışma "*iki rakip devletten biri, her iki rakip devlet için de stratejik öneme sahip bir üçüncü devlet ile iş birliği düzeyini artırdığında, diğer rakip devletin rakibine karşı siber bozma operasyonları başlatma olasılığı artar*" hipotezini öne sürmektedir.

Bu hipotezi test etmek için, 2014-2023 yılları arasında Birleşik Krallık'ın "Rusya-Ukrayna," "Çin-Hong Kong," ve "İran-İsrail" ile olan üçlü ilişkileri ile Birleşik Krallık'ı hedef alan siber bozma operasyonları arasındaki ilişki incelenmiştir. Birleşik Krallık'ın resmi raporlarına göre, Birleşik Krallık'ın öncelikli hedefi, özellikle Çin (sistemik tehdit), Rusya (en ciddi tehdit) ve İran'dan (istikrarsızlaştırıcı tehdit) kaynaklanan "devlet tehditlerine karşı koymaktır". Ayrıca, Çin, Rusya ve İran, Birleşik Krallık'ı hedef alan en önemli siber tehdit aktörleri olarak tanımlanmaktadır. Bu bağlamda bu çalışma, Birleşik Krallık'ın Ukrayna, Hong Kong ve İsrail gibi stratejik aktörlerle artan iş birliğine karşılık olarak siber bozma operasyonlarının "olağan şüpheliler" tarafından bir dış politika aracı olarak nasıl kullanıldığını araştırmaktadır. Bu inceleme için nicel araştırma yöntemleri kullanılmıştır. Öncelikle bu analiz için çok farklı siber saldırı türleri arasından, kolaylıkla gerçekleştirilebilmeleri, krizler ve jeopolitik olaylar sırasında kullanılmaları, siyasi ve askeri krizlerde tamamlayıcı rolleri ve nicel araştırmaya olanak tanıyan verilerin mevcudiyeti nedeniyle yalnızca DDoS saldırıları kullanılmıştır. İkinci olarak, Birleşik Krallık'ın belirli bir dönemdeki ilişkilerini niceliksel olarak analiz etmek için, bu çalışma, devletler arasındaki çeşitli siyasi olayları metin tabanlı analiz yoluyla kodlayan Olay Veri (Evet Data) metoduna başvurmaktadır. Kodlanan bu olaylar "-10 ile 10" değerleri arasında değişen Goldstein ölçeğine göre puanlanmaktadır. Siber saldırı ve olay verisi ile veri setleri oluşturulduktan ve bu üçlü ilişki tarihsel olarak incelendikten sonra, bu çalışmada Birleşik Krallık'ın üçlü ilişkileri ile onu hedef alan siber bozma operasyonları arasındaki nedensel ilişkiyi test etmek için üç "Lojistik Regresyon" analizi gerçekleştirilmiştir. Yapılan bu analizler, Birleşik Krallık'ın İsrail, Ukrayna ve Hong Kong ile iş birliği düzeyi artarken diğer taraftan Çin ve Rusya ile çatışma düzeyi arttığında Birleşik Krallık'a yönelik ciddi siber bozma operasyonları gerçekleşme olasılığının arttığını ortaya koymaktadır. Ayrıca, Birleşik Krallık-İran ilişkileriyle siber saldırılar arasında istatistiksel bir ilişkisi olmasa da bu çalışma, Birleşik Krallık'ın İran'ın bölgedeki başlıca düşmanı İsrail'le yakın ilişkilerinin İran'ın Birleşik Krallık'a karşı siber bozma operasyonlarını kullanması için daha fazla teşvik edici olabileceğini vurgulamaktadır. Bu bağlamda olağan şüpheliler DDoS saldırıları ile üst düzey askeri ya da devlet hedeflerinden ziyade halk tarafından yaygın olarak kullanılan kurumları/işletmeleri hedef almaktadır. Sık sık siber saldırılar

düzenleyerek, bu saldırılardan etkilenen bireylerin sayısını arttırmayı amaçlamaktadır. Saldırıların etkisi yıkıcı olmayıp sınırlı olsa da DDoS saldırılarının çok sık gerçekleştirilmesi ve kamuoyu ile saldırıların paylaşılması; güvensizlik algısını tırmandırarak hükümetlere olan güvenin sarsılmasına neden olmaktadır. Bir diğer ifadeyle siber bozma operasyonları toplumu etkilemek ve siyasi amaçlarla yıkım yaratmak için "etki operasyonları" olarak kullanılmaktadır. Bu doğrultuda bu çalışma, Birleşik Krallık'ın Ukrayna, Hong Kong ve İsrail ile iş birliğini arttırarak bölgesel/iç politika meselelerine müdahil olduğunda eylemlerini/politikalarını etkilemek için resmi/enformel diplomasiye (açık diplomasi- *explicit bargaining*) başvurmak yerine, olağan şüphelilerin zorlayıcı diplomasi (coercive diplomacy) çerçevesinde Birleşik Krallık'a karşı örtülü pazarlık (tacit bargaining) araçları olarak siber bozma operasyonları yürüttüğünü belirtmektedir.

Ayrıca, aynı bölgedeki müttefiklere karşı siber saldırıların kullanımını incelemek ve Birleşik Krallık ile Avrupa'daki diğer ülkeleri hedef alan siber saldırıların sıklığı arasında bir korelasyon olup olmadığını test etmek için Pearson Korelasyon Analizine başvurulmuştur. Yapılan bu analizle, 2015 ve 2022 yılları arasında Birleşik Krallık ile Almanya, Belçika, İtalya ve İspanya arasında siber saldırıların sıklığı açısından istatistiksel olarak anlamlı pozitif korelasyon olduğu gözlemlenmiştir. Bu bulgular, Avrupa'daki olası tehdit aktörleri, bölgesel dinamiklerde siber saldırıların kullanımı, Brexit sonrası Avrupa güvenlik dinamikleri, Birleşik Krallık'ın son on yıldaki dış politikası ve olağan şüphelilerin bu politikalara yönelik algısı hakkında önemli ipuçları sunmaktadır.

Son olarak ise, tüm bu bulgular doğrultusunda bu çalışma kapsamında Birleşik Krallık'ın ikili ilişkilerini ve onu hedef alan siber saldırıları eşzamanlı analiz eden ve devlet destekli siyasi amaç doğrultusunda gerçekleşen siber bozma operasyonlarını önceden tahmin etmek için yapay zekâ (YK) tabanlı bir erken uyarı sistemi geliştirilmiştir. Bu modeli geliştirmek için dört farklı makine öğrenmesi algoritması, Birleşik Krallık'ın 14 ülke ile ikili ilişkileri ve 2014-2023 yılları arasında Birleşik Krallık'ı hedef alan siber bozma operasyonları verileri ile eğitilmiştir. Bu modellerin validasyon ve test performanslarına göre, "K-En Yakın Komşular" (*K-Nearest Neighbors, KNN*) modelinin hem validasyon hem de test aşamalarında en yüksek performans metriklerine (doğruluk, kesinlik, duyarlılık ve F1-Skor) sahip olduğu görülmektedir. Bu sonuçlar, KNN'nin Birleşik Krallık'ı hedef alan olası siyasi amaçlı siber bozma saldırılarını tahmin etmek için etkili bir şekilde kullanılabileceğini göstermektedir. Ayrıca, KNN modeli, her bir ikili ilişkinin modelin performansı üzerindeki önemini gösteren ek bir özellik sunarak modelin daha da geliştirilmesine imkân tanımaktadır. Bu doğrultuda bu model, haberleri ve siber saldırıları gerçek zamanlı olarak toplayan ve devletler ile siber saldırılar arasındaki çatışma-iş birliği düzeyini analiz eden gerçek zamanlı erken uyarı sistemi gibi daha karmaşık ve gelişmiş bir sisteminin geliştirilmesi için bir örnek teşkil etmektedir. Böylece, bu çalışma ile geliştirilen model, Birleşik Krallık dışında diğer ülkeler tarafından da kullanılabilir ve geliştirilmeye açık bir örnek sunarak, devlet destekli siber bozma operasyonlarına karşı daha hızlı ve etkili müdahale imkânı sağlamakta, devletlerin ve toplumların siber saldırılara karşı direncini artırmaya önemli katkıda bulunmaktadır.

INTRODUCTION

Following the US-led military intervention in Iraq in 2003, there was debate about the possibility of a similar military operation against Iran. The former President of the United States (US), George W. Bush, expressed concerns about the dilemma regarding Iran: Whether to allow Iran to acquire nuclear weapons or to go to war to prevent Iran from acquiring them. When people are confronted with a dilemma, they tend to look for a third option, especially if they are not in favour of either option. Bush was also in such a situation, and he repeatedly told his secretary of state and national security adviser, "*I need a third option*" (Sanger, 2012, p. 191). Bush's search for the third option was the origin of an alleged joint US-Israeli cyber-attack (Stuxnet) on Iran's nuclear facility at Natanz to disrupt Iran's nuclear program. George W. Bush initiated a project code-named "Olympic Games" to develop a malicious computer worm designed to gradually sabotage centrifuges – the uranium enrichment machines– in order to hamper Iran's nuclear progress without carrying out a conventional military attack (This project continued during the Barack Obama administration until its discovery in 2010). Accordingly, by destroying nearly 1,000 of Iran's 6,000 centrifuges (Nakashima & Warrick, 2012), the Iranian nuclear program was severely damaged without the offensive military action as Bush desired. Hence, the Stuxnet attack marked the advent of a new alternative instrument in foreign policy for a situation in which states are reluctant or unable to use conventional tools but want to do "something without triggering significant response" rather than "doing nothing" against the actions of rivals. In this context, this study will explore how the "usual suspects" – Russia, China and Iran –utilise cyber disruption operations as instruments of foreign policy, particularly as a form of tacit bargaining, against the United Kingdom (UK) when the UK increases its cooperation with Ukraine, Hong Kong, and Israel, which are strategic actors for both the UK and the "usual suspects".

However, cyber-attacks are neither the first nor will they be the last instruments for providing alternative means for foreign policy strategies. Throughout history, states

have utilised new technologies to seek an advantage over their rivals by exploiting the advantages of new technologies (Chin, 2019). While some technological advances have a direct impact (e.g., nuclear weapons), others have a profound but indirect impact (e.g., television and radio for subversion strategies). Whether the effect is limited or great; states apply these tools as power instruments along with other tools (e.g., diplomatic, economic, military) with different levels in synchronised ways to achieve political goals without resorting to conventional means. In doing so, they seek to gain an advantage over the rival state by remaining in the grey zone, defined as the area where the line between peace and war is significantly blurred. Over the past two decades, the proliferation and widespread use of Information and Communication Technologies (ICTs) and the Internet of Things (IoTs) has led states to take advantage of new non-kinetic tools that further expand this grey zone. As a non-kinetic hybrid tool, cyber-attacks are among the most frequently used instruments in hybrid threats, which make "cyberspace a key arena for modern hybrid warfare" (Engström, 2022).

Nevertheless, there is a fundamental difference between cyber technologies and other technological advancements in other domains (land, sea, air, and space). Cyberspace, where cyber activities take place, has a distinct structure and logic: "*It is human-made",* and *"it prioritises secrecy over security".* As a result, in cyberspace, the physical laws and constraints of the real world do not apply, and it is difficult to be certain about other actors due to the great emphasis on secrecy. These unique characteristics of cyberspace make cyber-attacks inherently difficult to detect and attribute. Hence, cyber-attacks enable states to operate easily in grey zone primarily due to the advantages of creating ambiguity and offering more plausible deniability. Moreover, some scholars and experts argue that cyber-attacks would benefit weaker actors than strong ones based on the logic of asymmetry (Blank, 2008; Knapp & Boulton, 2006; McGraw, 2013; Obama, 2012). In today's world, because of the advantages offered by ICTs and IoT, developed countries, especially Western developed states, rely heavily on these technologies. As a result, ICTs and IoTs have become indispensable means for the continuation of daily life. However, this growing reliance on these technologies also makes states, particularly developed ones, more vulnerable to potential dangers (Kirsch, 2012, pp. 620–621). Thus, developed Western states which live in the great glass houses become easy targets of weaker actors that have less dependency on these technologies and cyberspace (Lindsay, 2013, p. 375).

In other words, cyber operations are rather impractical against a Stone Age tribe that uses a stone as a weapon (Maschmeyer, 2023b, p. 91).

In this respect, Fischerkeller et al. (2022, p.10) argue that while technological developments have a central role in political/military tactics and strategies, not all these developments result in a significant change in the strategic structure of security. However, cyber technologies have the potential to shape the concept of security itself. Therefore, cyber technologies create a new strategic environment (Fischerkeller et al., 2022). Within this new strategic environment, Lucas Kello (2013, p.8) stressed that the "*cyber revolution has not fundamentally changed the nature of war*"; however, "*the most obvious and important consequence of [cyber tools is their] ability to affect the balance of power*" (Kello, 2017, p. 100).

The perception that cyber tools can be effective in influencing the balance of power in the international system has also influenced attitudes towards cyber-attacks in terms of whether they are beneficial or harmful. Depending on which side of the double-faced Roman God "Janus" states look from, the usage of the cyber-attacks and their impacts also changes. On one facet, it creates a new realm of utility for states to pursue their interests; on the other, it presents a new threat. For instance, while Stuxnet offered alternative tools for the US against Iran, just after two years of revealing to Stuxnet, Barack Obama pointed to another aspect of the cyber tools: "*In a future conflict, an adversary unable to match our military supremacy on the battlefield might seek to exploit our computer vulnerabilities here at home… This is the future we have to avoid*" (Obama, 2012). While Bush used cyber-attacks as an alternative third option, Obama's statement that cyber-attacks can be used as an asymmetric tool that can replace conventional weapons, is a clear demonstration that different types of cyber-attacks are being used for different purposes based on states and their motivations. Therefore, it would be misleading to assume that there is only one type of cyber-attack and that all cyber-attacks are used for the same purposes.

This situation makes it necessary for researchers to examine cyber-attacks in more detail rather than evaluating them from the same perspective. In this regard, this study aims to explore the usage of cyber tools as a foreign policy instrument. To achieve this, the study will first address the question, "*under what circumstances do*

states resort to cyber-attacks as instruments of foreign policy?". Additionally, to elaborate on this research question, the study will also investigate "in which cases, which states utilise which type of cyber tools against which states". In order to address these questions, this study will initially discuss the hybrid warfare approach, in which cyber-attacks have been one of its main components in recent years.

Hybrid warfare is a "low-level conflict spanning the spectrum of capabilities" that merges kinetic and non-kinetic tools to "enable an actor to achieve its political aims without having to resort to large-scale conventional war" (Najžer, 2020, p. 29). Hybrid warfare has been engaged by the actors who seek to exploit the target's vulnerabilities by utilising all available means for political objectives, integrating tactics that align with one's strategic culture, geographical conditions, and available economic and military tools without engaging power politics by overt tools. This situation makes hybrid warfare a "*context-specific"* tool because *"components for hybrid warfare"* change based on the actors and situations (Najžer, 2020, p. 31). Thus, hybrid warfare is the synchronised use of different instruments of power tailored to specific vulnerabilities to produce synergistic effects on such a scale (Cullen & Reichborn-Kjennerud, 2017, p. 8). All these factors exacerbate the challenges of countering the modern hybrid threats. The targeted states encounter significant difficulties in detecting and attributing to these hybrid threats, especially when the threat is low-level and sponsor actors persistently deny any involvement. Moreover, while hybrid threats are already difficult to detect and attribute, it is even more challenging to adequately deter and respond adequately to them. As new methods technologies and methods, particularly Artificial Intelligence (AI), continue to develop, the number of offensive options and the variety of hybrid tools will significantly increase. This further will make it difficult to prevent these threats.

In this context, this study argues for the need to increase the resilience of states and societies in combating hybrid tools rather than trying to prevent them altogether. One of the first steps in enhancing resilience against hybrid threats is the early detection of the threats. Due to the design of the Internet, cyber-attacks are inherently difficult to detect and identify. Although the effects of Distributed Denial of service (DDoS) attacks are relatively easy to detect compared to other forms of cyber-attack, such as espionage and sabotage, it is crucial to determine whether the attack is state-

sponsored and which state is responsible. Therefore, anomaly detection is one of the priority steps in combating hybrid threats, especially cyber-attacks. Accordingly, this study also tries to answer the second main research question of this study: "*How can states enhance their detection and identify capabilities of politically motivated cyber-attacks as major hybrid threats?*" To further explore this research question, the study will also examine "*How can early warning systems be developed to analyse complex political indicators and alert states to the increasing possibility of state-sponsored cyber disruption operations based on these political indicators?".*

Based on these research questions, in the first chapter, basic assumptions of the hybrid warfare approach, the changing definitions of the concept of hybrid warfare and the transformation of the concept, especially after the annexation of Russia, will be addressed. Moreover, with the Russia-Ukraine crisis in 2014 and China's activities in East Asia, it will be discussed that instead of the combination of regular and irregular warfare, how hybrid warfare has come to refer to the synchronised use of non-military activities such as lawfare, economic coercion, cyber-attacks, disinformation campaigns and sabotage. In this context, this study will also address the criticisms that hybrid warfare has deviated significantly from its original form and has become a catch-all phrase and buzzword, reducing conceptual clarity. In addition, with the increasing emphasis on non-kinetic means, hybrid usage of tools has also been described with hybrid threat and grey zone warfare. Accordingly, there has been a growing body of research that suggests that hybrid warfare is different from hybrid threat and grey zone warfare/political warfare, and therefore, these concepts should not be used interchangeably (e.g. Sean Monaghan, 2019; Azad et al., 2023; Mazarr, 2015; Caliskan & Liégeois, 2021; Marsh, 2024). As the lines between these approaches have become increasingly blurred, this study will also elaborate on the differences and overlaps between them. In this respect, in the latter part of Chapter 1, hybrid warfare and hybrid threat will be compared in detail. A new sub-chapter (1.2) will be introduced in this study to compare grey zone warfare/conflict and hybrid warfare. This sub-chapter will compare these two approaches using Theodore Jensen's classification, which examines grey zone warfare through three camps: "the New Era Camp", "Hybrid Warfare Camp", and "Nothing New Camp" (T. Jensen, 2019).

Based on this literature review of hybrid warfare, this study will argue why more focus should be attained on the role of the instruments themselves rather than being part of further theoretical and conceptual debates. Following this discussion, this study will solely examine the role of cyber tools, which are one of the main components of all hybrid-related concepts. This study chose cyber-attacks since cyber-attacks are among the most frequently used instruments in hybrid threats, and "*cyberspace is a key arena for modern hybrid warfare*" (Engström, 2022). In comparison with other hybrid tools, cyber-attacks create more ambiguity and offer more plausible deniability. The "plausible deniability" of the cyber operations allows states both ambiguity and visibility at the same time. Some covert military actions can also offer the same level of plausible deniability; however, as a main distinct point, cyber operations do not cause physical destruction and death directly. If the aim is to inflict physical damage, states have a variety of traditional conventional tools at their disposal, which are more likely to be effective than cyber-attacks.

Also, in the event of a severe attack, regardless of whether the attack is conducted through kinetic or non-kinetic tools, it would seriously undermine plausible deniability, and states would respond strongly. On the other hand, due to limited impact and the importance of secrecy, cyber operations possess unique signalling characteristics (Lonergan & Lonergan, 2022, p. 98). Thus, instead of causing severe harm, cyber-attacks are generally utilised to conduct "influence operations" with the aim of influencing society and creating disruption for political purposes. For these reasons, as North Atlantic Treaty Organization (NATO) Secretary General Jens Stoltenberg stated that "*cyber is extremely important [for] hybrid warfare*" (NATO, 2015).

In this regard, in the second chapter, the focus of this study will be shifted to examining how cyber-tools are utilised by the states. In doing so, instead of individually evaluating all the assumptions and perspectives put forward by scholars, experts, and policymakers, all of them will be classified based on their shared overarching themes regarding the role of cyber tools. Some scholars may raise objections to this categorisation and advocate for an approach centred on examining cyber-attack cases individually. However, categorising like theories allows researchers to decide which facts matter and which do not among numerous possible factors

(Baylis et al., 2014, p.3). Accordingly, in the second chapter, the different roles of cyber tools in interstate relations were discussed based on the assumptions of "*three groups of scholars*".

The first group primarily asserts that cyber tools have changed the nature of war, so cyber technologies have led to a revolution in military affairs. Therefore, the first group emphasises the risk of cyber warfare, which is a substitute for conventional war, and that this war could change the balance of power in international systems. On the contrary, *the second group* argues that cyber tools are limited alone and hardly cause escalation and coercion. Instead, these tools are modern tools of political warfare and become more effective when combined with other traditional tools. Therefore, they argue that "cyber tools are not revolutionary but evolutionary; not substitutive but complementary". Also, some scholars in the second group claim that the reason for using cyber tools, despite their limited impact, is because they are used as conflict management tools between rivals. *The third group* argues that cyber tools are neither substitutive nor complementary but standalone tools. Accordingly, the third group mainly emphasises that the cumulative impact of cyber tools should be considered rather than single cyber-attacks. From this perspective, the third group perceives cyber tools as a changer in the balance of power in the international system as a "short of war". Moreover, some of the scholars in the third group (e.g., Fischerkeller et al., 2022) structuralised most of the assumptions of the third scholars under the *"Cyber Persistence Theory"*, which assumes that all states are in constant contact with each other in the interconnected environment and persistently exploit the vulnerabilities for their political purposes to gain strategic advantage over their rivals.

After examining these three groups, it will be argued in what ways they have remained limited and which additional factors should be taken into consideration to explain the role of cyber tools in interstate relations. In this context, the study will seek to expand the role of cyber-attacks by examining them through the lens of trilateral relations rather than bilateral ones. In the literature, the role of cyber-attacks is generally studied over bilateral relations, especially in case of a crisis. Although this approach is not wrong, it may overlook the fact that states maintain simultaneous conflictual and cooperative relationships with multiple actors at the same time. The relations between states can be conceptualised as complex networks. State interactions,

whether positive or negative, not only impact the involved state but also numerous countries, particularly those in the same region. Consequently, a single positive or negative change in bilateral relations can lead to various outcomes in other bilateral relations. This means that the deterioration or improvement of relations between two countries can impact the relationships of other states, and third parties can become directly or indirectly involved in any incidents between the two countries. Furthermore, due to the plausible deniability of cyber-attacks, states can easily expand beyond the scope of their bilateral relations. Even if an incident does not directly affect third parties, they can turn the crisis into an opportunity to conduct false flag operations and blame other parties involved. Therefore, when conducting case studies or quantitative research on the impact of cyber tools on the relationships between rival states, it is important to consider the role of third countries. These countries may be affected by or may influence the situation, especially if they are strategically important to both rival states.

Moreover, it is generally considered that states carry out cyber-attacks against each other when there is a crisis between them. On the other hand, the rapprochement of the two states may be interpreted by a third actor as a potential threat, leading to retaliatory cyberattacks against both states. Indeed, cyber-attacks – one of the tools that primarily enable states to operate in grey areas– are useful in such situations. This is because when dyadic relations deteriorate, states have various tools (e.g., economic, diplomatic, and military tools). However, in case a rival state improves its relations with a strategically significant country, states have relatively fewer foreign policy tools and options. At that point, cyber disruption operations could be alternative tools for states. Therefore, for states that are reluctant (or unable) to use other tools and want to "do something" rather than "do nothing", cyber-attacks offer strategic utility. In this context, this study will explore the use of cyber tools as an instrument of tacit bargaining, particularly in the form of coercive diplomacy, in trilateral relations. For this inquiry, this research will analyse how states use cyber-attacks when the rival increases its cooperation with a strategically important state in order to influence the rivals' policy choices through behaviour, using the case study of the United Kingdom and its trilateral relations.

To examine how level of state's relations (conflict-cooperation level) affect the likelihood of utilizing cyber-disruption operations as modern foreign policy tools; this study will employ quantitative research methods. Quantitative methodology principally collects data and uses statistical analysis techniques to test related hypotheses or theories (Mertler, 2021, p.107). In chapter three – methodology – the types of data for analysis, the source of these data, collecting and organising techniques of data from these sources and the analysing techniques to test these data will be outlined. In this chapter, it will be firstly discussed which kind of cyberattacks will be used. As will be discussed, there are different kinds of cyber-attacks. Each cyber-attack is executed using distinct methods and employed by various threat actors with varying motivations. Hence, classifying all these activities into the same category and analysing them from the same perspective could lead researchers to inaccurate conclusions. In this context, the study will discuss the reasons why DDoS attack, which is one form of a cyber disruption operation, will be chosen for analysis and in what respects DDoS attacks offer advantages for this study. Secondly, the sources and methods of collecting DDoS attacks will be explained. After the cyber-attack dataset will be prepared, thirdly, the methods of quantitatively analysing the state's dyadic relations will be discussed. In this respect, "Event Data", which is used as both "process" and "specific data type" in the generation of quantitative political data in the Political Science and International Relations disciplines, will be explained.

The event data method – which includes almost all incidents between states – offers to include a significant number of variables related to states and their dyadic relations. For example, instead of listing variables such as war, treaty, military alliance, criticism, condemnation, and diplomatic visit, event data consists of all these events and assigns a score (ranging from -10 to 10) to each event based on the Goldstein Scale (1992). Moreover, which data science techniques are necessary to organise the data prior to analysis will be addressed. Fourthly, the statistical methods (e.g., Binary Logistic Regression and Pearson Correlation Analysis) to be employed in the analysis of the datasets will be elaborated. Lastly, to enhance the detection capacities of the states regarding the second main research question, how to develop an AI-based early warning system to detect politically motivated cyber disruption operations based on the complex dynamic relations of states, will be presented in detail.

Following the methodology chapter, this study will conduct a quantitative analysis to examine the impact of trilateral relations on the use of cyber disruption operations as a foreign policy tool, particularly in the form of modern coercive diplomacy. For this inquiry, as a case study, this research will analyse how cyber disruption operations targeting the United Kingdom between 2014 and 2023 are affected by its trilateral relations with Russia-Ukraine, China-Hong Kong, and Iran-Israel. According to several official UK reports, the UK's primary objective is to "counter state threats", particularly those originating from China (systemic threat), Russia (most acute threat), and Iran (destabilizing threat) (United Kingdom Government, 2021, 2023a). Furthermore, China, Russia, and Iran are identified as the top cyber threat actors for the UK (United Kingdom Government, 2023b). In this context, this study will investigate how cyber disruption operations are utilised by these 'usual suspects' as a foreign policy instrument in response to the UK's increased cooperation with the strategic actors for both the UK and the "usual suspects". For this analysis, Chapter Four will first underline why the United Kingdom and its trilateral relations offer great promise. Secondly, the significance of the United Kingdom as a model country for this analysis and its trilateral relations will be examined from a historical perspective, with a particular focus on the contemporary era of these relations. By offering a historical perspective on these trilateral relations, this study will shed light on the strategic importance of Ukraine, Hong Kong, and Israel in the UK-Russia, UK-China, and UK-Iran relations, respectively.

After emphasising the importance of these relationships, in Chapter 4.4, this study will test whether the increase/decrease in conflict-cooperation scores of each trilateral relationship will have an impact on the increase/decrease in cyber disruption operations against the United Kingdom by Logistic Regression Analysis. By testing whether there is a relationship between trilateral relations and cyber-attacks over a 10-year period, this study will also provide important clues about the long-term use and impact of cyber-attacks. Additionally, to support the quantitative analyses, the key political events in which the UK has been the target of major cyber disruption operations will be reviewed. In this way, it will be explored how usual suspects utilize cyber disruption operations as instruments of tacit bargaining against the United Kingdom, specifically when the UK increases its cooperation with Ukraine, Hong Kong, and Israel—to influence the UK's foreign policies through behaviour.

In order to increase the internal validity of the analysis and provide more information about the role of cyber-attacks, this study will also conduct another analysis -Pearson Correlations– to compare the UK and other European countries (Western and Northern) in terms of being the target of cyber disruption operations. In this direction, an analysis from a broader perspective on the use of cyber-attacks will be provided by comparing which countries have been the target of cyber-attacks in this 10-year period. By identifying the countries that experience similar increases and decreases in cyber threats at similar times, it can be discerned which countries are facing similar threats. This can provide important clues about the potential cyber attackers and dynamics of European security.

After testing the hypotheses and providing significant answers to the first main research question in Chapter 4.5, to enhance the detection capacities of the states regarding the second main research question, this study will also develop an early warning system to detect politically motivated cyber disruption operations based on the complex relations of states. To develop such a system, it is necessary to create a model capable of simultaneously evaluating different bilateral relations of states, identifying patterns within these relations, and determining how these patterns influence the increase or decrease of cyber-attacks. However, evaluating all these variables simultaneously and finding patterns between them is a very challenging task. In this context, the ability to identify and recognise patterns within complex big data and the capacity to make high accuracy/precise predictions based on learning from the training data when a new dataset is introduced; this study will apply artificial intelligence (AI) models in developing an early warning system.

As AI models, supervised machine learning (SML) models offer great promise in developing such a model because they are used in a wide range of tasks across different sectors, from detecting anomalies in networks (Elmrabit et al., 2020; Nawir et al., 2018) to disease diagnosis (Sokoliuk et al., 2020). For a similar purpose, to predict/classify whether there will be cyber operations that exceed the threshold when new conflict-cooperation scores between countries are introduced to the model, this study will develop an early warning system by using different SML algorithms. These models will be trained using the two main datasets: One of the datasets includes the

United Kingdom's bilateral relations (conflict-cooperation score) with 14 different states. The second dataset includes data on whether the frequency and volume of DDoS attacks directed at the United Kingdom simultaneously exceed the threshold (in other words, whether there is a significant cyber disruption operation or not).

After training these different machine learning (ML) models, based on their performance metrics, this study will compare their performance to determine which model is superior in which aspects and which model is the most promising in overall performance. Based on this comparison, this study aims to obtain the best ML model to develop an early warning system for politically motivated cyber disruption operations. Indeed, obtaining the best model is a process of solving a complex mega puzzle. Not only the analysis chapter but all chapters, from discussing the reasons for choosing cyber-attacks to selecting types of cyber-attacks and deciding which countries should be included, are the pieces of this complex puzzle. Each piece needs to be explained and brought together carefully to solve this puzzle. If one piece is missing or the pieces are placed in the wrong place, it is impossible to complete the puzzle. Hence, in the following chapters, from the literature review of hybrid warfare to the theoretical part, from methodology to analysis chapters, all these pieces will be assembled carefully. Once all the pieces are assembled and the puzzle is completed, this study will reach its final goal: Early Warning System. This pioneering model will contribute to improving the resilience of states and societies by enhancing the readiness of public institutions, citizens, and private companies against cyber-attacks. However, even though the development of this model is like solving a mega puzzle, it is important to note that other, more complex puzzles always exist. In other words, despite the significant effort put into developing this model, further research and innovation are still necessary. In this regard, this study will be concluded by providing suggestions for further studies on developing more advanced, comprehensive, and complex early warning systems based on the current model.

1. HYBRID WARFARE: A LITERATURE REVIEW EXAMINING THE WIDENING OF THE GRAY ZONE BY NEW INSTRUMENTS

"The supreme art of war is to subdue your enemies without fighting".

-Sun Tzu

Almost 200 years ago, Prussian general and military strategist Carl von Clausewitz wrote his famous passage: "*War is merely the continuation of politics by other means*" (1976, p. 87). Since then, the political objectives have not changed essentially, but the means of war to reach political goals have broadened, especially with new technologies. Indeed, throughout history, human beings have always been seeking new methods and ways to wage war and to adopt new modes of warfare (Najžer, 2020, p. 1). Hence, as Clausewitz (1976, p. 593) asserted that "*every age had its own kind of war, its own limiting conditions, and its own peculiar preconceptions*. [Therefore] each age has "*its own theory of war*".

In the last two decades, ever-increasing new challenges have made the security environment increasingly complex. As Michael Rühle and Clare Roberts (2021) have pointed out, the era in which peace and war are clearly distinguishable phases, conflicts are largely fought by military means, and adversaries are well known, is over. Thus, the characteristics of contemporary warfare cannot be easily categorized as black or white anymore. Instead, the majority of warfare occurs in a grey zone, which is a domain where it is challenging to distinguish between war and peace due to the ambiguous tactics employed *(Azad et al., 2023, p. 101).* Moreover, war now encompasses a range of different tools and methods, such as cyber-attacks, disinformation campaigns, sabotage, employing special forces, lawfare, terrorism, and irregular warfare. These tools and methods are also used in combination. While a state might use economic and diplomatic tools, at the same time, non-state actors might launch cyber-attacks to target a country's critical infrastructure and conduct disinformation campaigns on social media platforms to destabilize political communities without the need for military intervention (Rühle & Roberts, 2021).

In this context, many strategists/theorists/policymakers have emphasized the emergence of new challenges that have changed the nature of modern warfare. To explain these new phenomena, hybrid warfare is employed as a primary theoretical approach. The new phenomenon – hybrid warfare – involves the integration of various instruments of conflict, including both traditional and non-traditional tactics. In this way, hybrid warfare seeks to exploit the target's vulnerabilities by utilizing all available means for political objectives, integrating tactics that align with one's strategic culture, geographical conditions, and available economic and military tools. Hence, *hybrid warfare is typically used by actors who do not wish to engage in classic overt forms of power politics, but still wish to achieve the goals associated with it* (Najžer, 2020, p. 4).

The increasing diversity of instruments possessed by states and the increasing feasibility of their simultaneous use, combined with the uncertainty associated with the blurring of the line between state and non-state actors, have made hybrid warfare a popular concept. Today, many [especially Western] states have drawn increasing attention to hybrid warfare and developed a counter strategy. Also, international organisations (e.g., NATO, European Union-EU) have given high priority to countering the hybrid threats. Nevertheless, due to widespread usage of the hybrid warfare concept and changing dynamics in the methods, technology and strategies, the hybrid warfare concept lacks a clear definition. The term "hybrid", defined as the "mixture of two very different things" (Cambridge Dictionary, 2024b) has become a catch-all term that defines almost all conflicts. Also, the concept has evolved significantly in scope over time. A comparison of articles from the beginning of the millennium with those from two decades later reveals that there have been major changes in the nature of warfare. From the involvement of non-state actors in warfare to the use of multiple non-kinetic means. Therefore, as Chiara Libiseller stated that "*one cannot use [hybrid warfare] without first having to clarify its history and changes in meaning*" (2023, p. 858).

In this respect, in the following two sections, firstly, how the concept of hybrid warfare has evolved over the last two decades will be discussed. Secondly, since the concept of hybrid warfare has been expanded, similarities and differences between

hybrid warfare and concepts such as hybrid threat and grey zone warfare will be addressed. In this way, it will be examined whether these concepts are distinct or intertwined and can be considered as part of the umbrella term, such as 'hybrid threats'. Following these discussions – with the example of cyber-attacks which are one of the main tools of all hybrid-related concepts – it will be briefly discussed why the role of tools (kinetic or non-kinetic) should be the main focus, rather than debating which tools should be included/excluded in concepts to counter these 'hybrid' threats.

1.1. Defining Hybrid Warfare: Mapping Its Expanding Scope

In the literature, there is no agreed-upon definition of hybrid warfare, and there are differing views as to when and by whom the term was coined. Despite different views, the origin of the concept of hybrid warfare can be traced back to the 1990s with Thomas R. Mockaitis' book entitled British Counterinsurgency in the Post-imperial Era (1995). In his book, Mockaitis (1995, p.14) characterizes the Indonesian confrontation with Malaysia from 1963 to 1966 as a hybrid war. This is because it involved a combination of "low-intensity conventional engagements with insurgency". While conventional forces were involved, Indonesian raiders also participated in the conflict and attacked police forces. Therefore, Mockaitis refers to it as a hybrid war (Mockaitis, 1995, p. 16).

Also, some researchers (e.g. Käihkö, 2021, p. 117) reference Robert G. Walker's master's thesis, named "Spec Fi: The United States Marine Corps and Special Operations", as one of the earliest conceptualisations. In his study, hybrid warfare was used to describe the warfare which "*lies in the interstices between special and conventional warfare"* (R. G. Walker, 1998, pp. 4–5). According to Walker, the hybrid warfare concept is not a new concept (p.5); however, the world has increasingly become uncertain due to hybrid threats (p.99). Despite increasing uncertainty, Walker emphasises the US's reluctance to employ unconventional forces. He argues that this reluctance has been valid throughout American military history, even during the American Revolution. When many historians stated that the United States would have won the American Revolution more quickly with a guerrilla campaign, Americans refrained from applying unconventional warfare. From this perspective, Walker

advocates for the use of hybrid forces and emphasizes their necessity in addressing the threats of an increasingly uncertain world.

As the 21st century approached, historians and theorists attempted to predict the future of warfare, as noted by Walker (1998, p.7). This quest was not confined to the Western security world but was valid throughout the world. The prominent book, *"Unrestricted Warfare"* (1999), by two colonels in the People's Liberation Army (China), Qiao Liang and Wang Xiangsui – has been considered as an early proponent of hybrid warfare, although hybrid warfare was not mentioned in the book. Moreover, the book has also been often regarded as a reference book for understanding China's strategic outlook (Barno & Bensahal, 2016). According to Liang and Xiangsui "*using armed force to compel the enemy to submit to one's will*" is no longer the concept of the new war but "*using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests".*

Nevertheless, the majority of the literature on hybrid warfare in the early 21st century has been produced by military strategists and former soldiers in the United States, despite the worldwide effort to understand and forecast the nature of this new type of warfare. In this respect, one of the earliest studies about hybrid warfare in the US was William J. Nemet, who formulated the concept of hybrid warfare based on the Chechen Insurgency in his master's thesis *'Future War and Chechnya: A Case For Hybrid Warfare*' (2002).

In his study, Nemet established a link between the society's form and its method of waging a war. According to Nemet, modern states are facing challenges by the violence resulting from the devolution of the states, which describes a state's return to a more traditional socio-political organisation. These societies are introducing a diverse combination of modern technology, along with various political and religious beliefs and structures, as they devolve. These societies have adopted primitive war but also employ modern technology and mobilisation methods. In this respect, according to Nemeth, "hybrid warfare is the contemporary form of guerrilla warfare and a continuation of pre-state warfare that has become more effective" (2002, p. 29). In short, Nemet emphasises that understanding the creation of a new warfare paradigm

requires consideration of not only military organisations but also society (2002, p.2). In this case, he formulates hybrid warfare as a way of waging war in hybrid societies, taking the Chechens as an example.

Although the concept of hybrid warfare was initially defined in various ways, it is generally accepted that James N. Mattis and Frank Hoffman presented the concept in their co-authored article titled "*Future Warfare: The Rise of Hybrid Warfare*" (2005). Based on the experience in Iraq and Afghanistan, they argued that although the fundamental nature of war has remained constant, there have been significant evolutionary and revolutionary changes in the way it is conducted (2005, p.18). Mattis and Hoffman highlighted the four types of emerging challenges/threats which were identified in the 2005 Department of Defence's (US) National Defense Strategy (2005, p. 2). These are *traditional*, *irregular*, *catastrophic*, and *disruptive* threats. They focused particularly on the *irregular threats* posed by potential future adversaries and warned that the "*enemy is a human being with the capacity to reason creatively*" and the adversaries of the US do not follow its rules. Instead, its adversaries [both states and non-state actors] "*move out of the traditional mode of war and seek some niche capability or some unexpected combination of technologies and tactics to gain an advantage*" (Mattis & Hoffman, 2005, p. 18). Hence, while the conventional threats still apply, "*the greatest probability is the rise of so-called irregular challengers*" and their "*exploiting of tactical advantages*". In this respect, they define hybrid warfare as follows:

> "*We expect future enemies to look at the four approaches [the traditional, the irregular, the catastrophic, and the disruptive] as a sort of menu and select a combination of techniques or tactics appealing to them. We do not face a range of four separate challengers as much as the combination of novel approaches—a merger of different modes and means of war. This unprecedented synthesis is what we call Hybrid Warfare"* (Mattis & Hoffman, 2005, p.18).

After the publication of this article, Frank Hoffman went on to publish a series of articles. In his article (2006), he again underlined similar themes and emphasised that *"irregular warfare is a natural reaction to globalisation and America's overwhelming military superiority"* (2006, p. 397). He criticises the proponents of Revolution in Military Affairs (RMA) and asserts that the next RMA will be complex irregular warfare that presents a "*mode of warfare that contests America's*

overwhelming conventional military capability" (Hoffman, 2006, p. 411). Therefore, instead of combating with the conventional capability, the US's adversaries will use their own strengths. Moreover, they will have the capacity and capability to conduct "*advanced irregular warfare*" "*with access to encrypted command systems, man-portable air defence missiles (MANPADS), and other modern lethal systems"* (2006, p.398). In this respect, the future will be "asymmetric warfare", and the future wars will be unpredictable and nonlinear operations (2006, p. 398).

In addition to the Afghanistan and Iraq Wars, for Hoffman, the 2006 Lebanon War also played a significant role in the conceptualisation of hybrid warfare. According to Hoffman, the 2006 Lebanon War is the most explicit example of a modern hybrid challenger, with Hezbollah demonstrating a range of "state-like military capabilities" and proving the "ability of non-state actors to deconstruct the vulnerabilities of Western-style militaries" (Hoffman, 2007, pp. 35–36). However, this does not mean hybrid warfare is the only way for non-state actors to wage war. On the contrary, Hoffman points out that "hybrid warfare can be conducted by both state and non-state actors." Additionally, states can also convert their conventional forces into irregular units and adopt new tactics, as was seen with Iraq's Fedayeen in 2003. In this context, Hoffman uses the term "hybrid" to describe both the organisational and instrumental components of war.

Furthermore, Hoffman emphasised that wars throughout history have had both regular and irregular components. While this may lead to criticization of the concept of hybrid warfare as not being new, Hoffman argues that in previous wars, these components were fought in different formations or theatres. The unique aspect of hybrid warfare is that these forces become blurred into the same force in the same battlespace. Moreover, the irregular component of the force is not only used to provoke or extend the cost to the target but is integrated and tactically fused with regular warfare to become operationally decisive (Hoffman, 2007, pp. 28-29). Lastly, Hoffman argues that it will be challenging to classify future wars as either irregular or conventional. For him, the distinction between conventional and irregular forces, combatants and non-combatants, and even the physical/kinetic and virtual dimensions of conflict is becoming increasingly blurred (2007, p. 33). In all these respects, he defined the hybrid warfare as follows:

> *"Hybrid Wars incorporate a range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder. [Hybrid Warfare] can be conducted by separate units, or even by the same unit, or even by the same unit but are generally operationally and tactically directed and coordinated within the main battlespace to achieve synergistic effects"* (2007, p. 29).

Since Hoffman has presented a framework for the concept of hybrid warfare, his definition is widely used in literature to define hybrid warfare. Thus, Hoffman is credited with the coining of the term "hybrid warfare". Since then, hybrid warfare gained popularity, especially in the military strategies in the US. As Ibrahim Muradov (2022, p. 169) pointed out, the term "hybrid" has now become a "*buzzword"* to describe *modern/new wars*.

On the other hand, there have been criticisms of Hoffman's conceptualisation of hybrid warfare. For example, John Jack McCuen argues that the 'West' is facing a new form of warfare, which he also labels as "hybrid warfare". Nevertheless, he contends that there is limited attention given to how to fight in such wars (2008, p. 107). According to McCuen, hybrid warfare is the combination of symmetric and asymmetric war. However, it is a spectrum war with "both physical and conceptual dimensions". By physical, he refers to a "combat against an armed adversary". In terms of conceptual dimensions, he describes a broader struggle, which includes the controlling and supporting of the indigenous population of the combat zone, intervening nations' domestic support and support of the international community (Mccuen, 2008, p. 108). In this way, he extends the conceptualisation of hybrid warfare from just battlefield to other elements -mainly societal aspects and international legitimacy. Indeed, it would not be wrong to assume that the US's failure in Iraq had a significant impact on his conceptualization of the counter-hybrid warfare strategy. It is because he attributes this failure to the lack of support from both the domestic and international community. He believes that the lack of legitimacy surrounding the Iraq War contributed to this outcome. Hence, he considers public support and international approval as crucial elements for winning a hybrid war. In this regard, he asserts that states *"must develop coherent strategies to avoid […] hybrid war and […] if there is no political or military will to fight hybrid war, it is better not fight"* (Mccuen, 2008, p. 113).

As McCuen, Russell W. Glenn (2009, p.3) also criticises only a military-focused approach to hybrid warfare because the "challenge posed is more than a military one". As Hoffman, Glenn also focussed on the 2006 Israel- Hezbollah War; however, he questions whether "hybrid concept is sufficiently original to merit addition to military intellectual discourse and – ultimately – armed forces doctrine as a separate form of warfare." He believes that the success is not only related to power or strategy of the Hezbollah but also the various failure of the Israel such as "shortfalls in leadership", "poor tactics", "over-reliance on air power" and "insufficient preparation". Hence, he assumed that "hybrid warfare may not merit adoption as a doctrinal concept even if it proves sufficiently unique were Hezbollah's success due more to Israel's difficulties than its adversary's performance" (2009, pp. 6-7). Therefore, "from a purely doctrinal perspective, hybrid threats and the methods they [Hezbollah] employ seem at best a subset of irregular warfare" (2009, p. 7). Also, he gave a metaphor of the "mule". In order to understand the evolution of the "mule", it should understand the evolution of horses and donkeys rather than focusing solely on the mules itself. Hence, according to Glenn (2009, p.8), the hybrid warfare concept "should not attain status as part of formal doctrine".

Moreover, Nathan Freier (2009) also criticises the rush to the conceptualisation of hybrid warfare. He argues that any rush of the US Department of Defence (DOD) to define hybrid challenges precisely would cause fundamental issues, which would be a great mistake (2009, p.82). Instead of focusing and giving attention to defining "hybrid warfare", focus should be given to the essence of the problems. It is because "war alone is not the only thing that is hybrid; an array of broader defence issues is hybrid as well" (2009, p.82). Moreover, he emphasises that many of the modern challenges are non-military, and these hybrid challenges cannot be resolved through military force alone. However, he underlines that just because these challenges are non-military, it does not mean that they are necessarily non-violent, aimless, disorganised, or harmless. Instead, they can be severe threats to the national interest that require a strategic response, even if their origins are not military. Hence, he emphasises the application of "innovative military resources" with the "other instruments of national power". (pp. 84-85). By military resource, it does only imply military force; however still, many satisfactory results are gained by the use or threat

of the use of force. In other words, he emphasises the importance of the strategic approach that leverages military resources in a broad, innovative, and coordinated manner, integrating them with other tools of national power to address the complex landscape of modern security threats.

In addition to Freier, Glenn, and Mccuen, other scholars have also either redefined or criticized the concept of hybrid warfare that Hoffman described. In 2009, Hoffman attempted to respond to these criticisms with a series of articles. He stated, "*I don't think [my] definition is vague; quite the opposite. If anything, it's too precise*" (Hoffman, 2009b). However, to clarify his definition of hybrid warfare and address the criticism that it is vague, he compares it to "compound war". This is because he acknowledges that his analysis benefited from Thomas Huber's conceptualization of 'Compound Wars' (2009b), which "*are major wars that have significant regular and irregular components fighting simultaneously under a unified direction*" (2009a, p. 36). Compound Warfare has an advantage thanks to its ability to exploit each force and combine them. In contrast, hybrid wars encompass more than just conflicts between states and other armed groups or the combination of regular and irregular forces. Hybrid threats encompass a wide range of warfare modes, including conventional capabilities, irregular tactics and formations, terrorist acts and criminal disorder. According to Hoffman (2009a, p. 36) "*these multi-modal activities can be conducted by separate units, or even by the same unit, but are generally operationally and tactically directed and coordinated within the main battlespace to achieve synergistic effects in the physical and psychological dimensions of conflict*". In essence, for Hoffman, hybrid warfare is distinct from previous wars as it combines regular and irregular components of war, resulting in complexity, fusion, and simultaneity. However, Hoffman's comparison of hybrid warfare with compound warfare was directly criticised by Thomas Huber himself due to mischaracterising and trivialising it. Moreover, Huber criticises the hybrid war since it is not historically new and it is just insurgency (Fleming, 2011, p. 15).

While the conceptual debate has continued in a narrow military strategist environment, the significant Distributed Denial of Service attacks (DDoS) on Estonia in 2007 and the usage of unconventional tools such as cyber-attacks, disinformation campaigns, diplomatic efforts and supporting proxies alongside the conventional war

in the Russo-Georgian War in 2008, the concept has started to discuss in various platforms. Especially following the Georgia-Russian War in 2008 (Goodson & Żakowska, 2023; Seskuria, 2021)- it was widely accepted that Russia's military intervention was aimed at preventing NATO from expanding into the near abroad of the Russian periphery (Nilsson, 2021, p. 56)- the concept of hybrid warfare began to be discussed in NATO and its member countries, and it was incorporated into their lexicon during this period. For instance, in the *US The Quadrennial Defense Review Report* (2010)[1] – that is the main public document of the Department of Defense that describes its strategic objectives and potential military threats – the hybrid term was used to capture "increased complexity of war, the multiplicity of actors involved, and the blurring between traditional categories of conflict (2010, p.8) and asserted that US's adversaries are using "a hybrid mix of approaches and capabilities" (p.15). Moreover, the US Government Accountability Office's (GAO) report on Hybrid Warfare, it is defined as blending "conventional and irregular warfare approaches across the full spectrum of conflict" (2010, p.16). Despite this definition, it was emphasised that the DOD "has not formally defined hybrid warfare and does not plan to do so because DOD does not consider it a new form of warfare (2010, p. 14).

Apart from the United States, The United Kingdom (UK) has also adopted the idea of hybrid threats. In the UK Ministry of Defence Future Character of Conflict Report (FCOC) (2010) it was stated that "future conflicts will increasingly be hybrid in character" due to a "shift in the mindset of [UK's] adversaries who aim to exploit [UK's] weaknesses by using a variety of high-end and low-end asymmetric techniques" (2010, p. 1). The report also underlined that these conflicts go beyond our conventional understanding of what constitutes irregular and regular military activities. In other words, the report accepted the change of "conflict paradigm" and urged a change of defence approaches as well.

Although there had been growing interest in academia, think tanks, and among policymakers, it was still primarily of interest to military experts and strategists. Also, it had been challenging to find a definition that had met the common ground. Nonetheless, the early definitions of hybrid warfare were primarily based on Frank Hoffman's description, which blurred lines of different modes of warfare, including

[1] Following the year 2018, the document was replaced by a "National Defense Strategy".

conventional capabilities, irregular tactics and formations, terror acts, and criminality. In other words, hybrid warfare was used to describe warfare that is neither completely conventional nor unconventional (Solmaz, 2022a, p. 92).

However, Russia's annexation of Crimea and interference in Eastern Ukraine in 2014 had a significant impact on both the popularity and content of hybrid warfare. The Russian campaign has been seen as a new kind of war, and it has been considered a prototype of hybrid warfare, especially among Western scholars/experts/policymakers (Rumer, 2019). Moreover, Chief of the General Staff of the Russian Armed Forces Valery Gerasimov's article published in the Russian newspaper Military-Industrial Courier in 2013 has been regarded as a doctrine of the Russian approach to war. Many associate the Gerasimov Doctrine with Russia's modern warfare approach (Mckew, 2020). In the article, Gerasimov stated:

> "*In the twenty-first century, we have seen a tendency toward blurring the lines between the states of war and peace. Wars are no longer declared and, having begun, proceed according to an unfamiliar template […] The very "rules of war" have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness* […] T*he focus of applied methods of conflict has altered in the direction of the broad use of political, economic, informational, humanitarian, and other nonmilitary measures—applied in coordination with the protest potential of the population*" (Gerasimov, 2016, p.24).

Furthermore, the subsequent Russian actions, such as disinformation campaigns by using social media platforms to create and escalate social divisions in countries perceived to be against Russia and interfering in elections, further strengthened the belief that the Gerasimov doctrine is a main driver of Russian foreign policy (Rumer, 2019). However, some criticize that the Gerasimov Doctrine is not a novel doctrine but a continuation of the Soviet and post-Soviet strategies. For instance, according to Eugene Rumer (2019, p. 4) the so-called Gerasimov Doctrine is hardly a driver of Russian national security policy and not a new concept but a continuation of a doctrine that has guided Russian foreign and defence policies for over two decades: the Primakov doctrine that named after the former foreign and prime minister of Russian Federation, Yevgeny Primakov. The Primakov doctrine proposes that a unipolar world under the dominance of the United States is unacceptable for Russia. To constrain the dominance of the US, Russia should pursue a multipolar world led by a concert of

major powers and compete with the US not alone but with the collaboration of other major powers, China and India (Rumer, 2019, p. 4).

On the other hand, there is also criticism that the Gerasimov Doctrine does not accurately reflect the Russian approach to warfare, but rather represents Russian military impressions of US approaches (Kofman et al., 2021, p. 27). For instance, James K. Wither (2023, p. 12) argues that "*from Gerasimov's perspective, contemporary hybrid warfare (Gibridnaya Voyna) was not invented in Russia*" Instead, Gerasimov viewed it as a Western strategy to destabilise states like Russia which hinder US supremacy. Hence, the involvement of the US in the events in the Middle East during the Arab Spring, and in the Russian sphere during events such as the "Color Revolutions" has been viewed as a hybrid form of warfare used to advance American interests (Wither, 2023, pp. 12–13; Kofman et al., 2021, p. 27). Therefore, in essence, Gerasimov was in search of a solution to the West's "Comprehensive Approach" against Russia rather than defining the new Russian approach to war (Johnson, 2018, p. 142).

Moreover, Bettina Renz (2016, p. 295) argues that the main reason for labelling Russian activities in Crimea as a hybrid is because of the usage of both military and non-military approaches. However, according to Renz, although the espionage disinformation operations psychological are significant non-military factors in reaching objectives, "Crimea was not 'won' by non-military means alone". Despite very limited direct combat took place in Crimea, Russia also applied its special forces and military personnel to achieve its objectives. In addition, Samuel Charap (2015, pp. 54–55) also asserts that even given limited objectives and a very permissive environment, Russia would not have succeeded in using hybrid tactics alone. In 2014, Russian-backed separatists were on the verge of defeat, although Russian forces were just across the border, special forces support, cyber operations, and disinformation campaigns. Hence, in a very old-fashioned, non-hybrid way, the Russian military intervened (pp. 54-55). Therefore, Charap puts forward that claiming Russia is conducting hybrid war is a "dangerous misuse of the word war" which leads to drawing wrong lessons (Charap, 2015, p. 52).

Despite these criticisms, following Russia's annexation of Crimea, the term "hybrid warfare" has expanded from a military concept to a widely used term to describe Russian foreign policy, particularly among Western academics, security experts and policymakers (Renz, 2016, p. 293). Thereafter, Hoffman's military-centric concept of hybrid warfare, previously confined to military circles in the US, has gained widespread recognition (Caliskan & Liégeois, 2021, p. 297). For instance, in 2014, General Phil Breedlove, NATO's supreme allied commander, argued that Russia's approach to war is hybrid, using all available tools to cause instability in other nations:

> *"What we see in Russia now, in this hybrid approach to war, is to use all the tools they have […] use their energy tools, use their finance tools, use what I think is probably the most amazing information warfare, […] using all these tools to stir up problems that they can then begin to exploit with their military tool – through coercion […] or through […] regular and irregular forces, these little green men without badges"* (Munich Security Conference, 2015, p.34).

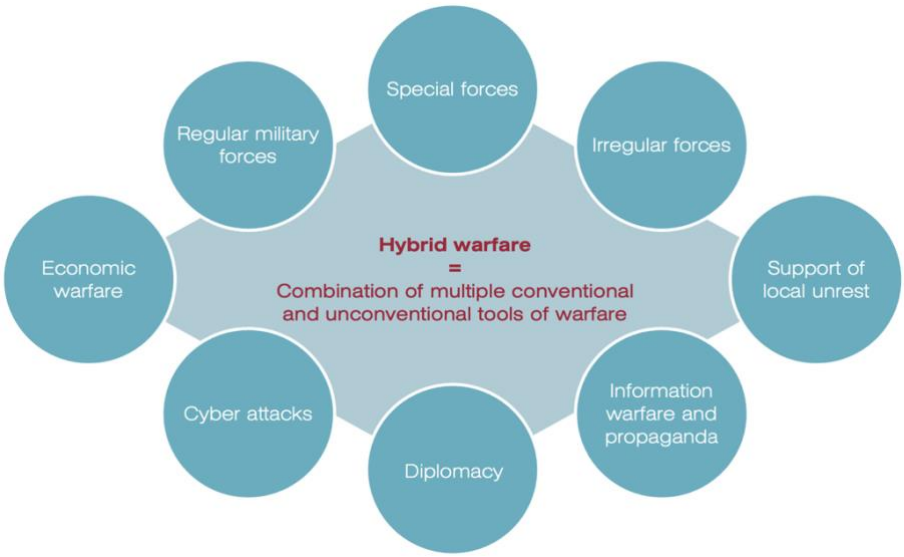

Figure 1. 1 Hybrid Warfare and Its Components

Source: (Munich Security Conference, 2015, p. 35)

Also, due to the widespread acceptance of hybrid warfare as a Russian tactic, Western states and organizations have started to describe hybrid warfare officially and devoted significant attention to developing counter-hybrid warfare strategies. For instance, at NATO's Wales Summit in 2014, NATO gave special attention to hybrid warfare threats, which are defined as "*a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design*" (NATO, 2014). In this respect, in the summit, to respond swiftly and firmly to new

security challenges, NATO also approved the "*Readiness Action Plan*", which is a "comprehensive package of assurance and adaptation measures" (NATO, n.d.-b). Thereafter, NATO officially defined the hybrid threats as combining *"military and non-military as well as covert and overt means, including disinformation, cyber-attacks, economic pressure, deployment of irregular armed groups and use of regular forces […] to blur the lines between war and peace and attempt to sow doubt in the minds of target populations* (NATO, n.d.-a).

In parallel to NATO, the European Union also defines the hybrid threats as follows: "*Mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare*" (European Commission, 2016). Also, hybrid tools are represented as a tool of authoritarian regimes to undermine the democratic values so as to "*polarise societies by using hybrid activities such as information manipulation, cyber-attacks, lawfare, economic coercion, or the instrumentalization of migrants*" (European Commission, 2022).

Moreover, against the criticism that there is nothing new about the usage of the combination of these tools and remaining below the threshold - breach of article Five in the case of NATO (Johnson, 2018, p. 142) - NATO also stresses that what is new about hybrid warfare as follows:

> *Hybrid methods of warfare – such as propaganda, deception, sabotage and other non-military tactics – have long been used to destabilise adversaries. What is new about attacks seen in recent years is their "speed", "scale" and "intensity", facilitated by rapid technological change and global interconnectivity* (NATO, n.d.-a).

With these three features -*speed, scale and intensity*- that are the result of increased interconnectivity and rapid technological change, hybrid usage of kinetic and non-kinetic tools creates an ambiguity which complicates the decision-making process. Ambiguity is a fundamental component of hybrid warfare because threat actors seek to blur the usual and explicit lines of international politics, international and external, illegal and legal, and war and peace (Hybrid CoE, n.d.). Threat actors use

multiple synchronised tools to create ambiguity, including cyber-attacks, disinformation campaigns, economic tools, criminal activities, and kinetic means. These tools are used by various actors (mostly by proxy actors/state-sponsored actors) at different times and intensities, making it difficult to attribute actions explicitly and for what purpose. In other words, activities that fall below the threshold make it difficult to attribute hybrid actors. Hence, hybrid warfare provides actors with a level of deniability, even in circumstances in which it would be obvious who the hybrid actor is (Najžer, 2020, p. 35). For instance, Heidi Reisinger and Alexandr Golts (2014, p. 6) emphasized that despite increasing evidence that proves Russian involvement in the fighting in Eastern Ukraine, Russia persistently denied its involvement with "strange explanations":

> *"In the beginning, one explanation was that Russian soldiers turned up in Eastern Ukraine by mistake. When a group of Russian paratroopers was arrested close to the Ukrainian city of Mariupol, the Russian news stated that "they patrolled the border and got lost." After the battle for Donetsk Airport on 26 May,25, with the first reports of Russian casualties and burials of paratroopers, the official narrative changed. Reportedly Russian servicemen were now "volunteers" following their convictions to fight for freedom." (Reisinger & Golts, 2014, p. 6)*

As the Russian case indicates, ambiguity makes it complicated to respond properly to Russian activities. As Tarık Solmaz asserts, Russia did not only combine conventional and unconventional tools but also deception and covert activities (Solmaz, 2022b). To achieve its political objectives without direct confrontation, Russia attempted to remain below the threshold of conventional warfare by creating ambiguity and enabling plausible deniability. Therefore, Andrew Mumford and Pascal Carlucci assert that the ambiguity of hybrid warfare in Ukraine has enabled Russia to achieve a political and military outcome that otherwise might have been costly and ineffective (2023, p. 205). By this account, they underline that hybrid warfare is a fight in the current international system because ambiguity makes hybrid warfare unique. Without ambiguity, hybrid warfare would be just a form of irregular warfare such as insurgency or terrorism (Mumford & Carlucci, 2023, pp. 198-199).

Furthermore, the fact that challenging the development of policy and strategic development due to ambiguity and plausible deniability renders hybrid warfare resilient to counter-strategies (Bilal, 2021; Mumford & Carlucci, 2023, p. 205).

Targeted countries may encounter difficulties in detecting hybrid threats and attributing them, particularly when the threat is low-level and sponsored actors persistently deny involvement. Therefore, while hybrid threats are already difficult to detect and attribute, deterring and responding to hybrid threats properly is even more challenging. For instance, a state's military capacity can be enough to deter conventional strikes. However, alone against the hybrid threats that remain sub-level of conventional war is rather difficult. This applies not only to the states but also to the organizations. In this respect, NATO and the European Union have identified countering hybrid threats as a priority for cooperation (Hybrid CoE, n.d.-a) and in 2017, after the signing of the memorandum of understanding between NATO and the EU, *The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) was established in* Finland. It is an "autonomous, network-based international organization countering hybrid threats" (Hybrid CoE, n.d.-b).

In addition, in the reports of the Multinational Capability Development Campaign's (MCDC) Countering Hybrid Warfare (CHW) project, it was argued that to develop any counter-strategy, firstly, conceptual confusion about hybrid warfare should be cleared up. In this regard, as Patrick J. Cullen and Erik Reichborn-Kjennerud stated that "*The international consensus on 'hybrid warfare' is clear: no one understands it, but everyone, including NATO and the European Union, agrees it is a problem"* (Cullen & Reichborn-Kjennerud, 2017, p.3). Therefore, they aim to clarify the conceptual confusion of hybrid warfare by introducing a uniform definition of the concept. In this regard, they define hybrid warfare as :

> "*Synchronised use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects*" (Cullen & Reichborn-Kjennerud, 2017, p. 8).

In this definition, instead of referring to the methods/techniques/ways of hybrid warfare, they prefer to use the term "*instruments of the power*." Any power instrument can be regarded as a part of hybrid warfare. In this way, instead of underlining the combination of different kinds of instruments of power, they define hybrid warfare as employing different instruments of power on both horizontal and vertical axes, "with varying degrees of emphasis on creativity, ambiguity and the cognitive elements of war." While horizontal means that there are varying numbers of power instruments that can be used to create "effects greater than through vertical escalation alone"; a

vertical increase means an increasing degree of usage of these power instruments. In this context, the degree and number of power instruments employed in hybrid warfare are tailored to the political motivations of the attacker and the vulnerabilities of the target state (Cullen & Reichborn-Kjennerud, 2017, p. 9).

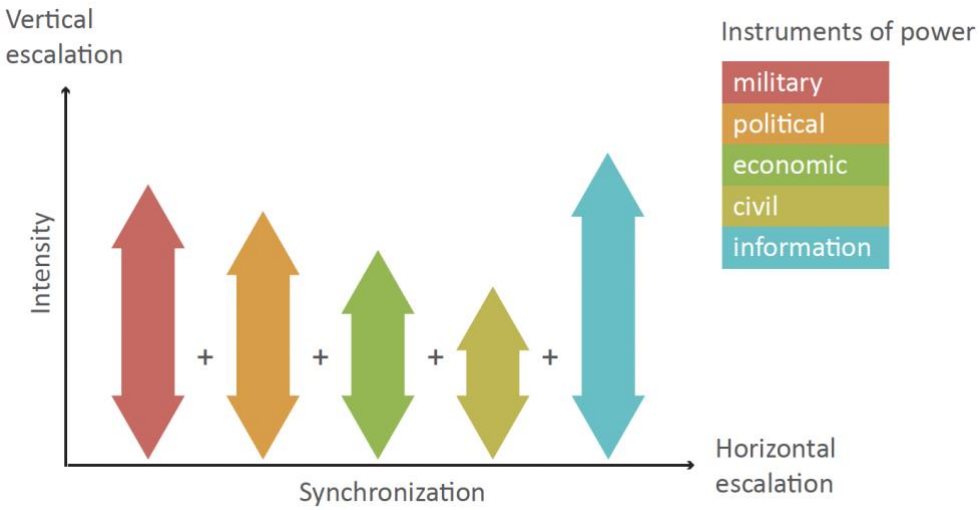

Figure 1. 2 Horizontal and Vertical Escalation of Power Instruments

Source: (Cullen & Reichborn-Kjennerud, 2017, p. 9)

In parallel, Brin Najžer (2020, p. 31) also argues that "*hybrid warfare is a method of combining as many, or as few, of the tools of coercion as is required [therefore] "there is no fixed set of components for hybrid warfare because it is context specific*" [which] differentiates it from other forms of warfare. However, he also stressed that although there are no fixed tools, to say it is hybrid warfare, it is required to blend of conventional and unconventional tools, as shown in Figure 1.3 below (Najžer, 2020, p. 31).

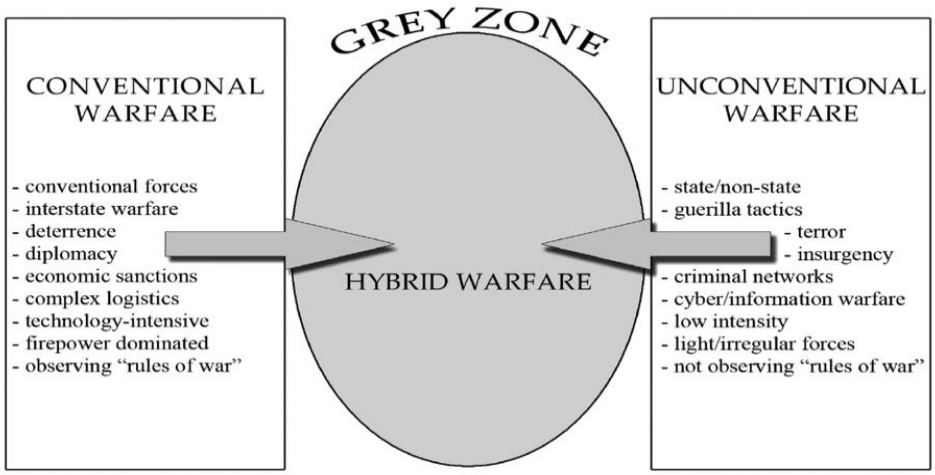

Figure 1. 3: Hybrid Warfare as Combination of Conventional and Unconventional Warfare

Source: (Najžer, 2020, p. 31)

Despite Najžer's emphasis on conventional tools in hybrid warfare, in the literature, there has been an increasing emphasis on the non-conventional tools of hybrid warfare. After the Russian intervention in Ukraine in 2014, non-kinetic tools became the main components of hybrid warfare. In other words, rather than the combination of regular and irregular warfare, hybrid warfare has started to be used to refer to non-military activities such as lawfare, economic coercion, cyber-attacks, disinformation campaigns and sabotages. In this regard, Tarık Solmaz (2022b) argues that this usage of hybrid warfare "*represents an extreme departure from the original approach*".

Indeed, one of the most important reasons for this trend is the increasing emphasis on the non-kinetic elements of this concept by NATO, which is one of the pioneers of the concept of hybrid warfare and one of the key actors in keeping it on the strategic agenda. As James Wither argues, the strategic thinking of NATO evolved from a blend of irregular and regular forms of warfare to a more comprehensive conception that embraces non-military challenges (2023, p.14). For example, based on in-depth interviews with NATO officials, Murat Çalışkan and Michel Liégeois found that almost all NATO officials consider hybrid warfare as synchronised and cautious use of all non-conventional tools to carry out activities that fall under the threshold of Article 5 of the United Nations (UN) Charter (Caliskan & Liégeois, 2021, p. 299). Also, an official at NATO describes hybrid warfare as

"everything else than military, below the threshold of war" to "achieve […] military objective, but ultimately political objective" (Caliskan & Liégeois, 2021, p. 299). Moreover, when asked to define hybrid warfare, Teija Tiilikainen, who is the European Centre of Excellence for Countering Hybrid Threats- answered as:

> "*It is about manipulation of the information space. It's about attacks on critical infrastructure. […] It is an ambiguous threat format […] The key distinguishing features of hybrid threats are that they almost never involve an actual "kinetic" attack - someone opening fire with a weapon"* (Gardner, 2023).

Moreover, in NATO's most recent Strategic Concept (2022) - which officially outlines NATO's roles, purposes and values - hybrid warfare is not even mentioned, but hybrid threats, hybrid challenges and hybrid means are. In this context, non-kinetic activities were generally underlined as malign activities in the Concept Report (NATO, 2022, p.3). Similarly, on the NATO websites, there is no description of hybrid warfare but only of hybrid threats (NATO, n.d.-a). In parallel to NATO, The European Union also prefers to use the term "hybrid threats" rather than "hybrid warfare" and develop strategies against hybrid threats (European Commission, 2016). Finally, the name of the organisation that was jointly established by NATO and the EU was even named *The European Centre of Excellence for Countering Hybrid Threats*. In this regard, it can be argued that NATO, European analysts, and policy documents in the West generally prefer to use hybrid threats rather than hybrid warfare, although hybrid threat and hybrid warfare terms are used interchangeably.

On the other hand, some studies claim that these two concepts are different, even though they are used interchangeably. For example, according to Sean Monaghan (2019, p. 3), while hybrid threats and hybrid warfare have the same basic cause, which is revisionist states' strategies to offset the conventional power of the status quo states, hybrid threats and hybrid warfare describe distinct challenges from each other. In this respect, he underlines the distinction between the two concepts as follows:

> *Hybrid threats combine a wide range of non-violent means to target vulnerabilities across the whole of society to undermine the functioning, unity, or will of their while […] avoiding reprisal through exploiting the 'gray zone' between peace and war.*

> *Hybrid warfare is the challenge presented by the increasing complexity of armed conflict, where adversaries may combine types of warfare plus non-military means to neutralise conventional military power. [Hence it represents] changes in the character of warfare against violent adversaries during armed conflict (Sean Monaghan, 2019, p. 3,8)*

Moreover, while hybrid warfare and hybrid threats are different challenges, this does not mean that they cannot be conducted simultaneously by the same actors. Actors can wage both types of challenges at the same time (Sean Monaghan, 2019, p. 3-8). In this respect, he considers the hybrid threat and hybrid warfare through the "*continuum of the war*" perspective, as shown below in Figure 1.4. According to the continuum of war, hybrid threats are the least intense and have a higher degree of occurrence, while hybrid warfare is less probable and includes a wider range of tools and tactics. In this context, Monaghan views the continuum of war as a process that moves from hybrid threat to hybrid warfare to conventional warfare as states increasingly use conventional means. In addition, he defines the "grey zone" as the area between war and peace, which is considered a stage of conflict that includes non-kinetic tools and limited conflict that falls between war and peace, and which is not expected to provoke a response.

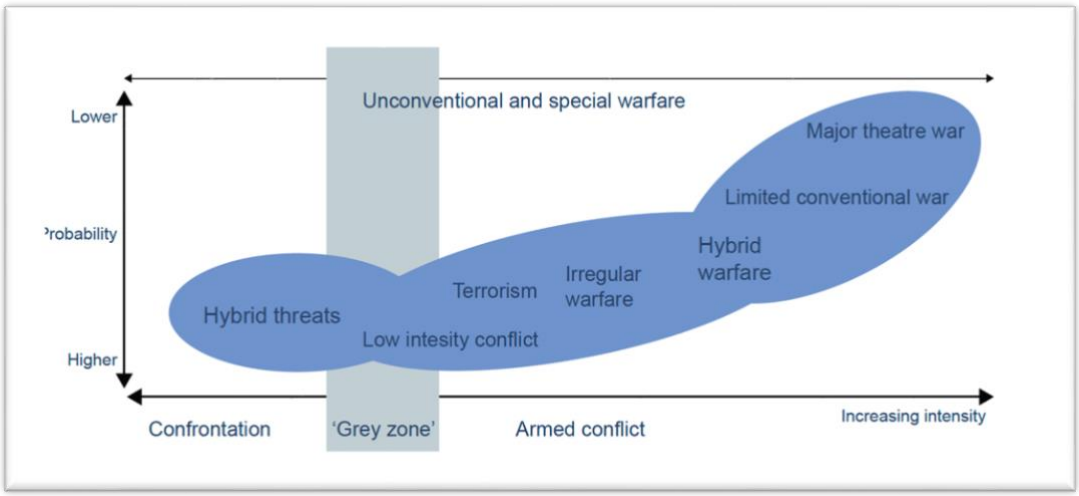

Figure 1. 4: Hybrid Threats and Hybrid Warfare Shown on a "Continium of Conflict"

Source: (Monaghan, 2019, p. 4)

In parallel to Sean Monaghan, Elisabeth Braw (2022, p. 9) and Frank Hoffman (2018, p. 39) have also made a similar differentiation between hybrid warfare and hybrid threat based on the usage of the kinetic and non-kinetic tools. Nevertheless, the two concepts are often used interchangeably. As a result, there has been a growing conceptual criticism against hybrid warfare/hybrid threat, as it has increasingly emphasised non-kinetic tools rather than being seen as a combination of conventional and non-conventional means. In this respect, it is first criticised as being a catch-all concept (Jordán, 2017). According to Colin Gray (2012, p. 41), when one asks, "*What are we talking about?*" for hybrid warfare, the answer is "*potentially everything*" [hence the concept is] "*too inclusive to be analytically useful*".

Also, Michael Kofman (2016) criticizes "hybrid warfare" for covering to describe all activities. Hence, by referring to Frederick the Great, who once said, "who defends everything defends nothing", Kofman argues that we are spending too much time chasing hybrid ghosts. In parallel, Damien Van Puyvelde (2015) also asserts that "*any threat can be hybrid as long as it is not limited to a single form and dimension of warfare*" [therefore hybrid warfare term] "*loses its value and causes confusion instead of clarifying the reality of modern warfare*." In addition, Chiara Libiseller put forward that as the studies about hybrid warfare increase, instead of becoming clear, the concept's "vagueness and ambiguity" increase (Libiseller, 2023, p. 870).

Because of this conceptual ambiguity, secondly, there is a criticism that hybrid warfare is used to refer to different concepts. For instance, according to findings from the content analysis of media items, Murat Çalışkan and Paul-Alexander Cramers (2018, p.12) demonstrated that hybrid warfare in media used 70% of the time for different concepts such as information warfare, political warfare and unconventional warfare. Moreover, Murat Çalışkan and Michel Liégeois argues that NATO officials indeed describe hybrid warfare in line with the "political warfare" because "they emphasise the non-military and non-lethal elements":

> *Most officials defined the concept in line with present NATO's definition [however] further discussions revealed that they often really mean 'political warfare' – or grey zone warfare when they say, 'hybrid warfare' (Caliskan & Liégeois, 2021, p.299,307).*

Indeed, Caliskan and Liégeois' criticism of the use of hybrid warfare instead of the grey zone warfare/political warfare concepts has been voiced by many researchers in recent years (e.g. Azad et al., 2023; Mazarr, 2015). In particular, after China's activities in the East China Sea and its cyber activities against Western countries, the use of the concept of grey zone warfare/conflict to define China's activities comes to the fore because it only contains non-kinetic tools. Therefore, while hybrid warfare is used to define Russia's actions, it is suggested that the grey zone is a more accurate approach to define China's behaviour, which does not involve kinetic tools (Akgül, 2021). In line with these discussions, there has been a growing body of research that suggests that hybrid warfare is different from grey zone warfare/conflict and that the two concepts should not be used interchangeably because they imply different phenomena. To ensure clarity in the use of these terms and to prevent further confusion in the following chapters, particularly regarding cyber-attacks, the next section will examine grey zone warfare/conflict and will elaborate on the differences and similarities between hybrid warfare and grey zone warfare.

1.2. Comparing Blurred Concepts: Hybrid Warfare and Grey Zone Warfare in the Age of Non-Kinetic Tools

In recent years, with increasing real and virtual connectivity through the wider use of information and communication technologies and growing economic dependency, the use of multiple tools in a synchronized way has become more effective. While the combination of the tools and methods in the early millennium have been battlefield-oriented conventional and unconventional tools, in the latest years, states have generally adopted non-kinetic tools and limitedly conventional methods. The ongoing war (2024) between Russia and Ukraine that started in 2022 can be given as an example of the opposite direction; however, it is constrained in Ukraine, and it has not yet spread beyond Ukraine's borders. In other words, it has remained confined to Ukraine's territory (particularly in the eastern part of the country), and the challenge between Russia and Western countries continues mostly through the use of non-kinetic

tools. While economic sanctions are the Western states' main tools against Russia; Russia applied variety of tools from cyber-attacks to disinformation campaigns, from exploiting gas leverage to acts of sabotage (Wither, 2023, p. 24). In this regard, while hybrid warfare has been coined the term the blend of irregular and regular warfare and battlefield-oriented concept, today, the concept has been used to refer to "non-violent disruptive actions" (Solmaz, 2022a, pp. 92–95).

This "*conceptual stretching*" led to the use of many different concepts interchangeably with hybrid warfare/threat. As Sean Monaghan highlights that in the media, policy papers and academic literature, hybrid warfare/threats are often conflated with the terms 'grey zone warfare' and political warfare (2019, p.1). As a result, studies that consider China's activities against US hegemony as similar to the Soviet struggle against the US during the Cold War and characterise them as political warfare or grey zone warfare have gained considerable prominence. This chapter will examine the grey zone warfare/conflict and underline the differences between the hybrid warfare/threat and gray zone conflict/warfare concepts. These different approaches will be addressed through the Theodore Jensen's classification of the three camps which are "*the New Era camp*", "*Hybrid Warfare camp*", and "*Nothing New camp*" (2019, p. 12). Thereafter, the roles of the cyber-attacks which are considered as one of the prominent instruments in both concepts will be elaborated.

According to the Cambridge Dictionary (2024), Gray Zone has two definitions: Firstly, it is defined as "*activities by a state that are harmful to another state and are sometimes considered to be acts of war, but are not legally acts of war*". Secondly, "*a situation in which it is not clear whether something is legal or illegal, acceptable or not acceptable*". In both definitions, the grey zone is used to describe the activity/situation in which it cannot be assigned to one of the parties of duality, such as illegal/legal. In parallel to general definition, in the security literature, the grey zone is mainly used to describe the undefined conflict [that] in does not fit into identified parameters of either war or peace (Jensen, 2019, p. 6). For instance, in the US Department of Defence's Quadrennial Defense Review in 2010 -that was one of the earliest examples in which the grey zone concept was used- the grey zone is used as the following quote indicates:

> *"Threats to our security in the decades to come are more likely to emanate from state weakness than from state strength. The future strategic landscape will increasingly feature challenges in the" ambiguous gray area" that is neither fully war nor fully peace"* (US Department of Defence, 2010, p. 73).

Also, according to Center for Strategic & International Studies' Gray Zone Project (n.d.), grey zone is described as follows :

> *"From fake news and online troll farms to terrorist financing and paramilitary provocations, these approaches often lie in the contested arena somewhere between routine statecraft and open warfare—the "gray zone."*

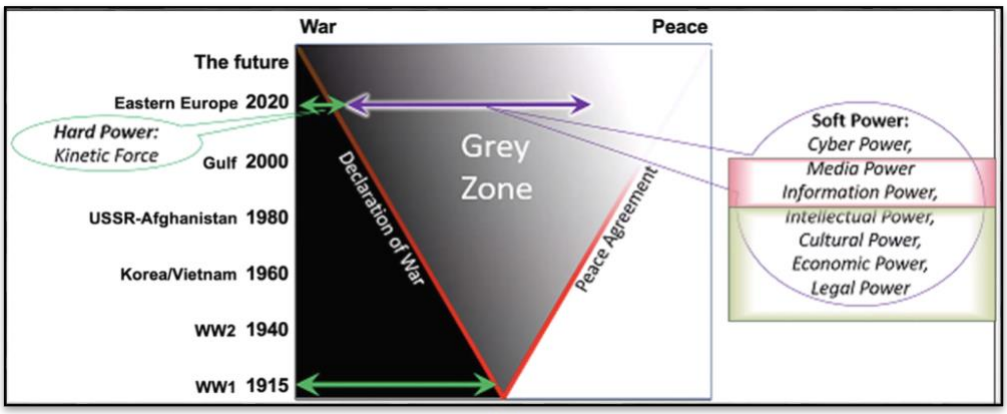

Figure 1. 5: Expanding of Grey Zone Since 1915

Source: (Davies, 2023)

The prevailing view in the literature is that the grey zone will expand much more in the future due to the increasing diversification of tools and their hybrid usage. Nevertheless, there is no consensus on whether gray zone conflict is a new concept or not, and whether hybrid warfare and the grey zone are the same or distinct concepts. While some argue that grey zone conflict and hybrid warfare are distinct concepts, some studies use them interchangeably. In this respect, so as to clarify these different approaches and to classify different views concerning gray zone, Theodore Jensen (2019, p. 12) proposes three camps.

According to Jensen, "*New Era Camp"* asserts that although the tools are not new, gray zone conflict is a distinct concept because it is the natural extension of "geopolitical shifts [in] international environments" (2019, p. 18). As Hal Brands argues (2016, p. 4) the changing international realms are the driving force of these new

challenges. Hence, the New Era Camp argues that previous concepts are indeed the product of the Cold War, which is the extension of the two-power competition. On the contrary, grey zone warfare is the product of the post-Cold War period. Based on this perspective, it can be assumed that the concept of "political warfare" coined by George Kennan to describe the US Foreign Policy against the Soviet Union, which is often used interchangeably with the term "grey zone" and considered as "the doctrinal roots of grey zone" (Akgül, 2021, p. 416); does not also accurately fit the definition of the grey zone. According to Kennan:

> *"Political warfare is the logical application of Clausewitz's doctrine in time of peace. In broadest definition, political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures (the Marshall Plan) […] to such covert operations as clandestine support of "friendly" foreign elements [and] psychological warfare* (Kennan, 1948).

Kennan's description of political warfare indeed has certain similarities not only with grey zone conflict but also with hybrid threats. However, according to one of the prominent names for the grey zone conflict, RAND political scientist Michael Mazarr, argued that a combination of the three elements – a) *rising revisionist intent*, b) *a form of strategic gradualism*, and c) *unconventional tools*, create a new form of conflict (2015, p. 4).

Firstly, Mazarr claims that revisionist powers' ambition against the status quo power is the root cause of grey zone conflicts. Based on Randall Schweller's definition of a different degree variety of revisionism, Mazarr argues that the main engine of the grey zone conflict is the "measured revisionist" powers (2015, p. 10). For these powers, there is need to open an paranthesis. By introducing the Balance of Interest Theory, in which alliances are analysed in terms of interests and profit rather than security or threat, Randall Schweller (1994, pp. 101–104) brought back the revisionist states ignored by Neorealist Theory (Tür & Salik, 2017, p. 17) and distinguishes four types of states: "*Lions*" (Status-quo powers of the first rank); *"Lambs"* (Weak status quo states); "*Jackal*" (States that value their possessions but also tend to be risk-averse and opportunistic) and "*Wolves*" (States that value what they covet far more than what they possess therefore they are willing to take great risk).

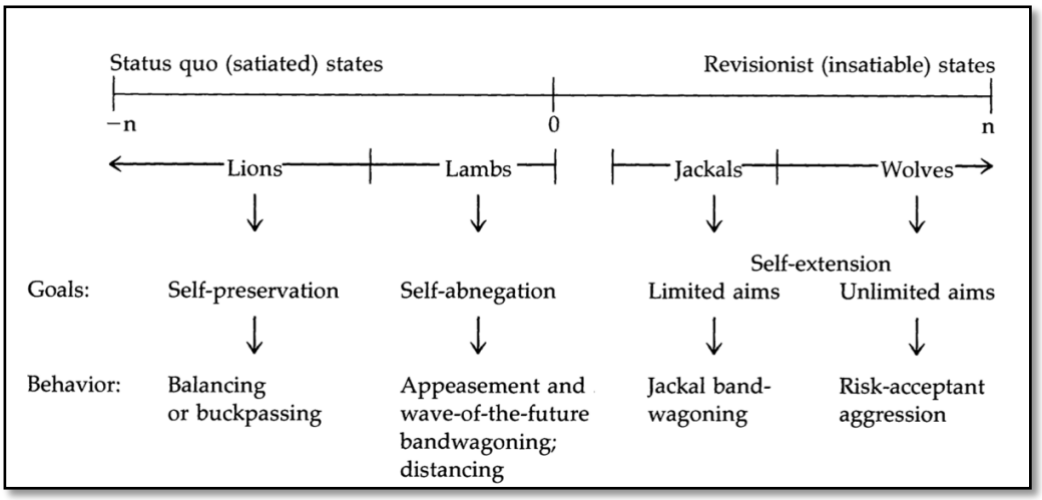

Figure 1. 6: Randall Schweller's Formulation of Four Types of Revisionist States

Source: (Schweller, 1994, p. 100)

Although Mazarr considers Schweller's analogy as suggestive, he asserted that this list needs to be extended with at least one additional category because the main antagonist to the current system (China, Russia and Iran) can be categorised as neither Wolf nor Jackal (2015, p. 17). It is because these states are partly satisfied with the current system, but they are determined to acquire a greater degree of control within it. They are more insistent and calculative in pushing their agenda than the more opportunistic jackals but will not come close to the wolves in their self-destructive drive for power. They pursue long-term campaigns and avoid jeopardising the entire system with sudden changes.

In this regard, Mazarr added a new category to Schweller's analogy to represent current China, Russia and Iran as "measured revisionist" as seen in the following Table 1.1 (2015, p. 18). These states are too dissatisfied to do anything; but on the other hand, they are too interdependent, which makes them accountable in case they engage in conventional military actions. They also benefit from this system but are not satisfied with the existing system. In this respect, they aim to shift the distribution of power in the international system, as well as international rules and norms, without going to war by using non-conventional tools below the threshold of war (Mazarr, 2015, p. 28). In other words, they turning to grey zone strategies as the cure for this dilemma. However, it should be noted that Mazarr underlines that grey zone strategies may be employed not only by revisionist states but also by the US and other countries. Nevertheless,

since revisionist states have the most urgent motive to effect change, grey zone strategies mostly come from revisionist states (2015, p. 10).

Table 1. 1: Micheal Mazarr's New Formulation of Revisionists States Based on Schweller's Analogy

Passive Status Quo ("Lambs")	Active Status Quo ("Lions")	Targeted Revisionist	Measured Revisionist	Opportunistic Predator ("Jackals")	Reckless Predator ("Wolves")
No motive to overturn system or gain relative advantage; limited investment in current-patterns. Security through appeasement and bandwagoning.	Powerful defense of existing status, supports rules-based order, little motive for aggressive relative gains acquisition. Self-defense, balancing.	Satisfied power with no motive to harm system, but revisionist and risk-accepting on a few issues; little ethno-nationalist motivation; sensitive to relative power, violent in defense of order.	Primary goal is preserving power; favors many elements of global order, but dissatisfied with current status, power relations and rule sets; strong nationalist narratives and motivation; determined to enhance relative power.	Seeks change in power balance, but risk-averse and self-protective; values security of regime more than change in status; will ally with lions as well as wolves.	Values relative gains more than security. Highly risk-tolerant and aggressive. Doctrinal or ideological requirement to spread territory. Determined to upset system. Unlimited aims.
Sweden	United Kingdom	United States	China	North Korea	Nazi Germany

Source: (Mazarr, 2015, p. 20)

Moreover, Mazarr's revisionist element for the grey zone conflict is indeed shared by some other scholars, experts, and policymakers. For instance, James E. Hayes III propose that China, Russia, and Iran are revisionist states that seek to change the post-Cold War global order. These countries are increasing their military capabilities and integrating various means such as information, cyber, and political methods to achieve their objectives. They do so while remaining below the threshold that would trigger a decisive response from the United States (Hayes III, 2018, p. 60). James J. Wirtz (2017) also regards the usage of the grey zone strategies so as to change the status quo to their liking by revisionist states and non-state actors. In addition, Freier et al. (2016, pp. 19-21) put forward that there are three types of actors – status quo, revisionist, and rejectionist– in the contemporary security environment. Revisionist states (for the authors, China, Russia and Iran) "pursue systemic change on a local, regional, or global basis to their decided advantage" and "operate inside the grey zone". In this way, revisionist powers pursue their interests in the grey zone by

using methods and instruments that minimise their exposure and avoid a direct military confrontation with the US (Freier et al., 2016, p. 4).

In addition, Hal Brands (2016, p. 1) also considers grey zone approaches as an area of the revisionist powers that aim to change the existing international environment. According to Brands (2016, p. 5), the strength of the international system persuades revisionist powers to take small steps that raise doubt about what is occurring and prevent severe responses, which might cross established red lines. As an example, as in the case of the other studies, the activities of the three usual suspects – China, Russia and Iran – are mentioned by Brands:

> *"China is using gray zone tactics as part of a campaign of creeping expansionism in the South China Sea. In the Middle East, Iran is using, as it has for many years, subversion and proxy warfare in an effort to destabilize adversaries and shift the balance of power in the region. These are leading examples of the gray zone phenomenon today"* (Brands, 2016, p. 6).

In this respect, most studies in the literature argue that grey strategies are a tool used by weak states against strong states (especially against the status quo power, the US and its allies). Therefore, it can be assumed that grey zone strategies are regarded as asymmetric tools that are adopted by revisionist parties in order to change the status quo in the international system in the long term. Furthermore, Jahara W. Matisek (2017, p. 5) even asserts that an activity/event can only be classified as a 'grey zone conflict' if it is related to shaping the United States-led Western order. If the event has no such relation, it cannot be considered a grey zone activity. For example, Matisek contends that the Tamil Tigers insurgency in Sri Lanka and Chechen rebels in Russia cannot be classified as grey zone conflicts since they do not affect American interests. However, the Moro Conflict in the Philippines is considered a grey zone conflict due to the US's national interest in the matter (2017, p. 5)

However, seeing the grey zone strategies through the only systemic perspective brings questions about the employment of these strategies. For instance, Azad and others (2023, p. 94) have criticised that the considering the grey zone strategies only through the lens of systemic level, especially as a strategy against the US-led international order. Instead, they argue that the status quo can also be regional, and it can even involve disputes between two countries over a contested territory. Moreover,

Mazarr also underlines that it is not necessary to be a revisionist state to engage in grey zone strategies. Although it is very limited, the status quo states can also apply these strategies. Nevertheless, Mazarr (2015, pp. 57-58) generally asserts that grey zone tools and techniques are the tools of weak states because they have no choice against the United States and its allies.

On the other hand, Hal Brands (2016, p. 6) considers that grey zone strategies might also be the tools of the strong states against weaker parties. He argues that grey zone strategies can be asymmetric tools not for the benefit of the weaker parties but for stronger parties. In fact, the statement made by Brands is logical and coherent because stronger parties -at least having considerable military capabilities- can adopt necessary conventional tools in case of escalation. In this context, Dani Belo and David Carment (2019, p. 2) argue that using conventional tools by stronger parties to weaker parties is more likely because the cost of applying conventional tools is much lower. It is because if a state considers that unconventional techniques remain limited to achieve the desired outcome, then they can apply more conventional tools. Therefore, they put forward that states are likely to rely heavily on unconventional tools in symmetric conflicts (Belo & Carment, 2019, p. 2).

Furthermore, Feng Jin (2019, p. 1) argues that in response to China's activities, the US has also applied various grey zone actions, such as imposing sanctions against Chinese military officers, selling military technologies to Taiwan and conducting freedom of navigation operations in the South China Sea. In this respect, instead of stating that the grey zone is a tool of revisionist states or stronger/weaker states, it is more apt to say that it is a tool of states (and state-sponsored actors) that aim to create ambiguity and plausible deniability by staying below the threshold of retaliatory action that is outlined in the United Nations Charter Article 51's guarantee of self-defence, but beyond normal diplomacy.

In relation to changing the status quo, according to Mazarr (2015, p. 33), the second element of the grey zone conflict is the employment of "*strategic gradualism*". Strategic gradualism is the long set of interconnected actions calculated to make gradual progress. In this way, grey zone campaigns are not designed for short-term and decisive gains; on the contrary, through a series of modest actions which help actors

to avoid the sort of fundamental clash. Indeed, when Mazarr conceptualises strategic gradualism, he built the concept on two existing concepts, "*salami-slicing tactics*" and "*faits accompli*".

Salami-slicing is a "*slow accumulation of small changes, none of which in isolation amounts to a casus belli, but which add up over time to a substantial change in the strategic picture*" (Haddick, 2014). Thomas Schelling explains salami slicing with a good analogy:

> *"Salami tactics, we can be sure, were invented by a child; whoever first expounded the adult version had already understood the principle when he was small. Tell a child not to go in the water and he'll sit on the bank and submerge his bare feet; he is not yet "in" the water. Acquiesce, and he'll stand up; no more of him is in the water than before. Think it over, and he'll start wading, not going any deeper; take a moment to decide whether this is different and he'll go a little deeper, arguing that since he goes back and forth it all averages out. Pretty soon we are calling to him not to swim out of sight, wondering whatever happened to all our discipline"*(Schelling, 2008, pp. 66–67).

According to Schelling (2008, p. 68), the effectiveness of salami tactics lies in the fact that the individual violations are small enough to increase imperceptibly and do not provoke a reaction. In recent years, for many scholars, experts, and policymakers, Chinese activities in South and East Asia have been regarded as an example of salami tactics. For instance, Indian Army Chief General, Manoj Mukund Naravane, underlined that China is conducting a salami-slicing strategy:

> *"China is in the habit of making small incremental moves to achieve its goals. Each such move may not be individually noticeable. It (China) has made use of the strategy to make gains in South China Sea without firing a shot or without loss of life. We have shown them this strategy will not work with us and every move will be met resolutely" (Singh, 2021).*

On the other hand, fait accompli is the limited unilateral gain at the expense of an adversary that is unwilling, unable or unaware to respond to the loss (Fischerkeller, 2020). According to Dan Altman (2017, p. 882), *"fait accompli*" aims to secure a small gain that the opponent can concede rather than escalate. Therefore, the key point of fait accompli is calculating the extent of the loss that the defender is willing to tolerate. For instance, whereas Argentina's attempt to seize the Falkland Islands backfired, Russia's 2014 annexation of the Crimea Peninsula is a successful example of the fait

accompli (Kofman, 2020). In this regard, gradualist approaches are attractive to measured revisionists in particular because they seek to bring down elements of the system without leading to general instability (Mazarr, 2015, pp. 33-34, 38). Furthermore, Mazarr argues that gradualist approaches are consistent with the strategic cultures of revisionist states. These cultures (especially Chinese and Iranian) value avoiding decisive battles and achieving strategic goals without the need for such battles (Mazarr, 2015, p. 34).

However, Mazarr (2015, p. 66) also points out a problem regarding the strategic gradualism of grey zone conflicts, which can last for years – even decades. Therefore, the victories of grey zone conflicts will be ambiguous. In addition, according to Azad and others (2023, p. 95), it may be problematic to consider considering grey zone strategies by 'pursuing long-term objectives'. For them, tactics and strategies such as information operations, fait accompli and cyber-attacks can be used intensively by both state and non-state actors to create ambiguity in the conflict. However, maintaining one of the essential aspects of grey zone strategies - ambiguity - over the long term is a challenging task. In support of this argument, Tobias Burgers and Scott Romaniuk (2021) evaluated that Chinese activities cannot be categorised as “salami slices” anymore because they are neither “small actions” nor “small transgressions”. On the contrary, China’s actions have become more evident than ever and it has evoked significant responses in recent years (Burgers & Romaniuk, 2021).

In addition to changing the status quo and employing strategic gradualism, according to Mazarr (2015, p. 43), a third and last part of the grey zone strategy is the employment of “*unconventional tools of statecraft that remain below the threshold of traditional conflict*”. Since the actors that employ the grey zone strategies aim to remain below the threshold to refrain from harsh responses, unconventional tools are being employed. However, the emphasis on the usage of unconventional tools is indeed not new. Instead, it is a significant aspect of various concepts such as political warfare and short-of-war. Moreover, in recent years, as discussed in the previous section, there has also been an increasing emphasis on the non-kinetic tools of the hybrid threat concept. Thus, the hybrid threat is, in some respects, also seen as a strategy for employing a variety of non-kinetic tools. Nevertheless, according to many researchers, the emphases the hybrid usage of the only non-kinetic tools are considered

as the main distinction point between gray zone conflict and hybrid warfare/hybrid threats.

For instance, Elisabeth Braw (2022, pp. 10–11) underlines that while gray zone is “hostile acts outside the realm of armed conflict to weaken a rival country, entity or alliance” on the other hand, hybrid warfare involves “the persistent use of military force”. In parallel to Braw, Fatih Akgül (2021, p. 428-429) underlines that while both concepts refer to hybridity in tools, actors and activities (and in this respect, they are similar in terms of content and execution), they are not the same. Hybrid warfare/threats generally involve the use of military/para-military force and conventional tools. Thus, hybrid tactics can be considered an illegal-criminal spectrum. On the other hand, grey zone conflict is the exploitation of the legal gap between crime and misdemeanour. Therefore, grey zone strategies do not constitute a “violation of international law”. For this reason, Akgül regards hybrid warfare as a kind of war, while grey zone activities are not (Akgül, 2021, p. 430). In this respect, Akgül contends that while hybrid warfare concepts can be used to explain Russian activities in Eastern Ukraine that involve military tools, the Gray Zone Concept is a better fit for China's economy-based strategies (Akgül, 2021, p. 432).

In a similar vein, Michael Mazarr contends that hybrid warfare presents a far more violent clash involving the direct deployment of many military tools. In this sense, he asserts that “hybrid war is truly ‘war’ in the Clausewitzian sense, whereas grey zone strategies are a less violent and looser form of conflict” (Mazarr, 2015, pp. 46-47). Unlike Akgül, Mazarr did not make a distinction between China and Russia and evaluated them along with Iran together as measured revisionist actors. In addition, according to Azad et al. (2023, p. 93) two concepts cannot be used interchangeably because while kinetic tools are limited to hybrid warfare, grey zone warfare is limited to non-kinetic tools. However, Russian activities challenge this kind of separation because both kinetic and non-kinetic means were employed. Hence, they consider the Russian case as an example in which both concepts can be used at the same time. In other words, just because two concepts can applied by states at the same time, it does not mean that they are synonymous concepts (Azad et al., 2023, p. 93).

In addition to the distinction regarding the usage of kinetic and non-kinetic tools, Akgül (2021, pp. 429-430) also differs between two concepts based on state-centrism. For him, using a lot of tools combined, coordinated and simultaneously in the long term necessitates great capacity, and the state has such capacity - even only big and revisionist states. Thus, the non-state actors cannot have such the capacity to conduct grey zone strategies. On the other hand, hybrid warfare is "literally hybrid". Therefore, contrary to some hybrid threats, states are the primary actors in grey zone activities. However, Azad and others (2023, p. 93) criticise this kind of classification because a diverse range of actors can employ both types of warfare. Non-state actors themselves do not have the capacity for grey zone warfare; however, states often use non-state actors (as proxy actors) to carry out their grey zone strategies, as this creates ambiguity and makes it difficult to attribute responsibility.

In contrast to assumptions of the in the *New Era Camp*, the "*Hybrid Warfare camp*" considers the grey zone conflict either as a part of the hybrid warfare concepts or used two concepts interchangeably by just using a "slash (/)" between two concepts (e.g. Cantwell, 2017; Freier et al., 2016). For instance, John Chambers (2016, p.13) defines grey-zone conflicts as those in which state and non-state actors use hybrid threats/tactics. He considers hybrid threats to be in two categories, which are "grey-zone hybrid threats" and "open-warfare hybrid threats" (Chambers, 016, p. 15). In this respect, he argues that hybrid tactics and grey-zone conflict are not independent of each other. They are closely linked, and aggressors employ hybrid tactics along the continuum of conflict to reach their goals (Chambers, 2016, p. 14). Also, there are some studies that questioned distinguishing hybrid warfare and grey zone warfare (Insisa, 2023, p. 170). For instance, according to Anthony H. Cordesman and Grace Hwang (2020, p. 4), it is difficult to distinguish between hybrid warfare and grey zone operations, and attempting to create a precise classification and defining these concepts is counterproductive.

Moreover, there are also studies that argue that Chinese coercive activities, which are generally considered to be a manifestation of the grey zone conflict, are indeed not grey zone warfare but an example of hybrid warfare. In this respect, Aurelio Insisa examined *"Science of Military Strategy"* reports published within the Chinese People's Liberation Army (PLA) ecosystem in 2013 and 2020. These two documents

underline the PLA strategies regarding the use of military forces. In this respect, according to the examination of these two documents, Insisa (2023) asserts that for China, there are no guidelines for creating and using 'grey zones' to achieve political and military objectives without the risk of a major military conflict with adversaries. Additionally, he highlighted that the *Science of Military Strategy in 2013* explicitly acknowledged the risk that such operations could lead to a significant military conflict. Therefore, Insisa argues that China's vision is closer to Euro-Atlantic concepts of hybrid warfare than to the grey zone concept prevalent in the Japanese-American sphere (2023, p. 181).

Similar to Insisa, Alessio Patalano also challenges describing Chinese activities through a 'grey zone' strategy. Instead, he asserts that Chinese activities, especially maritime activities, are the manifestation of the hybrid strategy (Patalano, 2018). China uses "*military, paramilitary, and constabulary means to achieve clear geostrategic objectives in which legal gains over the status of island features and portions of the [East and South China Seas] serve the projection of power and influence within and beyond these basins*". In other words, since the Chinese strategies do not rule out the use of force and China is steadily enhancing its military and law-enforcement capabilities in the region; Patalano argues that China's strategy of coercion in the East and South China Seas is the case of hybrid strategy, rather than grey zone strategy (2018, pp.831-832).

Apart from the "new era" and "hybrid warfare" camps, the "*nothing new* camp", consists of those who see no utility in using the term "grey zone" and believe that it is simply a rebranding of existing forms of warfare (Jensen, 2019, p. 23). Indeed, as Matisek (2017, p. 4) and Brands (2016, p. 4) underlined, there are many debates and criticisms of grey zone warfare as simply a tautological expression of already existing concepts and nothing new about it. In this respect, for instance, Adam Elkus (2015), a well-known critic of the grey zone concept, humorously points out that "*many men, as they age, start to worry about grey hairs. America's military men, however, worry about grey wars*". According to Elkus, various different conflicts are encompassed under the label of "grey zone conflict". He argues that applying grey zone conflict to explain many different kinds of conflicts, ranging from Chinese territorial disputes to Boko Haram's reign of terror in Nigeria to the Russian annexation of Crimea, is

incoherent. In addition to being so inclusive, Elkus also put forward that there is no need for new terminology (grey zone conflict) to explain these conflicts. Instead, according to Elkus, these cases can be explained by already existing concepts such as "*salami-slicing, coercive strategies, escalation dominance, and above all else compellence*". Thus, he believes that grey zone conflict is indeed a composite of two ideas: "Limited wars" and "Compellence" (Elkus, 2015).

> *"The fact that we have to invent new theory […] wars is an indictment of a refusal to exploit massive amounts of existing knowledge and experience. Your parents and grandparents' tax dollars paid for a massive research establishment [for these conflicts and how to counter such threats] much of which rots away unread in research libraries"* (Elkus, 2015).

He also argues that the current challenges, although considered new, are not actually novel. In this respect, he criticises the tendency to see Russia's activities as modern warfare because he argues that Russia's current strategies have been borrowed from the Soviet Union's toolkit. Hence, according to Elkus (2015) the issue is not whether the opponent [of the US] has changed or not, but rather that the US has refused to change. In other words, Elkus asserts that adversaries [of the US] have always used force and other coercive tools to creatively achieve their political goals, while the US has consistently been shocked by their actions. Similar to Elkus, John Arquilla *(2018, p. 121, 126)* also criticises the "notion of grey zone" due to causing confusion rather than clarifying the spectrum of conflict. According to Arquilla, grey zone conflict undermines the understanding of the current conflict landscape and leads to a significant loss of previous knowledge and insights. Therefore, he states that "*If we must have a fresh definition for war in this era—and I am still far from convinced that we should—let it be hybrid warfare the term for present and future conflict*".

Moreover, Donald Stoker and Craig Whiteside strongly (2020, p.2) criticise not only grey zone conflict but also hybrid warfare because they contend that these two concepts are failures to think clearly about political, military, and strategic issues and their vitally important connections. For Stoker and Whiteside, there are four key problems regarding these two concepts: 1) They are poorly constructed; 2) They distort or ignore history; 3) They promote a perilous tendency to conflate war and peace; and 4) They undermine [especially US] strategic thinking through flawed ideas (Stoker & Whiteside, 2020, p.3). In this regard, they argue that both concepts cause more harm

than advantage and lead to an increasingly dangerous misuse of the concepts of war, peace and geopolitical competition, with a resulting damaging effect on the framing of security strategy. Hence, they even advocate for the elimination of both terms from the strategic lexicon (Stoker & Whiteside, 2020, pp. 2-3)

By evaluating all these three camps, Jensen argues (2019, pp. 42-44) that all these examinations are valuable, but the definition of the grey zone still remains elusive. In this respect, he asserts that grey zone conflicts should be viewed as a form of "Restricted Hybrid Warfare". According to him, Restricted Hybrid Warfare is an "*ambiguous and aggressive application of combined national power to revise geopolitical realities or loosen international restrictions in favour of a specific nation state or non-state* actor". In this respect, Jensen argues that Restricted Hybrid Warfare is the product of the current geopolitical dynamics rather than the historical timeless realities. Furthermore, he highlights the strength of the current international order and its norms, which ultimately curtail the behaviour of powerful states and force them to act creatively. Nevertheless, he argues that the elements of the current international order cannot constrain cyber, drone, and information operations. Therefore, Jensen urges to implement new treaties that set the accepted threshold in these areas. In case of the failures to implement accepted threshold in those areas, he urges that "*today's Restricted Hybrid Warfare turn into Unrestricted Total War, in pursuit of an entirely new international system"* (Jensen, 2019, p. 41-44)

Although there are many prominent names and insightful studies related to hybrid warfare, hybrid threat and grey zone conflicts, there is still no commonly accepted definition, explicit distinction, and scope of these concepts. However, the following conclusion can be drawn: The level of the emphasis on the usage of the non-kinetic tools. While grey zone conflict generally draws attention to the hybridity of the usage of various non-conventional tools; on the other hand, hybrid warfare underlines the usage of both kinetic and non-kinetic tools. Thus, if the country's strategy and the examined cases contain non-kinetic tools, it is regarded as a grey zone conflict. In this regard, China's approach is seen as less militarized than Russia's activities. China's approach includes a wide range of non-kinetic activities, such as cyber-attacks, disinformation campaigns, the building and militarisation of small islands in the South China Sea, and economic coercion (Wither, 2023, p.20). However, there are studies

(e.g. Insisa, 2023; Patalano, 2018) that argue that while Chinese activities are given as a relevant popular example of the grey zone conflict, indeed, they should be examined from the lens of hybrid warfare. This is because China has always considered possible military escalation in its strategies even though it has significantly employed non-kinetic tools. Therefore, it would not be wrong to argue that the type of tools used is often the key element in the distinction between the two concepts.

Nevertheless, there is a fact that some tools' usage and impacts can be changed based on the motivation of the perpetrator. For instance, as will be discussed in the following chapter, there are different kinds of cyber-attacks and their roles and impacts differ. Espionage operations, DDoS, and sabotage attacks require different tools, and their impacts and usage aims considerably differ. In general, cyber-attacks are considered non-kinetic tools; however, as the Stuxnet case demonstrates, cyber-attacks can also cause significant physical damage as kinetic tools, even if they are rare. Also, with further technological developments (e.g. artificial intelligence) and an increasingly wide range of usage of these technologies, the offensive capabilities will significantly increase in the future. As, United Kingdom National Cyber Security Centre (2024) points out that "*all types of cyber threat actors are already using AI to varying degrees*", and "*AI will almost certainly increase the volume and heighten the impact of cyber-attacks*". Therefore, as Nathan Freier (2009, pp. 84-85) underscored that just because hybrid challenges are non-military, it does not mean that they are necessarily non-violent, aimless, disorganised, or harmless. Instead, they can be severe threats to the national interest that require a strategic response, even if their origins are not military.

This situation will make it more challenging to classify tools such as cyber-attacks in the future. Therefore, instead of being part of the further theoricatical and conceptual debate, this study offers to pay more attention to the roles of the tools themselves. In this respect, this study aims to examine the roles of cyber-tools which are one of the main tools of all three concepts, namely grey zone conflict, hybrid threats and hybrid warfare. As a hybrid tool, cyber-attacks are chosen since cyber-attacks are among the most frequently used instruments in hybrid warfare, and "cyberspace is a key arena for modern hybrid warfare" (Engström, 2022). ICTs and the Internet have become crucial aspects of the daily lives of modern societies, and therefore, these

technologies are being used by billions of people. As a result, cyber-attacks offer a wide range of exploitation opportunities for threat actors. Moreover, due to the uncentered design of the internet, cyber-attacks are non-attributable in nature. In comparison with other hybrid tools, actors can more easily deny their involvement in cyber activities. In this way, cyber-attacks create more ambiguity and offer plausible deniability. Furthermore, "much of cyberspace [are] in private hands" (Rühle & Roberts, 2021). Hybrid threat actors conduct large number of limited effected cyber-attacks towards to private sector, rather than the directly military and governmental sectors. This means hybrid threat actors can not only blur the lines between war and peace but also between state and society. In this way, while threat actors can directly target the societies -main targets of hybrid warfare-, on the other hand, they can remain below the threshold of conventional warfare. In these respects, as NATO Secretary General Jens Stoltenberg stated that "*cyber is extremely important as part of the […for] hybrid warfare*" (NATO, 2015).

While focusing on the role of the cyber-attacks, this study also adopts the approach of Sean Monaghan's (2019, p. 3) "continuum of the war". According to this approach, based on the usage of the tools, the level of the war moves from hybrid threat to hybrid warfare to conventional warfare as states increasingly use increasing number of tools with increasing intensity. In other words, this approach takes into account the increase of the tools both vertical (intensity) and horizontal. This approach will facilitate classifying tools such as cyber-attacks, which have different purposes and effects. Thus, it will be possible to examine how cyber-attacks are used as a complementary foreign policy tool by states at different motivations and levels. In this respect, in the next chapter, the different roles of cyber tools will be elaborated in detail.

2. THE MULTIFACETED ROLES OF THE CYBER TOOLS AS A FOREIGN POLICY INSTRUMENT

Throughout history, states have utilised new technologies to seek an advantage over their rivals. Whether it was the gunpowder technology of the 14th century, the nuclear technology of the Second World War or the space technologies of the Cold War, states have adapted these technologies to their foreign policies for their benefits. With Information and Communication Technologies (ICTs) becoming indispensable to daily life and their users increasing dramatically each year, states have started to include cyber technologies in their policies in the new millennium. However, technologies are like the double-faced Roman God "Janus". On one facet, it creates a new realm of utility for states to pursue their interests; on the other, it presents a new threat. States are trying to be active on both sides while seeking an advantage over other states and, at the same time, trying to overcome the security problems posed by new threats.

Depending on which side of Janus researchers look from, discussions in the literature also vary. The dual use of technologies leads scholars to focus on both the disruptive potential of technologies and the advancement of those technologies that promise major political, economic, and social benefits (Kavanagh, 2019). These debates also apply the role of cyber technologies as contemporary statecraft instruments. However, there is an essential distinction between cyber technologies and other technological developments in other dimensions (land, sea, air and space). Cyberspace, where cyber activities take place, has a distinct structure and logic: It is human-made and prioritizes secrecy over security. In this respect, Fischerkeller et al. (2022, p. 10) argue that while technological developments have a central role in political/military tactics and strategies, not all these developments result in a significant change in the strategic structure of security. However, cyber technologies have the potential to shape the concept of security itself. Therefore, cyber technologies create a new strategic environment (Fischerkeller et al.,2022)

This study aims to explore the *usage of cyber tools as a foreign policy instrument in the state's bilateral relations.* This requires an analysis of the different approaches to cyber tools. However, as Michael C. Horowitz (2020, p. 386) argues, "*studying new military technologies comes with challenges due to the limited available evidence".* Since cyber technologies are new technologies, these problems also apply to cyber tools. Moreover, since it is rather a new area of study, the number of studies that aim to explain the role of cyber tools in military and political warfare increases daily, and they shed light on different aspects of the cyber tools' role.

In this study, rather than individually evaluating all the assumptions and proposals put forward by scholars, experts, and policymakers, they will be classified based on their shared overarching themes regarding the role of cyber tools. Some scholars may raise objections to this categorisation, advocating for an approach centred on examining cyber-attacks or incidents. However, categorising like theories allows researchers to decide which facts matter and which do not among millions of possible facts (Baylis et al., 2014, p.3). For instance, Kenneth Waltz stated about the causes of the war: *"[Theories cannot explain everything because then theory] would be identical with the real word. [Therefore] People are … thinking in different causal terms; some are thinking that the causes are rooted in human…others saying that caused are found in states … and third way of looking [to the causes of war at rooted]at the international political level* (University of California Television (UCTV), 2008). In this respect, he argued that there were three categories (images) -individuals, states and international system" that explained the causes of war (Waltz, 2018).

In the following sections, the assumptions of the scholars, experts and policymakers about the roles of cyber tools in interstate relations will be examined through three distinct groups. After examining these three groups, it will be argued in what ways these three approaches remain limited and which additional elements should be taken into consideration to explain better the role of cyber tools in interstate relations.

2.1. Beyond Bombs and Bullets: The Revolutionary Role of Cyber Attacks as Substitutes for Conventional Warfare

Technology and war are the two sides of a coin. Throughout history, technology has played a significant role in shaping the methods and character of war. As John Arquilla and David Ronfeldt (1993, p.24) noted, the strategies, doctrines and manner of warfare have constantly undergone significant changes following the technological breakthroughs. While some technological advances have a direct impact on the conduct of war -such as gunpowder abolishing the age of castles and knights and ushering in the age of battalions and cavalry – some of them have profound but limited impact, such as the introduction of automatic machine guns (Kirsch, 2012, p. 620). Today, many scholars, experts, and policymakers contend that advancements in ICTs have once again revolutionised the nature of warfare (e.g., Betz & Stevens, 2011; Lynn, 2010; Liang & Xiangsui, 1999). In this context, this chapter will examine the main assumptions of proponents who assert that cyber tools are novel tools that revolutionise warfare in many aspects.

In general, when a new technology is introduced, even if it has many valuable and beneficial features, there is a tendency to emphasise the potential risks and dangers linked with that technological development. Indeed, this situation stems from the nature of the human beings. As Aristotle (2016, p. 2) once said *"All humans by nature desire to know."* It is because of this nature that people experience fear or anxiety when they are confronted with people or situations in which they have only limited information. "*The fear of the unknown*" is the condition in which individuals find themselves in an unfamiliar circumstance. This fear is especially experienced when one lacks information about the specific situation. As a result, people tend to feel unreasonable fears/anxiety, particularly when encountering people from different backgrounds or cultures. For instance, Xenophobia is the extreme version of the fear of the unknown (Azeem, 2022). Likewise, scholars and experts have emphasised the possible harmful impacts of information technologies as they bring a new threat to national security (Dunn Cavelty, 2007, p. 1).

Although this kind of perception about cyber threats became popular, particularly in the 1990s and 2000s, it is possible to trace the origins of cyber security discussions back to the 1960s, when the first type of affordable business computers

were in use. (Bayuk et al., 2012, p. 15). This period also marked the birth of the Internet. The Internet originated as the Advanced Research Projects Agency Network (ARPANET), a network financed by the US in order to maintain communications in case of a nuclear war (Brendon, 2001, pp. 76-79). In this regard, ARPANET had linked the distant computer sites of the military and some universities, corporations, and industries. However, as picturised in Figure 2.1 below, this design philosophy assigns centrality to one station in the network. While this design is useful to control the flow of the data in the network, the whole network can be down if the central station encounters a problem. Since the aim of creating such a network was to continue communication in case of a nuclear war, this design needed a change in design philosophy. In this respect, Paul Baran (1962) offered a "distributed network"- like a web, as shown in Figure 2.1 below. In the distributed network, each station connects to the other; therefore, even if one station encounters a problem, communication can be maintained through other stations.

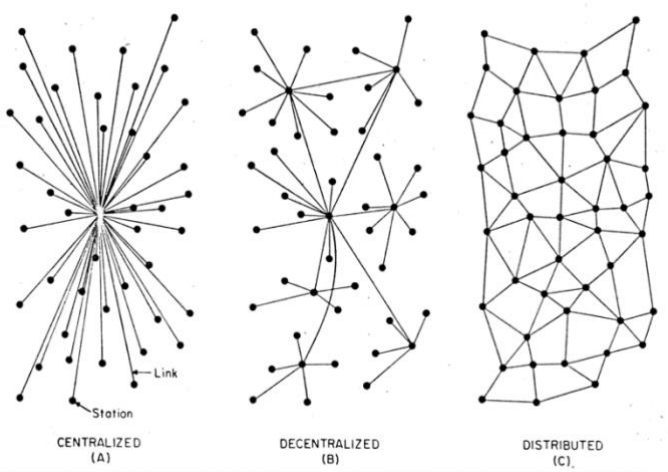

Figure 2. 1: Different Design Concepts of the Internet

Source: (Baran, 1962)

In the following years, as more countries connected to the ARPANET and the number of computers on the network increased, the network significantly expanded. Nevertheless, this growth also introduced new threats to the network, so the US decided to separate its military network from the ARPANET and created a MILNET in 1982 (Bıçakcı, 2014, p. 106). Since then, ARPANET has emerged as a global network with the participation of an increasing number of countries and computers in the network. Particularly following the end of the Cold War era, several bans were lifted, and the Internet became accessible to everyone. This led to the creating of a

virtual world that allows digital data to flow and interconnects all data processing devices worldwide (Bıçakcı, 2014, p. 102). As the network expanded during the 1970s and 1980s, giving rise to increased threats and security concerns, the unprecedented broadening of the network after the Cold War triggered experts, academics, and policymakers to address possible cyber security threats and formulate cyber security policies. In addition, with the advantages that ICTs and IoTs offer, societies' dependency on these technologies has increased exponentially each year. This growing reliance of the states, especially developed ones, where ICTs and IoTs are used more extensively, becomes more vulnerable to potential dangers (Kirsch, 2012, pp. 620–621).

In this regard, scholars have started to address the revolutionary aspects of information technologies and stressed the growing dependence on these technologies, which are ushering in new forms of conflict: Cyber War. This paradigm was evident in the pioneering work, *"Cyber War is Coming",* by analysts from the RAND Corporation, John Arquilla and David Ronfeldt (1993). According to them, as technological breakthroughs led to profound changes in military doctrines, organisations and strategies throughout history; the information revolution also shifted the nature of warfare that necessities new military doctrine, organisation and strategy for cyberspace (Arquilla & Ronfeldt, 1993, pp. 24-25). In this respect, they defined a new kind of war concept: *cyber war*- which is "*conducting and preparing to conduct, military operations according to information-related principles*" (1993, p.30). They examined the revolutionary aspects of the cyber war by comparing it with the strategies of Mongolians and Germans. They asked how "*a Mongol army of some 125,000 could topple a foe whose standing armies amounted to nearly half a million troops, with a similar number of reserves*" (Arquilla & Ronfeldt, 1993, p. 35). The key to Mongol success was "superior command, control, communication, and intelligence". The Mongolians brought extra horses and switched them when one tired. In this way, they could continue without interruption. Moreover, this rapid movement also provides almost real-time intelligence on the enemy's order of battle and intentions. Almost 700 years later, with the Blitzkrieg Doctrine, Germany could disrupt communications and control its enemies at the tactical and strategic levels (Arquilla & Ronfeldt, 1993, pp. 36-37). In other words, the Mongols and then Germans aimed first to disrupt an

enemy's communications, then to strike at his heart. Likewise, with cyber war, states can disrupt the enemy's communication and then launch a devastating attack.

In this respect, John Arquilla and David Ronfeldt argued that even though *cyber war may be to the 21st century what Blitzkrieg was to the 20th century* (p.31) however cyber war brings more revolutionary aspects to warfare. First of all, cyber war is not significantly dependent on geographic terrain, which changes the perception of what is considered a "battlefield". Secondly, with cyber war, states can achieve victory without destroying the enemy forces. In this way, cyber war provides an opportunity for states to defeat the enemy "*at low cost in blood and treasure*". Thirdly, cyber war changes the perspective of what constitutes attack and defeat in warfare (Arquilla & Ronfeldt, 1993, pp. 44-45, 52). For all these reasons, Arquilla and Ronfeldt urged scholars, experts and policymakers to pay attention to this technological change -which represents a major shift in conflict and warfare that no state was prepared for.

This call had broad repercussions in the literature -especially in the developed states- because even weak states could bring strong states to their knees with this revolutionary new bloodless war (Betz & Stevens, 2011; Lynn, 2010). This possibility prompted academics and pundits to focus on the possible impacts of cyber-attacks targeting critical infrastructures that were fundamental to the continuation of modern daily life. In this respect, the popular discourse in the literature was about the vulnerability of the 'critical infrastructure" against cyber-attacks. For instance, Ellis et al. (1997) submitted a report to "The President's Commission on Critical Infrastructure Protection" (in the US), which highlighted the growing ties between the internet and critical infrastructure would increase the significant vulnerabilities and exploitation of these vulnerabilities through cyber-attacks could be devastating (p.iii). Similarly, the US National Research Council (1991, p.7) stated the cyber threats that the United States might face:

> *"To date, we have been remarkably lucky…. We are at risk. Increasingly, America depends on computers. They control power delivery, communications, aviation, and financial services…Although we trust them, they are vulnerable—to the effects of poor design and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."*

Concerns about the vulnerability of critical infrastructures to cyber-attacks have also been raised by Chinese scholars and experts. The prominent book, *"Unrestricted Warfare"*, by Qiao Liang and Wang Xiangsui - is often regarded as a reference book for understanding China's strategic outlook (Barno & Bensahal, 2016)- also shares the same aspect of American counterparts. According to Liang and Xiangsui (1999, p.7), war is no longer about using armed forces to compel the enemy to submit to one's will, as in the classic Clausewitzian sense; "but rather are using all means". In this new war, the battlefield is everywhere, and the enemy is on the network. A war can start from a computer room, and a "hacker + a modem" can do almost as much damage and loss to an enemy as conventional warfare. The only difference between them is "*there is no smell of gunpowder or the odour of blood"* (Liang & Xiangsui, 1999, p.43,129,199).

While the headlines draw alarming cyber-doomsday scenarios and cyber-security experts fear "*cyber-Armageddon*" and called for a "*clichéd*" (Hammond, 2023) *Cyber Manhattan Project* (Richtell, 1997); the 11 September terrorist attacks were a catalyst to boost the fear and threat from the cyber-attacks targeted critical infrastructure. In this respect, the use of cyber tools by terrorists against critical infrastructure become a major concern among experts (Weimann, 2004). For instance, former director of the Federal Bureau of Investigation's (FBI) National Infrastructure Protection, Ronald Dick stated that:

> "*The event I fear most is a physical attack in conjunction with a successful cyber-attack on the responders' 9/11 system or on the power grid… (cyber-attacks) additions to a conventional al Qaeda attack might mean that "the first responders couldn't get there… and water didn't flow, hospitals didn't have power. Is that an unreasonable scenario? Not in this world. And that keeps me awake at night.* (Gellman, 2002)

Also, a letter co-signed by prominent computer scientists was sent to former US President George W. Bush to stress the vulnerabilities of the critical infrastructure of the US to cyber-attacks which could cause even more damage than the September 11 attacks:

> *"Our nation is at grave risk of a cyber-attack that could devastate the national psyche and economy more broadly than did the September 11th attack….The critical infrastructure of the United States …is highly vulnerable to cyber-attack. Fast and resolute mitigating action is needed to avoid national*

> *disaster. We urge you to act immediately by former a Cyber-Warfare Defense Project modelled in the style of the Manhattan Project" (A Letter From Concerned Scientists, 2003).*

The growing concern about cyber-terrorism among academics and officials has had a profound impact on public opinion as well. Survey results, as underlined by Weimann (2004, p. 3) indicated that cyber-terrorism was seen as a major threat on a level with biological and chemical weapons. From this perspective, Myriam Dunn Cavelty (2007, p.1,8) evaluated all these cyber threats from the Copenhagen School's' securitisation approach and referred to them as "cyber threat stories". Indeed, Dunn Cavelty's assertation held merit. It is because, following the heightened threat perception by policymakers and recognition of these threats as security problem by the public, as a last step of the securitisation process, the United States Air Force officially acknowledged cyberspace as the fifth domain of warfare in 2006 (US Air Force, 2006). Indeed, this decision symbolised that cyber-attacks had been successfully turned into a "security issue" by states. However, with the taking the place of major cyber-attacks toward Estonia (2007), Georgia (2008) and Iran (2010), it was assumed that "*the era of cyber war had already arrived*" (Gartzke, 2013, p. 41) and cyber security has become a concern of International Relations department as well.

In 2007, Estonia, then Europe's most wired country, was taken down for almost a month by Russian hackers (Davis, 2007). Several weeks before the 9th of May, which is celebrated as Victory Day against the Nazis by Russia, the Estonian government decided to relocate the Bronze Soldier Memorial, a Russian World War II memorial to the Unknown Soldier, from the centre of Tallinn to a spot on its outskirts. This decision was considered an "*insult to the war dead*" (Kosachev, 2007) by the Russian-speaking population in Estonia and Russia, resulting in a strong reaction. Subsequently, there were unprecedented street riots in Tallinn. Meanwhile, official websites were also targeted with a series of DDoS attacks (Tikk-Ringas et al., 2010, pp.15-16). While the frequency and volume of DDoS attacks had been gradually increasing, the cyber-attacks reached their highest point on 9th May, causing numerous government and major organisational websites to be taken down (Ottis, 2008). After suffering from several attacks, Estonia requested emergency assistance from NATO (Joubert, 2012, p.2). The support from NATO helped reduce the effects of these attacks.

Cyber-attacks on Estonia are regarded as a “first war in cyberspace” in the history (Landler & Markoff, 2007) because, as former Estonia Ministry of Defence- Jaak Aaviksoo - underlined “*this was the first time that a botnet threatened the national security of an entire nation*.” (Davis, 2007). In this regard, this attack has been seen as a “*wake-up call*” (McGuinness, 2017), and NATO approved its first policy on “Cyber Defence” in 2008 (NATO, 2023). After a short time, NATO established the “Cooperative Cyber Defence Centre of Excellence” (CCDCOE) in Tallinn, Estonia. Moreover, at the 2010 NATO Summit in Lisbon, for the first time, NATO included cyber threats in Strategic Concepts by underlining that cyber-attacks could pose significant threats to both member states and NATO (NATO, 2023).

Only a year later after the first war in cyberspace, in the 2008 Russo-Georgian War- *Europe’s first twenty-first-century war* (Dickinson, 2021)- the world witnessed a series of cyber-attacks that synchronised with battlefield (Hollis, 2011, p.2). Russia and Georgia’s bilateral relations had been deteriorating after the Rose Revolution (Kakachia, 2010, p. 88). Since then, Georgia has been seeking to join NATO and developed significant ties with the United States and NATO. As a result of developing ties with NATO, at the Bucharest Summit in 2008, NATO agreed to consider Georgia and Ukraine to include a Membership Action Plan, the initial step for joining NATO (NATO, 2008). This decision was strongly criticised by Russia. The increasing tension turned into a war between the two countries over South Ossetia on 8 August 2008. Indeed, several weeks before war broke out, Georgia’s presidential and officials’ websites had been started to be the target of serious DDoS attacks (Danchev, 2008a). However, On August 8, 2008, when Russian forces began the invasion of Georgia, the DDoS attacks reached a peak point (Danchev, 2008b). In a statement released, the Georgian Ministry of Foreign Affairs said: "*A cyber warfare campaign by Russia is seriously disrupting many Georgian websites, including that of the Ministry of Foreign Affairs*" (Swaine, 2008). Nevertheless, with the end of the war, the cyber-attacks were also alleviated. In this context, experts asserted that the Georgian case represents the “birth of operational cyber warfare” that the use of cyber tools in conjunction with conventional military operations (Thomson, 2008).

However, six years later, Jordan Robertson and Michael Riley (2014) uncovered a new facet of the Russian-Georgian war. On August 5, 2008, three days before the

war, there was an explosion in the Baku-Tbilisi-Ceyhan (BTC) pipeline - which transports oil from the Caspian Sea to Turkey's Mediterranean coast- in Refahiye, Erzincan. At the time, the Kurdistan Workers' Party (PKK) terrorist organization claimed responsibility, while the Turkish government attributed it to a malfunction (Kurt & Erinç, 2021, p. 10). Although each centimetre of the pipeline has been under surveillance, 60 hours of surveillance video that recorded the area of the explosion had been erased. According to the report of Robertson and Riley (2014), a single infrared camera that was not connected to the same network captured images of two men with laptops walking near the pipeline days before the explosion. Experts who evaluated the incident stated that two people with computers could have been in the area to infiltrate wireless networks (Varlık, 2014). In this regard, it was assumed hackers deactivated alarm systems, disrupted communications, and over-pressurised crude oil, leading to an explosion (Robertson & Riley, 2014). Following the event, neither Russian nor Turkish officials commented on the matter. However, US intelligence agencies claimed that the attack was orchestrated by Russia, as Russian jets dropped bombs near the pipeline after the explosion, and Alexander Dugin, a prominent supporter of Russian expansionism, stressed that "*BTC was dead*" (Kucera, 2014).

While Chris Blask, who is an expert on Industrial Control Systems, evaluated this attack as a case of the young history of cyber war, Prof. Derek Reveron at the US Naval War College asserted that this cyber-attack "*rewrites the history of cyber war* (Robertson & Riley, 2014). However, for many experts, *Stuxnet* is the cyber-attack that "*opens new era of warfare*" (CBC NEWS, 2012). As part of the broader US cyber campaign against Iran (Olympic Games), allegedly a joint US-Israeli cyber-attack caused damage to more than 1000 centrifuges at Iran's uranium enrichment facility in Natanz (Sanger, 2012). Experts claimed that Stuxnet was one of the "*technologically most sophisticated malicious program developed for a targeted attack*" (Matrosov et al., 2011, p.62). Since Stuxnet caused physical damage to a nuclear facility without an internet connection, for many experts and scholars, Stuxnet represents a "*Revolution in Military Affairs (RMA)"* that fundamentally changes the "nature of cyber warfare" (Shakarian, 2011, p. 1). Therefore, as Cassandra M. Kirsch stressed (2012, p. 621), "*cyber warfare is no longer science fiction"*. In this respect, former US Director of the Central Intelligence Agency and National Security Agency, Mike Hayden, stated, "*We have entered into a new phase of conflict in which we use a cyberweapon to create*

physical destruction" (CBC NEWS, 2012). Furthermore, some experts even equated Stuxnet with the dropping of the atom bomb (Groll, 2016). Similarly, Dmitry Rogozin, Russia's ambassador to NATO in 2011, claimed that Stuxnet could have triggered a nuclear disaster on the scale of Chornobyl (The Moscow Times, 2011). Hence, according to the majority of the literature, Stuxnet means that "*for cyber war, the future is now*" (Farwell & Rohozinski, 2011, p.23).

On the other hand, there was also a concern that many revolutionary advantages of cyber-attacks, similar to Stuxnet, would benefit weaker actors than strong ones due to the logic of asymmetry. Since developed states, especially great powers, live in glass houses, they are vulnerable to attacks from weaker actors with less dependency on cyberspace (Lindsay, 2013, p. 375). In this respect, Sean Collins and Stephen McCombie (2012, pp. 87-89) stated that "cyber warfare does not only open to nation states but also the aggressors". Therefore, they emphasise that the greatest risk of Stuxnet is that hackers, organised crime networks or terrorists may reproduce or modify its code. These actors could develop cyber tools similar to Stuxnet to achieve their goals, and they may not limit their impact as the US and Israel did in their operations against Iran. Therefore, Stuxnet may have triggered a new arms race carrying potentially significant security implications (Collins & McCombie, 2012, p. 80). In addition, Lucas Kello (2013, p.8) stressed that the "cyber revolution has not fundamentally changed the nature of war"; however, the "*most obvious and important consequence of new technology is its ability to affect the balance of power*" (Kello, 2017, p. 100).

Cyber revolution expands the range of harm beyond the war by including non-military foreign threats and the ability of non-traditional players. Hence, revolutionary cyber technologies are a force of systemic disruption that can drastically affect the character of the international order (Kello, 2017, p. 100, 199). Therefore, for the cyber revolutionist, even though the US carried out Stuxnet, the US is the country most at risk, both because of the logic of asymmetry and because of the change in the balance of power in the international system. In other words, new revolutionary cyber technologies put the US at greater risk in terms of both national and international security. In the article former US President Barack Obama wrote for the Washington Post, he also shared this assumption:

> "*In a future conflict, an adversary unable to match our military supremacy on the battlefield might seek to exploit our computer vulnerabilities here at home… This is the future we have to avoid*" (Obama, 2012).

Moreover, Former US Defense Secretary Leon E. Panetta warned that the United States was facing the possibility of a "*cyber-Pearl Harbor*":

> *"An aggressor nation or extremist group could use these kinds of cyber tools to gain control of critical switches. They could derail passenger trains, or even more dangerous, derail passenger trains loaded with lethal chemicals. They could contaminate the water supply in major cities, or shut down the power grid across large parts of the country (Bumiller & Shanker, 2012).*
>
> *"The potential for the next Pearl Harbor could very well be a cyber-attack" (ABC News, 2021).*

As Jon R. Lindsay (2013, p.366) indicated, with the Stuxnet, "*genie is out of the bottle"*. After the Stuxnet, the major cyber incidents such as Sony Hack, Ukrainian Power Grids attacks, and hacking of the Democratic National Committee (US) WannaCry, NotPetya, and SolarWinds took place. After each of these incidents, the cyber revolutionists have continued to emphasise the revolutionary aspects of cyber-attacks in different aspects. However, if cyber tools are as revolutionary as nuclear weapons (Mazanec, 2016, p.102) and if the next threat to national security is cyber war" (Clarke & Knake, 2010) which has been keeping strategic planners from sleeping peacefully at night (Mead, 2015); then, literature also try to find answer the question of Clint Hinote (2015): *How can we stop the next cyber-attack* that threats overall stability and security of our societies (Klimburg, 2017, p. 2). There have been many proposals, theories, and strategies in the literature to answer this question. However, this chapter will also briefly discuss the deterrence strategy and approaches of normative school.

Due to the success of deterrence strategies during the Cold War, many scholars have tried implementing deterrence in cyber strategies. The root of the cyber deterrence concept goes back to "information warfare" during Operation Desert Storm in 1991 (Stevens, 2012, p. 149). With the introduction of the "cyber war concept", the cyber deterrence concept was also introduced (Derian, 1994). Since then, scholars have been striving to implement appropriate deterrence strategies for the cyber domain for years (Libicki, 2009; Harknett R. J., 1996; Goodman, 2010; Ryan, 2018; Limnell,

2017; Elliot, 2011). As Gorwa and Smeets (2019, p. 10) underline, with the prominent cyber-attacks on Estonia, Georgia, and Iran (Stuxnet), deterrence attained its reputation, and cyber deterrence lived its "golden age" between 2010-15. However, the idiosyncratic cyber domain obstacles -signalling credible threat, proportionate response, and attribution problem- complicate applying cyber deterrence strategies (Taddeo, 2018b; Libicki, 2009). To overcome those challenges, scholars have offered insightful solutions (Buchanan, 2014; Lasconjarias, 2017; Lupovici, 2014, 2021; Rid & Buchanan, 2015).

Also, new forms of deterrence in cyberspace have been proposed. For instance, Lucas Kello (2017) endorses "punctuated deterrence' instead of tit-for-tat replies for a succession of measures that have a cumulative impact. Similarly, Uri Tor (2017) introduces the concept of "cumulative cyber deterrence", which contends that defences should aim to prevent a succession of attacks rather than a single attack. However, the golden age of the deterrence concept for cyberspace has been gradually fading, and the assumption that "*deterrence is not a credible strategy for cyberspace*" has become prominent (Fischerkeller & Harknett, 2017). In addition, the US's abandonment of deterrence as a cyber strategy in 2018 and the adoption of the "Defend Forward" approach instead catalysed the decline in the interest in deterrence strategies in the literature.

On the other hand, since cyber-attacks have revolutionised the battlefield, there are calls for multilateral treaties and regulations like the Geneva Convention for cyberspace (Kirsch, 2012, p. 620). For instance, Secretary-General of the United Nations, António Guterres, stated that:

> "*When one looks at today's cyberspace, it is clear that we are witnessing, in a more or less disguised way, cyber wars between states…. I think it's high time to have a serious discussion about the international legal framework in which cyber wars take place.* (UN Secretary General, 2018)

There have also been calls from the technology giants for a "Digital Geneva Convention":

> *"Just as the Fourth Geneva Convention has long protected civilians in times of war, we now need a Digital Geneva Convention that will commit governments to protecting civilians from nation-state attacks in times of peace"* Brad Smith (Microsoft's Vice Chair and President) (2017).

In this context, Taddeo (2018a, p. 326) stated that norms - *standards of behaviour defined in terms of rights and obligations* - are the most effective way to limit and change the undesirable behaviour of states and foster stability in cyberspace. Also, to reduce/prevent adverse actions in cyberspace, Joseph Nye underlined that normative taboos might deter some cyber-attacks by incurring reputational costs (pp. 54–55). Indeed, we have witnessed the strive for cyber norms and regulation of cyberspace for more than two decades. The issue of information security has been on the UN agenda since 1998. In this respect, in 2004, the United Nations established a "*Group of Governmental Experts (UNGGE)*" (UN Office for Disarmament Affairs, 2023). UNGGE comprises 25 countries (2024) based on equitable geographical distribution and includes major cyber powers such as the US, China, and Russia (NATO Cooperative Cyber Defence Centre of Excellence, 2023). The main objective of the UNGGE is to reach an agreement on a set of voluntary rules for state behaviour in cyberspace (Taddeo & Floridi, 2018, p.297). Moreover, in 2015, UNGGE even adopted a consensus report (UN General Assembly, 2015) that proposes norms of responsible behaviour and includes comments on how international law applies. Although it is an undeniable fact that these norms are an important step for the construction of the international cyber society, the general theme of accepted norms is related to "state sovereignty", such as "prohibition of the use of destructive cyber weapons", "the right to self-defence" and "principle of non-interference in the internal affairs of other states". This fact indicates that "*state sovereignty*" is the only norm that states can have a consensus about cyberspace at this stage.

In addition to UNGGE, Tallinn Manuel (I-II), initiatives of NATO CCDCE, bring together experts from governments, private companies, NGOs and academia to analyse cyber issues and how to apply international law to cyberspace. As outputs of this initiative, Tallin Manuel I (Schmitt, 2013) and Tallinn Manuel II (Schmitt, 2017) have been the most compressive studies on applying international law to cyber operations. However, it is non-binding and just an academic study. Martha Finnemore and Kathryn Sikkink (1998, p. 901) noted that a norm gains international recognition in its life cycle if endorsed by one-third of the states and the major powers. China and Russia do not favour and support the Tallinn Manual, while the United States abstains from some articles. In this respect, Brian Mazanec (2015, pp. 86, 107) argued that self-interested states, especially great powers, will not implement mechanisms that will

limit themselves. Instead, they defend only international cyber norms and rules parallel to their political agendas. However, James Woord Forsyth and Billy Pope (2014, p.114) and Hidemi Suganami, Madeline Carr, and Adam Humphreys (2017, p.16) asserted that great powers will inevitably cooperate to establish rules, norms, and standards for cyberspace because norms and international law will reduce the grey in cyberspace by providing some predictability and certainty. For this reason, they stressed that "it is inevitable that states will cooperate in the future".

Since ongoing normative studies and the absence of a cyber-attack that would materialise into the long-feared 'cyber doom' scenario (Lawson, 2021), the depiction of cyber-Armageddon has long been abandoned (Shandler & Gomez, 2022, p. 1). However, as Russia increased its military build-up along Ukraine's border and the Russia-Ukraine war appeared on the horizon (The Economist, 2022); *"the spectre of cyber war is back"* (Lennart & Nadiya, 2022). For cyber security experts and scholars, the Russia-Ukraine War has been substantial in many aspects. First of all, it could give the world its first experience of a true cyber war (Miller, 2022). For the first time, a state (Russia) that has real cyber capacity with significant conventional offensive capabilities is part of the war (Maschmeyer & Dunn Cavelty, 2022, p. 2). Secondly, Russia has conducted numerous significant cyber-attacks; again, it could employ a new significant one. In this way, this war may redefine how we think about cyber conflict and give clues about what the future of warfare might look like (Marks, 2022). Thirdly, since 2014, when Russia-Ukraine bilateral relations collapsed after Russia annexed Crimea and heavy support for pro-Russian separatists in Eastern Ukraine (Caferov, 2022), Ukraine has been the constant target of Russian cyber-attacks. For instance, in 2015, cyber-attacks which targeted Ukrainian power plants caused a power outage for more than 225,000 residents (BBC News, 2016). Moreover, in December 2016, almost one year after the power grid attacks, Ukraine's former president, Petro Poroshenko, revealed that:

> *Ukrainian state institutions about 6,500 times in the past two months were targeted and investigations shows that complicity directly or indirectly of Russian security services waging a cyber war against our country (Ukraine)* (Zinets, 2016).

In this respect, Ukraine has been considered as "*Russian test lab for cyber war*", and cyber-attacks on Ukraine were regarded as the trial run of the cyber-attack that can

be used in the future against rivals of Russia (Greenberg, 2017; Maschmeyer & Dunn Cavelty, 2022, p.2). Accordingly, analysts (e.g., Giles, 2021) and former British Prime Minister Boris Johnson claimed that Russia could achieve its aims without invading Ukraine but carrying out cyber-attacks.

> *"World leaders must not let images of tanks panic them into forgetting Russia has other options than invasion. Stand-off strikes using missiles, or potentially a destructive cyber onslaught, could target military command and control systems or civilian critical infrastructure and pressure Kyiv into concessions and its friends abroad into meeting Russia's demands" (Giles, 2021).*

> *"The old concept of fighting big tank battles on the European land mass are over … there are other big things that we should be investing in … [like] cyber—this is how warfare of the future is going to be" -Former British Prime Minister Boris Johnson- (Martin, 2022).*

On the other hand, many officials and scholars warned that "if Russia does attack Ukraine, the opening salvo is likely to be with offensive cyber capabilities" (Healey, 2022). In other words, even if Russia invades Ukraine employing conventional means, Russia would initially deploy cyber-attacks to create "*shock and awe"* that cause Ukraine's defence to collapse (Brennan et al., 2022; Courtney & Wilson, 2021). In this respect, "Ukraine seemed to be the ideal battle space for such an apocalyptic cyber-attacks" (Rid, 2022).

On 24 February 2022, Russia started a military operation against Ukraine. Since then, we have witnessed different types of high-tech weapons, from armed drones to jet fighters. However, Russia has not yet launched a costly cyber war against either Ukraine or its Western allies (Mueller et al., 2023, p.2). Therefore, Thomas Rid asked:

> *For decades now, we were warned that cyber war is coming and the next big state-on-state military confrontation could start with a flash-bang cyberattack…In 2022 the war came but why you haven't heard about the secret Cyber war in Ukraine?"(Rid, 2022).*

On the other hand, David Cattler and Daniel Black (2022) asserted that "missing cyber war is a myth" and Russia's attacks succeeded in Ukraine. Based on the forensic analysis of security companies, they emphasised that the lack of overwhelming "shock and awe" in cyberspace has led to flawed presumptions and dangerous misdiagnoses. Instead of one single attack, the cumulative effects of the Russian cyber-attacks were substantial. Through this perspective, they claimed that Russian cyber operations had

been the biggest military success of Russia to date in the war (Cattler & Black, 2022). As a response, Brondon Valerione (2022) stated that:

> *"When a cyber conflict did not materialize, pundits fell back on the typical claim that it was really happening, but we just couldn't see it. The cyber war is mainly fought in the shadows, or perhaps the "Upside Down" like in Stranger Things. It's all there, we just don't know where to look, apparently."*

Now, two years later, it can be asserted that despite deploying numerous cyber-attacks, as indicated by Chris Martin (2022), "the next war did not take place in cyberspace after all". Furthermore, there have not been any severe cyber-attacks or noteworthy strategic changes resulting from the cumulative effect of cyber operations to date. If cyber-attacks were to replace kinetic warfare, why did Russia opt for conventional military operations? Perhaps the answer lies in the fact that "missiles are more straightforward than computer code", as underlined by Gordon Corera (2022). However, three decades ago, John Arquilla and David Ronfeldt (1993, p.41) not only warned that "cyber war is coming" but also about the potential misperception that the implications of revolutionary technologies may not be widely perceived at first. In this regard, Chris Blattman (2022) urged us that just because there was no reprisal in 2022, it does not mean the world might get so lucky in 2023. Although these warnings should never be disregarded, the belief about the revolutionary role of cyber-tools in changing the nature of war has been significantly undermined by the Russia-Ukraine War. Brandon Valerione (2022b) even jokingly criticised those who are still looking for cyber warfare after the Russia-Ukraine war: There is little difference between Harry Potter's adventures and mythical cyber warriors. *So, do you believe in cyber magic or not?* In the next chapter, scholars who assert why we should not believe in cyber magic and why the next Pearl Harbour is much more likely to occur in Hawaii than in cyberspace (Gartzke, 2013, p.73), will be discussed.

2.2. Limited But Complementary Role of Cyber-Tools in Interstate Relations

In the previous section, the arguments which assume the role of cyber tools as revolutionary in military affairs and they can cause similar or even more damage than conventional wars were discussed. As indicated in the previous chapter, a cyber doom incident has not occurred yet. Such a kind of cyber-attack may still be forthcoming, but past and present evidence indicates that these threats are overstated than the real

evidence (Shandler & Gomes, 2022, p. 1). Particularly in the case of the Russia-Ukraine War, in which most pundits and scholars warned of the dramatic consequences of cyber warfare, the absence of such a cyber-attack has led many scholars to conclude that cyber tools are unlikely to substitute for the use of conventional force (Maschmeyer & Kostyuk, 2022). In this regard, some scholars criticise the premise of the revolutionary role of cyber tools in changing the nature of warfare (e.g. Rid, 2012; Valeriano et al., 2018). For them, the revolutionary features attributed to cyber tools in terms of *asymmetry*, *offensive-defensive balance*, and *balance of power* are flawed. Instead, they are rather limited tools that can be useful instruments to amplify political warfare in the modern era. In this regard, this chapter will examine in detail those approaches that argue that cyber tools are evolutionary and complementary rather than revolutionary and substitutive.

Martin Libicki (2012, p. 335) argues that considering cyberspace as a warfighting domain is deceiving and even possibly dangerous. This perception does not help us understand what can and should be done to defend and attack networked systems (p. 322). If such a portrayal leads strategists and operators to form presumptions or conclusions that lack experience and observation, it may mislead them. To put it another way, the main problem is the connotations rather than denotations. *The argument that cyberspace is a warfighting domain, only a really different one, begets the question of what purpose is served by calling cyberspace a domain in the first place. Our purpose is, therefore, akin to what our ancient Chinese friends would have called the rectification of terms: making the name of the thing match the nature of the thing.* (p. 322). In short, Libicki warns that by naming and labelling cyberspace as a domain and even a warfighting domain, fruitless hours are spent developing a comprehensive theory covering this agglomeration (p.336).

While Libicki questioned whether the cyber domain is warfighting or not, Thomas Rid (2012) criticise the concept of cyber war itself. According to Rid, so as to define an event as war, it must meet Clausewitz's three requirements: "Violent", "Instrumental", and "Political". As written on the first page of Clausewitz's prominent piece, "On War", *"War is an act of force to compel the enemy to do our will"* (Clausewitz, 1976). All warfare is inherently violent. If an action is not potentially violent, then it cannot be considered an act of war. In Clausewitz's way of

understanding, violence is the key to all war. Secondly, an act of war is always instrumental. Being instrumental describes that there must be a *means* and an *end*. While physical violence can be a *means* to change the adversary's decision, it can be an *end. At the tactical, operational, strategic, and political levels, the* instrumental use of *means* takes place. At each level, it is increasingly difficult to achieve the end. In fact, this explains Clausewitz's famous words: "*War is …true political instrument, a continuation of political intercourse, carried on with other means*" (1976, p. 87). In this respect, war is never an isolated act but carries larger political purposes. Hence, an act of war is always political (Rid, 2012, p.8). Also, to be political, a political entity must have a will. This "will" must be communicated to the adversaries and attributed to these political actors (Rid, 2012, p.8).

However, according to Thomas Rid (2012, p. 10), while no cyber-attack has so far met all three of Clausewitz's criteria, there are also very few cyber-attacks in history that meet only one of them. Therefore, he argued that "*cyber war has never happened in the past. Cyber war does not take place in the present. And it is highly unlikely that cyber war will occur in the future*" (p.6). Instead, according to Rid, "all past and present political cyber-attacks are merely sophisticated versions of three activities that are as old as warfare itself: *subversion, espionage, and sabotage* (p.6). In this respect, cyber-attacks rarely, if ever, kill or physically harm anyone. They have an effect: Usually to gather information through espionage, to influence outcomes through subversion, or to disrupt through sabotage. But even cyber sabotage is an indirect result.

Similarly, Ciaran Martin (2022) has emphasised that the constraints of cyber tools as a tool of warfare are not adequately understood. Cyber instruments do not perform the same in a war as fighter jets, missiles, or soldiers. Rather than carrying out physical attacks, they can cause a battlefield impact by disrupting the adversary's military's logistical and operational capabilities. This means that cyber tools are not the instruments to be used to cause two trains to crash but rather to stop working them. Therefore, the cyber tools may have an effect on the war, but they will not be able to shift the course of the war.

Erik Gartzke (2013) also echoes Thomas Rid's view on cyber war. He emphasises that war is fundamentally a political process, and therefore, cyber war should not be seen as the ultimate determinant in an anarchical world but as a part of traditional forms of political violence (2013, p. 42). According to Garzke, the belief of cyber pessimists that cyber tools can substitute traditional physical conflict due to their potential for harm is flawed (p.57). Contrary to the popular portrayal of catastrophic damage caused by cyber-attacks, cyber-attacks actually have only a short-term impact (p.57). To achieve long-term effects, cyber-attacks must be accompanied by more traditional means (pp.58-59). So, there is no reason to believe that cyber tools will substitute conventional instruments of warfare.

Moreover, Garzke also asks, “If the aim is to destroy, why an attacker should deploy cyber-tools which has no guarantee of success? One can answer this question as cyber-attacks are useful for states with limited military capabilities against the major powers due to the logic of asymmetry. Therefore, these states can opt for cyber capabilities, which are easier to obtain than missiles. However, Gartzke asserts that "*rather than threatening to overturn the existing world order, cyber war may perpetuate or even increase current military inequality*” (p.63). In other words, cyber tools cannot change the balance of power between states. In order to enhance his assumption, Gartzke gives the most famous Estonia, Georgia and Stuxnet incidents and argues that these attacks are important and effective not just because these cyber-attacks are revolutionary but because attacker states had an advantage in conventional capabilities. In other words, *cyberattacks will be most efficacious when the conventional military balance already favours an attacker* (p.65). Because of these reasons, Gartzke concludes that “*cyber war is not a revolution in military affairs in strategic (military) terms, nor is cyber war likely to prove revolutionary in political terms, by threatening or transforming existing global or regional power structures*” (pp.63-64). Cyber war is just a *“myth”* (p.41). Hence, he asserts that a surprising, devastating attack will be more likely to occur in Hawaii than in cyberspace (p.73).

Similar to Garztke, Jon. R. Lindsay (2013, p. 403) also opposes the idea of cyber revolution in military affairs and puts forward that cyber war will continue to evolve as a complement to traditional military and intelligence operations. According to Lindsay, Stuxnet, which is often cited as an example of the revolution in military

affairs, does not meet any of the conventional notions of the cyber revolution, which are "*asymmetry*", "*failure of deterrence*", and "*offensive dominance*". Regarding asymmetry, he challenges the view that weak actors will be empowered while strong actors will become seriously vulnerable because advanced industrialised countries depend more on cyberspace than less wired countries (p.375). In contrast to major powers, weaker actors have limited resources to weaponize cyber tools and are vulnerable to retaliation if they manage to damage the stronger actors. On the other hand, major states have the resources and risk-taking capacity to carry out cyber-attacks against relatively weaker targets (pp. 386-390). Therefore, there is a high frequency of low-intensity cyber-attacks but a remarkably low frequency of high-intensity cyber warfare resulting in serious infrastructure damage (p.374). In this respect, Lindsay states that cyber tools do not alter the balance of power in favour of weaker but stronger, as Stuxnet demonstrated.

With respect to the balance of power, Adam Liff (2012) also objects to the idea that cyber tools are equalisers of the power between strong and weak states. He argues that assessing cyber tools as "game-changing" in international peace and stability is an exaggeration (2013, p. 137). Since weaker states cannot follow the conventional force after the cyber-attacks, they cannot afford to escalate the crisis against the stronger parties even if they have the capacity to develop devastating ones (2012, p.425). Moreover, even if conducting cyber-operations is relatively low cost, it is doubtful that weak states can bring organisational and technical capacity together to launch a sustainable cyber-attack against a stronger state (2012, p.425). Therefore, Liff argues that cyber tools are not novel absolute weapons but tools for states to "pursue political (strategic) and/or military (tactical) objectives at relatively low cost in very limited circumstances" (2012, p. 426).

As for the failure of deterrence, Lindsay underlines that deterrence may have been effective. After the Stuxnet incident, Iran retaliated by launching DDoS attacks against major banks in the US, and this retaliation was considered an act that was regarded as a cyber-war and a failure of deterrence (2013, p.397). However, Lindsay argues that the planners of the Stuxnet were actually concerned about the potential for retaliation, and therefore, they restrained the scope of Stuxnet. In other words, the US was indeed deterred from conducting an overt attack on Iran. However, the United

States decided to participate in a joint cyber operation to reassure Israel. If there is evidence of deliberate restraint over the scale of the cyber-attack, as in the case of Stuxnet and Iran's retaliation, Lindsay argues that this suggests that deterrence is effective between two states. Therefore, Lindsay suggests that the logic behind the "*stability-instability paradox*" in classical Nuclear Deterrence Theory, which indicates that nuclear stability leads to limited conventional instability, also applies to cyberspace. As a result, a significant amount of limited cyber-attacks may be deployed, while serious attacks with significant consequences are unlikely to occur (p. 401).

Moreover, scholars also criticise the main assumption that "offence has the upper hand in cyberspace" (Lieberthal & Singer, 2012, p.14; Lynn, 2010, p.98). In IR, "offence has the advantage" refers to a situation in which "*it is easier to destroy the other's army and take its territory than it is to defend one's own*" (Jervis, 1978, p. 187). In other words, "*war is more likely when conquest is easy*" (van Evera, 1998, p. 6). According to the Offense-Defence Theory, changes in the offense-defence balance significantly affect the risk of war. Therefore, in order to prevent a war, the defence should have an advantage over the offence (Glaser & Kaufmann, 1998, p.44). Nevertheless, to achieve balance, there is need to measure both offence and defence. In this respect, while some scholars (Glaser & Kaufmann, 1998) try to find ways of measuring offense-defence balance, on the other hand, some scholars argue that measuring the offense-defence balance is problematic because states cannot perceive offense-defence balance correctly (Lynn-Jones, 1995, pp. 677–679).

As in the IR, the offence-defence dichotomy is a popular topic in cyber security. The main idea of the offence-defence theory – the advantage of offence makes war easier- has also been adopted by many scholars and experts to underline the risk of cyber war. Most scholars contend that cyberspace favours the offence due to the "internet's design", which prioritises the ease of sharing information anonymously over security (Nye, 2010, p. 5; Lieberthal & Singer, 2012, p. 14) and "ICT-induced cyber capabilities" that can severely restrict adversaries' ability to retaliate by disabling enemy's military capabilities (Saltzman, 2013, p. 44). On the other hand, Erik Gartzke and Jon R. Lindsay (2015, pp. 323–324) ask that if the offence has an advantage on the defence, why are we not seeing the offensive destructive cyber-attacks? Major powers are subject to millions of cyber-attacks daily. However, the

most concerning cyber-attacks have not yet taken place despite decades of warnings. Furthermore, even the most devastating cyber-attacks to date, such as Stuxnet, only resulted in limited and temporary disruption. Therefore, the absence of such attacks could suggest that cyberspace favours defence over offence (Lindsay, 2013). In this regard, Lindsay argues that the cyber revolutionaries' cases are mostly about cyber theft and espionage and therefore "cyberspace may be offense dominant for criminals and spies, but not for soldiers" (p.398-399).

In addition, Rebecca Slayton (2017, p.106) also counters the argument that cyberspace favours the offence and argues that "offence *dominance of cyberspace are fundamentally flawed*" (Slayton, 2017, p.106). Cyber tools offer significant advantages due to anonymity. Nevertheless, if cyber tools are designed to target physical systems, their cost substantially increases due to the expense of cyber operations that attempt to control complicated systems. Such operations can be costly in terms of both the preparation process and possible results. Consequently, the cost of the offence exceeds the defence, significantly diminishing the offence's advantage (Slayton, 2017, pp. 106-108).

Since many cyber revolutionist scholars assume that offence has the upper hand over defence, they also underline that using cyber tools may lead to military escalation, even resulting in nuclear warfare (Lonergan, 2022). For instance, Jason Healey and Robert Jervis (2020, p. 36) argued that "*a cyber incident might cross the threshold into armed conflict either through a sense of impunity or through miscalculation or mistake*". In IR, questions such as - "*how and why do crises occur*" and "*under what conditions are crises resolved peacefully and what conditions tend to make them escalate to war?*" (Snyder & Diesing, 1977, p.10) have been given significance importance and have been discussed by many scholars (Axelrod & Hamilton, 1981; Fearon, 1995; Gochman & Leng, 1983; Powell, 2002; Schelling, 1957). Similar questions have also been addressed regarding cyber tools, and it has often been asserted that cyber tools have the potential to lead to an escalation between rivals. For scholars, cyber-attacks are considered escalatory tools between rival states because of the conjunction of several problems related to cyberspace, which are a) the advantage of offence over defence, b) asymmetric relations between strong and weak states, c)

attribution problem, d) lack of exact red lines (threshold) between war and peace and e) inadequate command and control mechanism in cyberspace.

Nevertheless, Erica D. Borghard and Shawn W. Lonergan assert that there is empirical evidence to suspect that the likelihood of cyber escalation may be exaggerated. If cyberspace does indeed generate severe escalation risks, why have cyber tools not yet triggered a war? (Lonergan, 2022). Contrary to expectation, cyber tools have remained limited -below the use-of-force threshold- and have not escalated to war. Thus, Borghard and Shawn (2019, p.123) underline that "*cyber escalation has not occurred because cyber operations are poor tools of escalation*" due to the four key characteristics of offensive cyber capabilities.

Table 2.1: Linking Offensive Cyber Attributes with Escalation Pathways

Cyber Attributes	Escalation Pathways
Role of access, nonuniversal lethality, and temporal nature of access and capability development and maintenance	Lack of cyber escalation options at the desired time and implications for considering alternative courses of action
Nonphysical nature of offensive cyber capabilities and limits on cost generation	Limited costliness of effects
Role of secrecy, attribution, and espionage	Countervailing tradeoffs
Nonphysical nature of offensive cyber capabilities, nonuniversal lethality, and limits on cost generation	Lack of willingness for cross-domain escalation in response to cyber incident with limited relative costs

Source: (Borghard & Lonergan, 2019, p. 125)

First of all, cyber operations are poor tools for escalation because retaliatory offensive cyber operations may not be available for deployment when they are required due to various technical reasons. As most cyber-attacks (except DDoS) rely on exploiting target vulnerabilities to gain access, fixing such vulnerabilities would prevent unauthorised access. If the target fixes the vulnerabilities, then the cyber tools become obsolete (Borghard & Lonergan, 2019, p. 125). In addition to being dependent on access to the target's systems, secondly, cyber tools impact may not cause severe costs, which could lead to escalation between rivals (pp.131-133). The essential limitation on the cost-generating ability of offensive cyber operations is rooted in the absence of physical violence. Cyber tools could be utilised to disrupt an adversary's networks and systems. Such actions can render the networks temporarily non-functional or impair confidence in their reliability. In addition, these weapons could cause destructive effects, such as damaging data stored on these systems. Rarely, they

can even generate physical effects. However, they lack universal effectiveness. This means that while conventional tools can be used against different targets, cyber weapons can be used only against specific targets. This is why cyber operations have a unique "*use it and lose it*" character (B. Jensen & Banks, 2021). Hence, developing unique cyber weapons for each target increases the cost of establishing an arsenal of offensive cyber capabilities (Linn, 2016).

Thirdly, even if a state can use cyber tools to escalate, its willingness to do so could be dampened by three characteristics of offensive cyber operations: *the operational need for secrecy, the difficulty of attribution, and the role of espionage* (pp. 133-137). In this regard, if a cyber-attack triggers escalation, it will diminish the benefits that the three elements of offensive cyber tools provide. Last but not least, cyber operations are not only imperfect tools for escalation in cyberspace but also reduce the probability of cross-domain escalations (pp.137-138). Cyber-attacks can cause significant economic costs on the target, and as in the case of Stuxnet, it can lead to limited physical damage. Moreover, as in the case of the alleged Iranian cyber-attack on Israeli water utilities, which intended to poison water supplies by increasing chlorine levels, cyber-attacks even endanger people's lives indirectly (Burgess, 2021; Gross, 2021). However, they have not yet produced the physical violence and horrors of conventional warfare that would trigger a strong public response to prompt decision-makers towards escalating measures - especially measures that would cross an important threshold from cyber to kinetic force. For instance, after the alleged Iranian attack on Israeli water supplies, as an act of retaliation, Israel deployed a cyber-attack that disrupted a major port in Iran. (Bergman & Halbfinger, 2020). Hence, according to (Borghard & Lonergan, 2019, p. 137), psychological and tangible costs of cyber-operation could constrain the domestic political willingness to use cross-domain instruments against adversarial cyber operations. In sum, (Borghard & Lonergan, 2017, 2019; Lonergan & Lonergan, 2023) underline that due to technical characteristics of cyber capabilities, offensive cyber operations are poor tools of escalation and unlikely to trigger escalatory responses both from cyberspace and other domains.

In addition to the problematisation of the escalation dynamics in cyberspace (Valeriano et al., 2018; Valeriano, 2022e; Valeriano & Jensen, 2019a, 2022; Valeriano

& Maness, 2014) examine the coercive effects of cyber operations. According to Valeriano et al. (2018, p.19) cyber coercion is a new tool that is used to pressure adversaries to change their behaviours; however, it is a particularly limited form of coercive action that is unlikely to produce concessions. According to the empirical findings of Valeriano and Maness (2014, 2015), while the number of cyber conflicts is increasing, most of them are low-level conflicts that do not lead to an escalation in what could be called a cyber war. This stems from what Valeriano and Maness (2015) called it *cyber restraint position* that the options of states in cyberspace have been limited and are unlikely to resort to cyber conflict. Therefore, according to Valeriano et al., (2018, p.2), what we have been witnessing in cyberspace is not a war but a limited coercive operation that aims to change the balance of information. Nevertheless, despite this limited impact, states utilise cyber tools as additional foreign policy instruments in modern strategic competition, according to Valeriano et al. (2018, pp. 7-9). As states are in constant competition, they use cyber tools in conjunction with conventional instruments, such as economic sanctions, diplomatic pressure and military threats. In other words, in contrast to the revolutionary accounts, they consider cyber tools as complementary to traditional instruments. In addition, Nadiya Kostyuk and Erik A. Gartzke's (2019, p. 3) empirical studies also support this assumption. According to their findings, cyber operations, especially disruptive ones, are mostly used as complementary tools to traditional modes of conflict. Also, they found that strong nations, with advanced technology and abundant resources, are more likely to fight opponents on land, sea, air, and space as well as in the cyber domain.

By this account, Valeriano et al. (2018, p.9) conceptualise *cyber strategy as a modern novel version of coercive diplomacy*. In contrast to military strategy, coercive diplomacy is a political and diplomatic strategy that aims to influence an adversary's will or incentives without resorting to military force (Levy, 2008, p. 539). In this respect, coercive diplomacy is a defensive strategy (George, 1994, p. 8) and an alternative to reliance on military action. Coercive diplomacy aims to persuade an adversary to stop an action already embarked upon (George, 1991, p.5). Coercive diplomacy combines "threats of force" with "limited and selective use of force", if necessary, within a controlled framework of gradual escalation. This strategy is employed as part of a bargaining strategy that also includes positive inducements. The aim is to induce an adversary to comply with one's demands or to negotiate the most

favourable compromise possible while simultaneously managing the crisis to prevent unwanted military escalation (Levy, 2008, p. 539). In this respect, coercive diplomacy seems similar to deterrence; however, according to Alexander George, it should be distinguished from it (1991, p.5). While “deterrence” uses threats to discourage an adversary from taking an unwanted action, “coercive diplomacy” is a response to an action that has already been embarked upon (George, 1991, p.5). This distinction looks similar to the differentiation of “deterrence” and “compelling” by Thomas Schelling (1966). However, there is a small and important nuance between them. While Alexander George distinguished coercive diplomacy from compellence, Schelling defines compellence and deterrence as two forms of coercion, and diplomacy and demonstration as two basic forms of compellence. Moreover, George's work on coercive diplomacy emphasises the use of threats, positive inducements and accommodations to influence an opponent's behaviour, whereas Schelling's work on compellence focuses on the use of threats to force an opponent to take a specific action (Levy, 2008, p. 540).

While Valeriano et al. (2018, p.11) acknowledge that “cyber strategy” builds upon previous works on coercive diplomacy and recent studies on cyber coercion, it is important to note that there is a significant difference: Cyber strategy does not necessarily aim to obtain direct concessions and is more likely to be executed covertly. This is because rival states use indirect cyber tools to shape long-term rivalry rather than to obtain immediate concessions. Moreover, they categorise cyber strategies into three categories: “Disruption”, “espionage” and “degradation”. While disruption and espionage focus on the shape of a rival’s behaviour in the long run, degradation is a more blunt and immediate tool of coercion (p.39). Also, according to their empirical findings, cyber degradation -which is coercive operations seeking to disrupt the networks, operations, or systems of adversaries- is more likely to have a *compellent* effect than either disruptions or espionage. However, they observed that even though degradation is the only strategy that can be coercive, they take place in limited numbers because the target is hardened or too complex to be taken down for long periods of time by malicious cyber actions (p.12). Therefore, cyber coercion is a limited form of coercion that will often fail to achieve concessions.

While Valerio et al. consider cyber operations as a new form of coercive diplomacy; on the other hand, Lennart Maschmeyer (2021a, 2021b, 2023a, 2023b) regards cyber operations as a "pure" form of subversion. Subversion is an instrument of covert operations, defined as intelligence operations involving active intervention in an adversary's affairs, rather than just passive collection of information (Maschmeyer, 2023a, p.575). It is based on exploiting vulnerabilities in opponents' systems to manipulate them to produce results not expected or intended by their designers or participants. Subversion's dependence on exploitation distinguishes it from the two classic instruments of power in the security competition, *diplomacy and warfare* (Maschmeyer, 2021a, p.54). Subversion offers an alternative to diplomacy and promises similar results with warfare at lower risk and costs (Maschmeyer, 2023a, p. 575). In other words, subversion promises a way for states to intervene in adversary affairs when diplomacy falls short of producing results, and yet at lower risks and costs than going to war (Maschmeyer, 2021a, p.61).

Subversion has a promising strategic role because of two main characteristics of exploitation: "its secrecy" and "its indirect reliance on the systems" of its adversaries (Maschmeyer, 2021a, p.54). In this respect, subversion secretly exploits the vulnerabilities in systems and their components, manipulating them to convert their advantages into harm (Maschmeyer, 2023b, p. 95). Therefore, not only the subverter's capacities and skills play an important role but also the capacities of targeted entities (or as defined as *power base*) (Maschmeyer, 2023b, p. 101). In other words, the subversion depends on targeted entities' capacities to produce effects. According to Maschmeyer, cyber operations utilise similar functional methods for reversing structural power as traditional subversion, specifically by exploiting structural vulnerabilities and utilising similar power bases to produce similar effects (Alan, (2023a, p.91). Whereas traditional subversion tries to affect social structures, cyber operations target socio-technical structures, including networked computer systems and services within societies. Accordingly, cyber operations are tools for subverting the benefits of ICTs through manipulating them to convert the advantages of ICTs into harms (Maschmeyer, 2023b, p.95) Consequently, subverter actors might have organisational capacity and hacking skills; however, without the targeted entity has no capacity, there is no way to produce an effect (Maschmeyer, 2023b, p. 101). In other

words, cyber operations are rather impractical against a Stone Age tribe that uses a stone as a weapon (Maschmeyer, 2023b, p. 91).

In addition to these similarities between cyber operation and subversion, there are also similarities in terms of the limitations. Maschmeyer (2021a, p.62) asserts that subversion is likely to fall short of what it promises in practice because of the *subversive trilemma* that limits the effectiveness and constrains the strategic utility. Cyber operations are not exempt from this trilemma. Obtaining strategic utility from cyber operations demands trading off three variables- "*operational speed*", "*intensity of effect*", and "*control*". However, these variables are negatively correlated and cause a subversive trilemma, as Figure 2.2 below shows (Maschmeyer, 2021a, p.64). In other words, improving the one variable is most likely to lead to losses of other remaining variables.

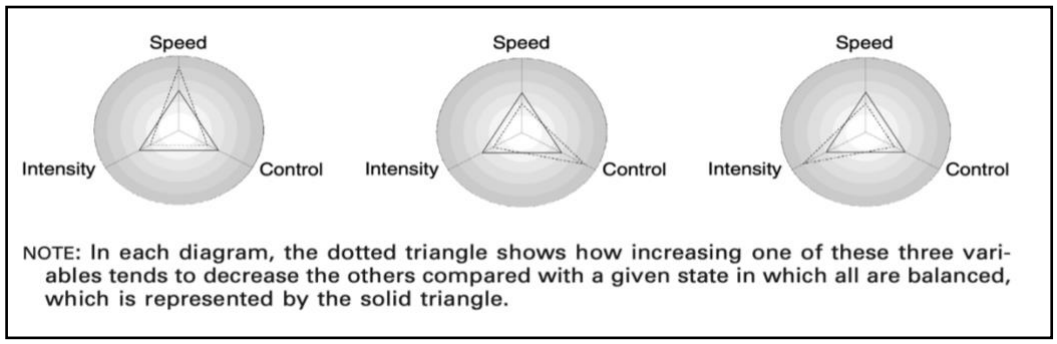

Figure 2. 2: Subversion Trilemma

Source: (Maschmeyer, 2021a, p.65)

If operational speed is increased, it could result in limited time for reconnaissance and the development of cyber tools. This, in turn, increases the risk of errors and detection of the cyber operation by the target. Increasing control requires a great amount of time for reconnaissance and development, which reduces the speed. In the same way, increasing intensity demands subverter actors to broaden the extent of access to systems and expand the cyber operation's impact, resulting in a higher risk of exposure. On the other hand, if an actor desires to expand the scope of the attack without being discovered, then the actor needs additional time, which reduces the operation's speed (Maschmeyer, 2021a, pp.64-65). In short, due to the negative correlation between these three variables, subversive trilemma falls short of cyber operations' strategic promise in practice. Therefore, Maschmeyer states that cyber

operations alone are insufficient to produce the effect that cyber revolutionists expect. Instead, they tend to be more practical when embedded in traditional subversion (2021a, p.87). Thus, the subversive trilemma offers a potential explanation for the "lack of cyber war despite 30 years of warnings" and "why cyber operations tend to be too slow, lack intensity, and unreliability to achieve political goals or shift the balance of power" (2021a, p.86-88). In this regard, Maschmeyer asserts that cyber operations represent an evolution of subversion rather than revolutionising conflict (Maschmeyer, 2021b).

Moreover, Lennart Maschemeyer et al. (2021) argued that while the potential of subversion to produce impact at the international level is limited, a significant amount of cyber operations target weaker actors – particularly civil society. States, particularly authoritarian ones, take advantage of ICT benefits in people's daily lives by turning them into harm (Maschmeyer, 2023b, p. 96). Hence, cyber conflict should also be acknowledged as a major human rights concern, rather than the prevailing conceptualisation of cyber conflict as an inter-state confrontation and international security problem. In the same way, Ryan Shandler and Miguel Alberto Gomez (2022, p. 1) also emphasised that the main threat of cyber-attacks is not cataclysmic physical destruction. Instead, the main threat is "*long-term, psychological and societal harms such as diminishing public trust in government*."

In sum, these scholars consider cyber tools as modern tools of interstate strategic competition instead of changing the nature of the military or politics. Therefore, they oppose the idea of cyber war and assert that cyber-attacks are limited tools for escalation and coercion. In this respect, they underline that there will be no such scenario in which cyber war will substitute the conventional war and cause apocalyptic results. Furthermore, these scholars paid considerable attention to the war between Russia and Ukraine. It is because Russia -which actively and effectively employs cyber tools, ultimately opted for conventional weapons instead of cyber tools. In addition, the long-expected catastrophic cyber-attacks did not materialise. In this respect, they emphasise that cyber tools possess limited capabilities, and their effectiveness can only be materialised when used in conjunction with other tools. They also challenge the view that "cyber tools are tools of the weak states" because an effective cyber-attack with serious consequences requires cost and time. Since states with cyber capabilities

also hold conventional power, cyber tools will likely shift the balance of power in favour of stronger states rather than weaker ones. In this regard, they put forward that cyber-tools are not revolutionary but evolutionary; not substitutive but complementary. However, one may ask, "Why do states still use these cyber tools excessively if their impact is limited? The following subchapter examines this question.

2.2.1. Cyber Operations as Conflict Management and De-Escalation Tools

Brandon Valeriano (2022e) calls for cybersecurity literature to move beyond the essentials. He states that the literature keeps asking the same questions: Is this attack a cyber war; is deterrence a useful strategy in cyberspace, or could cyber operations change the nature of conflict/warfare? Then, Valeriano et al. (2018, p. 13) ask that if cyber operations are unlikely to lead to political compromises between rivals, contrary to much media coverage and work in the literature, what is the role of cyber operations in international politics? In a similar question, Erica Lonergan (2022) argues that policymakers have for too long drawn the wrong lessons from cyber operations. As the Russia-Ukraine conflict has reinforced once again, the lack of escalation in decades of strategic interaction in cyberspace should lead policymakers to re-assess long-held assertions about cyberspace (Lonergan, 2022). In this respect, this chapter will examine how scholars -who consider cyber-attacks as having a limited impact- evaluate the situation in which states continue to conduct a significant number of cyber-attacks, although they mostly remain constrained.

Despite cyber operations' limited effect, Valeriano et al., (2018, p.16) assert that states keep employing cyber operations because they lack better options against rivals. In the same way, (Lonergan & Lonergan, 2023, p. 86) argues that cyber operations allow states to "do something" during a crisis, although they are poor and limited tools for signaling. However, according to these scholars, during the crisis, usage of cyber operations also can play another role: "*Escalation management and de-escalation*" (Lonergan, 2022; Lonergan & Lonergan, 2022, 2023; Valeriano et al., 2018; Valeriano & Jensen, 2019a, 2019b, 2022). In other words, they assume that cyber operations can also be de-escalation tools during the crisis".

In literature, cyber-attacks are often analysed from the perspective of coercion and escalation. In this regard, cyber tools are viewed as a contemporary form of coercive diplomacy (Valeriano et al., 2018, p. 13). Nevertheless, the role of crisis management, which is an essential part of coercive diplomacy, is often disregarded. In addition to coercive threats to encourage adversaries, coercive diplomacy also employs "rational persuasion" and "accommodation" (George, 1994, p. 7). During a crisis, crisis management is essential because no state wants the loss of control, which leads to bursting out of control into war. As Snyder and Diesing (1977, p. 207) underline, officials are not only interested in avoiding war but also in advancing or protecting their interests by minimising losses in a crisis. Hence, while accommodation and coercion are considered two different poles, they are intertwined in crisis bargaining, albeit with difficulty in finding the optimal trade-off between them (Snyder and Diesing, 1977, p. 207).

In this regard, according to Valeriano et al. (2018, p.13), cyber strategy - coercive diplomacy and political warfare customised for the 21st century- relies on *tacit bargaining* and *ambiguous signaling*. In contrast to explicit bargaining, which relies on informal or formal diplomat exchanges, tacit bargaining occurs when "*a state attempts to influence the policy choices of another state through behaviours"*.

> *"The process is tacit because actions, rather than rhetoric, constitute the critical medium of communication. It is bargaining and not coercion because the actions aimed at influencing an outcome that can only be achieved by some measure of joint voluntary behaviour"* (Downs & Rocke, 1987, p. 297).

In certain cases, states are unable to bargain explicitly. As Thomas Schelling (1957, p.19) underlines that "during the war/conflict, negotiation is severely inhibited because communication becomes difficult between adversaries". The parties may desire to resolve the crisis, but they have not yet expressed willingness to establish a formal resolution of the issue in conflict (Snyder & Diesing, 1977, p. 18). For this situation, Schelling (1957, pp.19-20) gives an example of a man who loses his wife in the store without any prior arrangement on where to meet if they get lost. For him, when wife and husband lose each other, each will think of some obvious place to meet. In the same way, states also follow the recognisable patterns when communication is difficult, alike war:

> *"The limits in limited war are arrived at not by verbal bargaining, but by maneuver, by actions, and by statements and declarations that are not direct communication to the enemy. Each side tends to act in some kind of recognizable pattern, so that any limits that it is actually observing can be appreciated by the enemy; and each tries to perceive what restraints the other is observing"* (Schelling, 1960, p. 903).

In this regard, Lonergan and Lonergan (2022, p. 33) argue that because of their limited impact, cyber-attacks may demonstrate a willingness to refrain from more harmful and costly actions that escalate the crisis in another dimension. Low-cost cyber-attacks, like DDoS, are often used to convey dissatisfaction. These cyber-attacks are useful because they do not result in a costly outcome that would cause the other side to retaliate in a painful way (Lonergan & Lonergan, 2023, p.86). Therefore, instead of military threats or displays, conveying ambiguous signals through cyber tools offers states a tool for tacit bargaining. In this respect, using cyber capabilities instead of the more costly tools in other domains can be an accommodation signal by indicating that "more violent responses are off the table" (Libicki, 2013, p.4). Consequently, instead of an escalatory form of war, cyber tools are inherently designed to abstain from war (Lonergan, 2022). In other words, using cyber operations aims to de-escalate rather than escalate a crisis (Valeriano & Jensen, 2022, p.74).

However, one may question why states opt for cyber tools to signal their willingness to de-escalate rather than resorting to alternative conventional instruments. According to Lonergan and Lonergan (2022, p. 98), cyber operations possess a unique characteristic regarding de-escalation as they enable states to take advantage of cyber operations' ambiguity and exhibit strategic behaviours in managing their public disclosure. In other words, the "*plausible deniability*" of the cyber operations allows states both ambiguity and visibility at the same time. Some covert military actions can also offer the same level of plausible deniability; however, as a main distinct point, cyber operations do not cause physical destruction and death directly. Therefore, due to the limited impact and the importance of secrecy, cyber operations possess unique signaling characteristics (p.98).

Furthermore, cyber operations target not only adversary states but also the public on both sides. In times of crisis, both sides may attempt to de-escalate rather than escalate the situation. However, in the modern era, where social media platforms are

critical in pushing states towards a more aggressive stance against adversaries, cyber operations may offer utility for states (Lonergan & Lonergan, 2022, p.33). The covert nature of cyber operations enables leaders to satisfy hawkish domestic pressure groups while avoiding more robust action that could be a catalyst for escalation (Lonergan & Lonergan, 2022, p.37; Lonergan & Lonergan, 2023, p.94). In this respect, domestic political pressures can be eased without escalating the crisis.

However, it is important to consider that the choice of the target of cyber-attacks also plays a critical role in whether a crisis escalates or de-escalates. During a crisis, the target can publicly attribute a cyber-attack to a rival or keep it private (Lonergan & Lonergan, 2023, p.98). The decision to attribute the cyber-attack or to keep it private will determine the role of the cyber operation in the crisis. If both sides keep the cyber operation private and refrain from making it public, this could create a precondition for mitigating the crisis. Nonetheless, if one party attributes the cyber-attack while the other seeks plausible deniability, it will be difficult for the attacker to offer any accommodation.

The 2022 Albania-Iran crisis is a good example of such a situation. In September 2022, the Albanian Prime Minister, Edi Rama, declared that an investigation had revealed "undeniable evidence" that Iran had recruited groups to carry out major cyber-attacks against Albania. After this acquisition, Albania severed diplomatic ties with Iran and ordered all Iranian embassy personnel to depart (Gritten, 2022). As a response, Iran dismissed all allegations and denounced Albania for severing diplomatic relations injudiciously. Many experts believe that Iran's motivation for conducting large-scale cyber attacks is mostly related to Albania's hosting of around 3,000 members of People's Mujahedeen of Iran (Mujahedeen-e-Khalq, MEK) that Iran recognises MEK as a terrorist organisation (Elezi, 2022). Furthermore, a few days after Albania severed its diplomatic ties with Iran, the Albanian leader met with Israeli officials to discuss cyber security (L. Berman, 2022). This meeting demonstrates that when one attributes the cyber attack while the other seeks to maintain plausible deniability, it becomes challenging for the attacker to offer any accommodations. Table 2.2 below demonstrates how the two parties' decisions change the cyber-attack outcome in detail.

Table 2.2: The Results of Different Responses to Cyber Attacks

	Attacking State Conceals Responsibility	Attacking State Reveals Responsibility
Target Conceals Attribution	Mutual plausible deniability prevails (even if states privately communicate knowledge about responsibility); both parties implicitly coordinate to keep attribution of cyber operations private, creating conditions for de-escalation.	Self-attribution by the attacking state creates political costs for the target; may make it more difficult for the latter to offer concessions.
Target Reveals Attribution	Public attribution by the target state creates political costs for the attacking state; may make it more difficult for the latter to offer concessions.	Public attribution by both parties makes it difficult for either side to offer public concessions; de-escalation is least likely following a cyber operation in this scenario.

Source: (Lonergan & Lonergan, 2023, p.99)

However, Brandon K. Yoder (2022) criticises these approaches, particularly Erica D. Lonergan and Shawn W. Lonergan's de-escalation assumptions. He criticises various aspects of the de-escalation approaches, but his main focus is on the impact of cyber-escalation on the domestic audience. While cyber operations may be perceived as a show of strength and may satisfy domestic pressures within attacking states, it is unclear why the target state's domestic audiences view such cyber-attacks as toothless gestures (p.759). In essence, if the signal is the same, why should the audiences of the two states perceive it differently?

Moreover, secrecy also differs based on the position of the audience. According to Lonergan and Lonergan (2022, 2023), in order to be successful in de-escalation, both sides should keep cyber-attacks private. However, the attacker informs its domestic audience about the attack to satisfy public opinion while leaving the target government unaware or uncertain. Yoder (2022, p. 760) problematise the nature of this approach. For instance, if the targeted state chooses not to attribute the attack and keeps it private, how can the attacker's public have confidence in tracing the cyber attack? In other words, if the attacker's domestic audience can trace the cyber attack, what prevents the target's audience from keeping track of cyber operations? This problem about theory also brings a question about the role of ambiguity. It is unclear how an attacker state can claim responsibility for a cyber-attack to its domestic audience in

order to gain credit while at the same time relying on plausible deniability of its responsibility for the attack to the target state's public, according to Yoder (2022, pp. 760-761). Therefore, keeping cyber-operations secret and signaling strength to the domestic audience of attackers at the same time contradict each other.

Lastly, Yoder (2022, p.763) also criticises the given cases as an example of de-escalation. Cyber attacks cannot be attributed as the sole cause of crisis de-escalation when de-escalation would have occurred anyway. For example, after the following days, the Türkiye shot down the Russian Fighter Jet, Türkiye witnessed noteworthy cyber-attacks in terms of both number and impact. More than 400,000 websites, including government institutions, were brought down (Murgia, 2015). However, the crisis between the two countries did not escalate into war and remained limited. These cyber-attacks are regarded as Russia's desire not to escalate, and Türkiye's decision to keep these cyber-operations private seems de-escalatory. However, as Yoder (2022, p.763) emphasised, the crisis was settled with a formal apology from Türkiye a month later. This means there is no empirical evidence that cyber-attacks play a de-escalatory role within the crisis; de-escalation would have occurred anyway.

The underlined points of the Yoder are important, and his critics should be given great attention. Indeed, the problematisation of domestic politics and plausible denial need additional revision by scholars. However, the choice of the cyber-attack rather than the conventional military option itself can also be regarded as de-escalation behaviour. For instance, Ukraine has been targeted by Russian cyber-attacks for years. However, the escalation was limited until 2022, when Russia opted for conventional weapons. Also, one of the most mentioned examples in the literature, the US-Iranian crisis in 2019, demonstrates how leaders choose cyber weapons as an alternative to conventional weapons to manage the escalation.

In May and June of 2019, there was a significant increase in tension between Iran and the United States, resulting in a militarised crisis. On 6 May, the former US National Security Adviser, John Bolton, announced that the US had sent an aircraft carrier and bomber task force to the region to send a direct message to the Iranian regime (BBC News, 2019a). During May and June 2019, tankers were attacked in the Gulf, and the US blamed those attacks on Iran while Iran denied all the accusations

(Wintour & Borger, 2019). These attacks were seen as a part of the Iran-Saudi Arabia conflict in the region because two of the oil tankers belonged to Saudi Arabia's Aramco Company (Wintour, 2019a). Moreover, Iran-backed Houthi rebels (Juneau, 2021) conducted several attacks on Saudi's oil infrastructures (Kalin & El Gamel, 2019) and Saudi international airports (Wintour, 2019b). While the tense situation in the region had been continuing, the crisis reached a peak point with the shot-down of a US drone by Iran. US officials stated that during the US surveillance aircraft's mission, there was no provocation, and it had not violated Iranian airspace at any time (Garamone, 2019). As a response to this action, former US President Donald Trump decided to conduct an airstrike on Iran. However, he backed down from the airstrike decision because he acknowledged that responding with airstrikes in retaliation for shooting down a drone would be disproportionate. He wrote on X, formerly Twitter, that:

"On Monday they shot down an unmanned drone flying in International Waters. We were cocked & loaded to retaliate last night on 3 different sights when I asked, how many will die. 150 people, sir, was the answer from a General. 10 minutes before the strike I stopped it, not proportionate to shooting down an unmanned drone. I am in no hurry, our Military is rebuilt, new, and ready to go, by far the best in the world. Sanctions are biting & more added last night" (Margolin et al., 2019).

Even though Donald Trump backed away from conventional strikes, US officials stated that US military cyber forces launched a strike against Iranian military computer systems to disable the controlled rocket and missile launchers with the approval of Donald Trump. Accordingly, this decision is regarded by some experts and scholars as "an off-ramp from a kinetic response that might have led to further escalation" (Pomerleau & Eversden, 2019). In addition, Valeriano and Jensen (2019b) claim that Trump's decision also proves that national security decision-makers are increasingly turning to cyber responses because cyber operations allow leaders to preserve flexibility and give an off-ramp to war. In order to test this trend, Jensen and Valeriano (2019) conducted an experimental study that included war games and simulations with 295 participants, including graduate and undergraduate students from IR-related programs, government and military officers, and private sector employees. According to their findings, when participants were faced with a militarized crisis and given multiple response options, their choice of cyber responses was found to de-escalate conflicts, (Jensen & Valeriano, 2019, pp. 18-22) as was observed in the Iran-US crisis in 2019.

In sum, two aspects of cyber operations - producing limited effects and providing plausible deniability - serve as accommodating signaling. This advantageous aspect of cyber operations enables states to maintain bargaining leverage while simultaneously signaling an unwillingness to escalate. In this respect, Valeriono and Jensen (2022, p.87) even claim that cyber operations have less potential risk as off-ramps to the first confrontation. However, this does not imply that cyber operations alone can lead to peace. Instead, they can be used as tools for avoiding war and moving toward peaceful resolutions (Valeriano & Jensen, 2022, p.66, 87). However, some scholars argue that just because a single cyber attack does not lead to war does not mean that cyber tools are limited. Cyber attacks individually are not revolutionary, but the cumulative effect of limited cyber attacks may change the balance of power. Therefore, one can ask: "What if states deliberately limit themselves to increase the cumulative impact of cyber-attacks in the long term? The next chapter will attempt to answer this question.

2.3. Standalone Role of Cyber Tools: Shifting the Balance of Power Without Military Action

In the previous chapters, it was discussed that scholars and experts generally evaluate cyber-attack's impact via whether it causes physical impact or not. While scholars in the first group consider cyber-attacks that bring a revolution in military affairs and warn against possible impacts of cyber-war, on the other hand, scholars in the second group assert that cyber-attacks are limited tools because they neither cause escalation nor impact. In addition to these two groups, there is another group of scholars who perceive cyber tools as new "*standalone tools"* (Maschmeyer & Kostyuk, 2022) that can change the balance of power between states without resorting to the use of force.

In this regard, Ben Buchanan (2020, p. 8) argues that comparing cyber tools to nuclear and conventional weapons is misleading because cyber tools are neither as powerful nor as reliable as conventional and nuclear weapons. However, they can shape the future of the world for better or worse (p.9):

> *Rather than…apocalyptic vision, however, cyber-attacks have become a low-grade yet persistent part of geopolitical competition. They happen every day. Government hackers play an unending game of espionage and deception,*

> *attack and counterattack, destabilization and retaliation. This is a new form of statecraft, more subtle than policymakers imagined, yet with impacts that are world-changing* (Buchanan, 2020, p. 3).

Similarly, Richard Harknett and Max Smeets also criticise the previous two approaches. They contend that scholars should evaluate cyber-attacks through the prospect of achieving strategic goals without resorting to the use of force. Accordingly, they argue that war and coercion are not the only options because cyberspace has enabled a new mechanism of power politics for states to gain a strategic advantage: Cyber campaigns - that consist of a large number of low-level cyber-attacks- rather than a single devastating cyber-attack have a potential to shift the balance of power (on a bilateral, regional or international level) in favour of the cyber campaigner (Harknett & Smeets, 2022, pp. 535-543). The conceptualisation of the strategic advantage through cyber campaigns needs an additional explanation because, in the literature, hacking, cyber operation and cyber campaign are interchangeably used for cyber-attacks. However, all these terms have different meanings, and these differences play a major role in (mis)conceptualising cyberspace. To perceive the third school's approach accurately, especially about the cumulative impact of cyber-operations, the recognition of the distinctions between these terms is crucial.

The cyber operation is a process that includes different coordinated actions, from targeting actors gaining access to exfiltration directed at the target's computers or network devices to achieve a specific objective (Monte, 2015). Depending on the objective, target, device and network, the types of cyber operations may also change. If the objective is to obtain an unclassified document, cyber espionage operations can be carried out. If the aim is to disrupt the flow in a system, a disruption or DDoS type of cyber operation can be carried out. On the other hand, a cyber campaign is a set of coordinated cyber operations conducted over time to achieve a cumulative result that provides a strategic advantage (Harknett & Smeets, 2022, p. 541). Since cyber campaigns contain different types of cyber operations that target different actors through different tools, their success should be evaluated according to their long-term impacts. Suppose the primary objective of a cyber campaign is to neutralise a rival country's defence systems and gain a strategic advantage in the event of a possible conflict. In this context, a limited cyber espionage operation directed at a hotel would be considered irrelevant. However, the objective of this espionage attack might be to

obtain the personal details of the person who works as an assistant in the security company that is responsible for the military computers. By discovering this person's bank account, their electronic devices can be traced, and another cyber operation can be carried out. It is important to remember that many successful cyber-attacks result from basic human mistakes. By identifying an individual's preferences and vulnerabilities in any subject, a simple phishing email can be used to gain access to a military network. Although this may seem an exaggerated story, it is nevertheless significant in illustrating how different actors' separate, unrelated cyber operations against different targets can be part of a single cyber campaign.

Moreover, Max Smeeth (2018) emphasises that to grasp the strategic value of offensive cyber operations, it is helpful to distinguish between countervalue and counterforce cyber capabilities. While counterforce cyber capabilities are designed to target the military operations of adversaries, counter-value cyber capabilities target vital assets of the adversaries (p.94). This distinction is important to understand the cyber offensive's psychological impact on the target. The psychological impact of cyber operations does not stem from a fear that conventional weapons do; however, it is because of humiliation and confidence degradation (Smeeth, 2018, p.101). Max Smeeth argues that Stuxnet, often considered the most sophisticated cyber-attack due to its ability to cause physical damage, in fact, damaged Iran psychologically more than physically. In other words, Stuxnet was designed to cause damage as well as to embarrass the Iranians by revealing to the world how vulnerable Iran's most protected infrastructure actually is.

However, Stuxnet marked a turning point for Iran because Iran drew crucial lessons from the attack. According to Boaz Dolev and David Siman-Tov (2022), Iran has been conducting cyber-operations against Israel to produce a psychological effect. Iranian-affiliated cyber actors carry out numerous low-level cyber-attacks and publicise them via social media accounts. Through these attacks, Iran intends to induce fear in the Israeli public that the government cannot provide adequate security and that Iran may launch more serious cyber-attacks in the future. Thus, Iran's strategic objective is to pressure the public and thereby influence Israeli decision-makers and the ongoing conflict between Israel and Iran (Dolev & Siman-Tov, 2022).

These cases provide a striking example of why evaluating the impact of cyber-attacks through their physical effects, whether they escalate or cause damage similar to conventional weapons, leads to a misinterpretation of the strategic value of cyber tools. Harknett and Smeets (2022, pp.549-550) give a good example of this misinterpretation: If we only consider cyber activities in the context of cyber war, then China should be regarded as the "most peaceful" cyber power. In contrast, China has been a proactive actor, conducting a wide range of low-intensity cyber operations to achieve its strategic goal: Changing the balance of power in the international system. This change does not require military intervention and is achieved through limited, low-level cyber-attacks akin to Chinese torture methods - *death by thousand cuts*. Shifting the focus from conflict to strategic competition provides a different perspective on China's cyber behaviour. According to Ben Buchanan (2020, p.7), it must be examined operations and their cumulative strategic impacts to understand contemporary statecraft. This is similar to a boxing match. A boxer can win by scoring more points without knocking out his opponent. This is why Harknett and Smeets (2022, p.558) stress that cyber tools should not be seen as enablers of war (even though they have potential) but rather as a strategic alternative to it. Therefore, Fischerkeller et al. (2022) suggest that policymakers should approach planning with a "campaign mindset" instead of focusing on individual cyber operations.

There are different assumptions regarding the role of cyber tools among the scholars in the third group. However, the common assumption of these scholars about cyber tools is that they are neither a complement to force nor revolution in military affairs but a standalone strategic tool. "Cyber Persistence Theory" (CPT), which is articulated by Richard J. Harknett and Michael P. Fischerkeller, frames the main assumptions of most of these scholars. In this respect, it offers a structured explanation of cyber-tools' role. Moreover, the states have adopted assumptions of the Cyber Persistence Theory. For instance, the United States adopted *cyber persistence* as a national cyber strategy in 2018 instead of deterrence and restraint (Maschmeyer, 2020). Moreover, in the 2022 National Cyber Strategy, the United Kingdom also adopted the theory's paradigms (Harknett et al., 2023). The adoption of the same strategy by the US and the UK demonstrates the popularity and analytical power of the CPT (Harknett et al., 2023). In this respect, more attention should be given to

understanding how states use cyber-tools in the contemporary era. For all these reasons, the “Cyber Persistence Theory” will be discussed in the following sub-chapter.

2.3.1. Cyber Persistence Theory

Cyber Persistence Theory, as does Neo-Realism in IR, adopts a system level of analysis to explain the behaviour of states in cyberspace. As a structural theory, its proponents first draw a structural framework of cyberspace. Fischerkeller et al. (2022) argue that technological developments have a central role in political/military tactics and strategies; however, not all of these developments result in a significant change in the strategic structure of security. According to them, what distinguishes the strategic structure of the environment is "not the technology itself, but how the technology shapes the concept of security" (2022, p.10). In this respect, it is asserted that cyber technologies are not merely new tools of statecraft; they are also transforming the concept of security itself. Consequently, the structural environment of cyberspace differs significantly from the two other existing environments, namely, the conventional and nuclear environments. While security paradigms of conventional and nuclear weapon environments rely on warfighting and deterrence, cyberspace relies on a different logic.

Conventional strategic environment- predominated throughout history- is primarily based on the alignment of strategy to relative advantage or disadvantage by engaging in defensive (protecting) and offensive (extending) control of the unevenly distributed power sources. Also, the power source relies on the territory (energy sources, waters, populations, lands, etc.). Therefore, control over power sources determines relative security (Fischerkeller et al., 2022, pp.12- 14). As power is distributed unevenly, an increase for one diminishes others, resulting in the "*tragedy*" described by Mearsheimer (2001). Thus, states' security in a conventional strategic environment depends on their ability to handle the relative advantages of offence and defence. However, the advent of the atomic bomb marked a fundamental change in the conventional strategic environment. Brodie et al. (1946, p. 76) announced this fundamental change with the following statement: *Thus far, the chief purpose of our military establishment has been to win wars. From now on, its chief purpose must be to avert them. It can have almost no other useful purpose”.* In this new strategic

environment, the focus shifted from winning wars to achieving security without absolute defence. This implies that security is no longer in our hands but in the minds of our adversaries (Fischerkeller et al., 2022, p. 16). As a result, in the context of nuclear strategic deterrence, states must persuade their opponents not to attack, as there are no reliable weapons to prevent the consequences of a nuclear attack. So, this mindset demonstrates how the concept of nuclear deterrence was born and implemented during the Cold War. In this context, Fischerkeller et al. (2022, p. 16) argue that deterrence should be a structural necessity. Deterrence was a necessary security strategy because the defence no longer provided adequate security.

Since then, the two strategic environments have coexisted, with only a limited number of states having to manage both simultaneously (p.21). However, seven decades ago Bernard Brodie announced the new strategic environment; today, (Fischerkeller et al., 2022; Fischerkeller & Harknett, 2017) announced a new one: *Cyber Strategic Environment*. They contend that what happened in and through cyberspace cannot be explained with the logic of existing two strategic environments-offence/defence, deterrence, coercion, or warfare (in terms of both military and political warfare). States' behaviour in cyberspace does not start with the aim of changing the behaviour of other states but with *exploiting* the inherent vulnerabilities of cyberspace. Therefore, this new environment is not a space of coercion but an exploitation. Each state aims to enhance its security by exploiting vulnerabilities that enable states to gain access, manipulate, and ultimately control without direct exchange, coercive shaping of behaviour or, most importantly, without war. Hence, the cyber strategic environment rests in neither the presence nor absence of war but in the alternative to war through the cumulative impact of the constant exploration of others (Fischerkeller et al., 2022, p.21-26; Fischerkeller & Harknett, 2017, pp. 385–388). In this regard, they criticise the efforts of scholars and policymakers to explain this new dimension with the existing strategies of two previous strategic environments. Instead, a new theory is required for a cyber strategic environment, and they offer *Cyber Persistent Theory.*

As anarchy is the main structural feature and ordering principle of the international system for Neo-Realism (Waltz, 1979, pp.88–93); Cyber Persistent Theory premises that the core structural feature of cyberspace -the sociotechnical

environment- is *interconnectedness.* It is a core feature because structurally, all states are in a *condition of constant contact* with all other actors (Fischerkeller et al., 2022, p.35, 119). According to proponents of the theory, constant contact is not a policy choice but a necessity resulting from an interconnected world. In addition to these features, there is also reinforcing structural feature: Core technical features such as a vulnerable and resilient technological system. The combination of the interconnectedness, condition of the constant contact and reinforcing structural features forms the basic distinct logic of cyberspace: *Exploitation.* Therefore, so as to achieve security, the strategic cyber environment constitutes a form of strategic behaviour as "*persistent engagement*" (Fischerkeller et al., 2022, p. 35). Persistent engagement refers to continuously engaging and challenging adversaries while manoeuvring for strategic advantage within cyberspace by intentionally remaining below a threshold (Fischerkeller & Harknett, 2018). In this regard, the activities below the level of armed conflict (it can also be referred to as activities within the grey zone) are not an anomaly but a sign of the emergence of a new competitive space where there is no agreement over what unacceptable or acceptable yet (Fischerkeller et al., 2022, p. 124).

However, it should be noted that for the Cyber Persistent Theory, states' self-restraint in using cyber tools does not stem from the fear of retaliation or coercion but rather from the possibility of reward. Cyberspace is full of vulnerabilities; therefore, unilateral exploitation is a primary motivation for states to carry out cyber operations below the armed attack threshold. Additionally, despite different missions, states exhibit similar behaviour, which is exploiting the vulnerabilities of others whilst reducing their own (Fischerkeller et al., 2022, p.38, 43). In this respect, the primary behaviour of the states is the cyber *fait accompli,* which is limited unilateral gain at the expense of an adversary that is unwilling, unable or unaware to respond to the loss (Fischerkeller, 2020). According to Dan Altman (2017, p. 882), *"fait accompli*" aims to secure a small gain that the opponent can concede rather than escalate. Therefore, the crucial point of fait accompli is calculating the extent of the loss that the defender is willing to tolerate. For instance, whereas Argentina's attempt to seize the Falkland Islands backfired, Russia's 2014 annexation of the Crimea Peninsula is a successful example of the fait accompli (Kofman, 2020). Thus, according to Altman (2017), fait accompli and coercion are distinct strategies to gain an advantage over an adversary:

While coercive methods force the adversary into accepting a concession reluctantly, the faits accomplis are unilaterally acquired without the consent of the adversaries. In this regard, Fischerkeller et al. (2022) draw similar assumptions and claim that the logic of coercion does not fit cyberspace but the fait accompli that can alter the balance of power in the international system through cumulative impact in the long term.

While states primarily engage in cyber fait accompli behaviour, Fischerkeller et al. (2022, p.44) contend that this does not rule out mutually dependent behaviour, which they call *direct cyber engagement.* This cyber behaviour is a mutual confrontation for control of critical cyberspace terrain where both states consider it as strategically, operationally, or tactically significant for their securities. As cyber fait accompli, direct cyber engagement is exploitive short of armed- attack; however, it is secondary and scarce in cyber engagement. The scarcity of direct engagement stems from the situational awareness of the states in which they are aware of the abundance of opportunities for *faits accomplsi*. Therefore, they refrain from direct engagement (Fischerkeller et al. 2022, p.45). Moreover, direct cyber engagement could also be used to show that certain behaviours are unacceptable. Through continuing direct engagements, states can meet based on a mutual understanding of acceptable and unacceptable behaviours. In this respect, direct cyber engagement can be used as a tacit bargaining between states while the tacit coordination characterises the cyber faits accomplis (Fischerkeller et al. 2022, pp. 55-56). Therefore, this distinction between these two prominent behaviours in the strategic cyber environment is crucial to understanding how states can construct "cyber norms" (Fischerkeller et al. 2022, p.45; Fischerkeller & Harknett, 2019, p. 273). Although cyber activities used for tacit bargaining (direct cyber engagements) are rare cases, Fischerkeller and Harknett, (2018) emphasise that states should adopt the tacit bargaining approach to enhance the prospect of a more secure and stable cyberspace.

Last but not least, cyber faits *accomplis* and direct engagements as competitive interaction also produce an interstate phenomenon of cyber-agreed competition (Fischerkeller et al. 2022, p.50, 56). Although it is a distinct concept, it is built upon the concept of *agreed battle* (or limited conflict) coined by Max Singer but prominently developed by Herman Kahn (1968). Agreed battle emphasises a particular level of escalation or specific situation between the parties of the conflict (Kahn, 2010,

p. 5). In an agreed battle, there is an agreement between parties to the conflict over what is legitimate and illegitimate behaviour, what is an escalation behaviour and what is within the rules (Kahn, 2010, p. xiii). This is a try to explain the proxy war between the United States and Soviet Union. By agreeing to compete in the proxy war, they refrained from spreading a nuclear war. However, (Fischerkeller et al., 2022, p.49) argue that while states limit themselves in the conventional and nuclear environment for fear of escalation, on the other hand, they limit themselves in cyberspace for a different reason: *Reward*.

Nevertheless, the Cyber Persistent Theory is also not exempt from the criticisms. With the US and the UK adopting persistent engagement as a national cyber strategy, the theory has received significant critical reactions from the literature. Many of them target the "continuous exploitation of the vulnerabilities" and urge that it will lead to escalation rather than stability in cyberspace. From this perspective, Jason Healey (2019, p. 12) contends that "persistent engagement places military and intelligence forces in close contact", actively competing with each other. Countries have different understandings, and there is always a chance of miscalculation. This dominant strategy might have explosive consequences. Therefore, constant contact is "new and highly risky", and it can trigger a "*New Forever War"* (Healey, 2018). In addition, Max Smeets (2019) highlights the potential for new friction arising from adopting this persistent engagement as a cyber strategy. He argues that long before the introduction of persistent engagement, the US has been operating in networks close to adversaries. However, the US has become an active disrupter with a persistent engagement strategy. Even without consent, the US may act within allied networks to achieve this objective. For instance, to remove ISIS propaganda, the US conducted an operation on a server in Germany without obtaining advance consent from Germany. In the case of Germany, even if the mission is successful, it could create unintended friction with the Allies. Therefore, Smeets (2019) believes that this strategy carries a genuine risk of eroding the trust and confidence between allies.

Moreover, Lennart Maschmeyer (2020) asserts that the theory relies on incomplete and flawed logic". According to Lennart, assessing 'interconnectedness' as a key structural feature is flawed because actors are not forced but free to choose to be in cyberspace. Therefore, actors themselves determine their level of

interconnectedness. To limit their exposure, they can choose to disconnect for either a short or long period. Secondly, and most importantly, Maschmeyer (2020) argues that CPT neglects the role of "secrecy". Actors can engage in cyber activities below the threshold of conflict not due to interconnectedness but because secrecy enables states to avoid escalation. Hence, according to Maschmeyer (2020), information technologies do not create a new strategic environment but provide new tools for states to compete under secrecy.

In response these criticisms, Fischerkeller et al. (2023) point to the Russian-Ukrainian war. They argue that although Russia has exceeded the limits of agreed competition by attacking Ukrainian critical infrastructures, Russia has not targeted non-belligerent states in a similar way. Russia is still seeking strategic advantage but seems aware of the escalation risks. Moscow's restraint indicates that there are still tacit limits, even in the presence of armed conflict. Also, as a response to interconnectedness criticism, Fischerkeller et al. (2022, p. 31) claim that disconnection is not a "*sustainable solution*" because this method prevents one from benefiting from the advantages of cyberspace. They also noted that interactions between states, companies and people continued even during the war, as witnessed in the Russia-Ukraine war (Fischerkeller et al., 2023).

In conclusion, the CPT is a novel strategic approach that seeks to explain state behaviour in cyberspace from a structural standpoint. CPT primarily argues that the structural logic of the conventional and nuclear environments remains limited in explaining the cyber phenomena. Instead, cyber activities should be evaluated from the lens of a new strategic environment – a strategic cyber environment. Through assessing the cyber-activities from this respect, it can be recognised that the primary behaviour of the cyber-activities is exploitation rather than coercion or war. Exploitation is the primary behaviour because the new environment is abundant with technical vulnerabilities, and it provides states an opportunity to achieve their objectives without resorting to war. This situation incentivises states to engage in a cyber-agreed competition through persistently engaging in exploitive behaviour- cyber faits accomplis and direct cyber engagements. As a result of this persistent engagement with adversaries for the advantage of the grey zone, CPT assumes that these behaviours will facilitate a strategic process of tacit bargaining about what is acceptable and

unacceptable behaviour. Then, this exploitative behaviour will provide stability and security in cyberspace in the long term since it indicates what is acceptable and unacceptable behaviour. In other words, exploitative behaviour will eventually lead to the construction of cyber norms and a more secure and stable cyberspace (Fischerkeller & Harknett, 2018).

Thus, CPT presents a structural assumption and a constructivist stance. However, as with any theory, it is also not exempt from criticism. Following the adoption of persistent engagement as a national cyber strategy by the US and, subsequently, the UK, CPT has received considerable criticism in the literature. The majority of criticisms are directed at the assumption of "continuous exploitation of vulnerabilities" and claim that this exploitative behaviour will lead to escalation between states (even allies) rather than stability in cyberspace. Additionally, some criticisms target the basic conceptualisation of the theory based on interconnectedness. Despite these severe criticisms in the literature, the acceptance of the strategy by the US and the UK indicates that at least this theory is becoming more widely accepted among policymakers. Therefore, further discussions about this theory is required in the literature. Accordingly, this study also aimed to address the fundamental assumptions of this theory, albeit to a limited extent.

2.4. Revisiting the Roles of Cyber-Tools Through the Trilateral Relations Lens

In the previous chapters, the different roles of cyber tools in interstate relations were discussed based on the assumptions of three groups of scholars. Although each group's proponents have a different perspective, a classification relies on the broadest common point that brings scholars, experts, and policymakers together. In this respect, the common point of the first group is the assumption that "cyber-attacks are changing the nature of war" and "have led to a revolution in military affairs". Because it is revolutionary, they stress that a new war - cyber war - is on the horizon and that states are not ready for this new war. Therefore, they argue that cyber war would substitute for conventional war, and cyber tools could change the balance of power in the international system. On the other hand, the second group opposes the concept of cyber war, stressing that there is no scenario in which cyber war would replace substitute conventional war and have apocalyptic consequences. On the contrary, cyber tools are

rather limited in terms of escalation and coercion, and cyber tools become effective when combined with other traditional tools. From this perspective, they argue that "cyber tools are not revolutionary but evolutionary; not substitutive but complementary". Moreover, some of the scholars in the second group assert that cyber tools are being used as conflict management tools. They argue that the main motivation for states to choose a limited-effect cyber-attack instead of a conventional weapon is to primarily prevent the escalation of conflict while at the same time eliminating critics of "nothing is being done" from the domestic audience.

Lastly, the proponents in the third group assume that cyber tools are new standalone tools that can change the balance of power between states without using force through the cumulative impact of short-of-war cyber-attacks. One can argue that this group of scholars is similar to the first group's view of cyber-attacks as revolutionary because they assume that cyber-tools are standalone tools that substitute conventional war and change the balance of power. However, there is an important distinction: Contrary to the first view, the third group claims that cyber-attacks are not tools that can lead to cyber war. Cyber-attacks are short of war and states intentionally limit themselves to increase the rewards. Also, they disagree with the notion that cyber tools are limited because they do not lead to war or conflict. Their viewpoint is that such a perspective is misguided because evaluating cyber-attacks based on their physical effects can misinterpret the behaviour of states. Instead, they propose evaluating the long-term cumulative effects of cyber-attacks instead of analysing their individual effectiveness. It is because the cumulative impacts of cyber-attacks can alter the balance of power in the international system. Furthermore, although it does reflect all the proponents of the third school and is even criticised by some of them, the Cyber Persistence Theory is the most structured account of the third group. CPT argues that all states are in *constant contact* with each other in the *interconnected* environment and persistently exploit the vulnerabilities for their political purposes. This persistent exploiting behaviour provides strategic advantages to states in the long term and can even change the balance of power. Moreover, as this exploitative behaviour sets the standards for acceptable and unacceptable conduct, proponents of the theory even argue that these cyber activities will ensure stability and security in cyberspace in the following years.

As seen from these discussions, there are numerous and contradicting views about cyber tools' role in the literature. Each perspective sheds light on the different aspects of the cyber-tools. For instance, when the role and impact of cyber tools are evaluated through the lens of the war, claiming that cyber tools are limited appears to be a reasoning. As in the case of the Russia-Ukraine War, parties have not yet employed cyberattacks as a substitute for conventional tools in the conflict. On the other hand, cyber tools can be functional in political terms and even indirectly lead a state to launch a military operation. For instance, as discussed in the previous chapters, the tension escalated between Iran and Albania over a series of cyber-attacks. It had such a disturbing impact on Albania, and it severed diplomatic ties with Iran. Therefore, evaluating cyber-attack effects solely from a war perspective may lead to incomplete/incorrect interpretation of states' behaviours in cyberspace.

Moreover, it is worth noting that all these approaches share the common ground that states have been using cyber tools to gain an advantage over their rivals. Their perspectives differ about the methods of gaining that advantageous position. Accordingly, scholars in the third group argue that each state tries to exploit cyberspace's vulnerabilities to its advantage, just as states tried to explore the resources of the undiscovered ocean in history. However, it can be challenging to analyse the role of the cumulative impact of cyber-attacks. For IR experts, it is not unexpected to witness a situation in which a country gains enough power to shift the balance of power within the international system and launch a Hegemonic War, as conceptualised by Robert Gilpin (1988). However, assessing impacts of cyber-attacks on the balance of power is challenging if there is a gradual shift through persistent exploitation. In other words, how can the role of other traditional tools -such as economic, political, and diplomatic- be ignored, and only the role of cyber-attacks can be evaluated? Therefore, although the cumulative effect is a rational approach, it is challenging to assess. Additionally, just as no cyber tools were available to states 50 years ago, there may be a new tool that will make people forget cyber tools in the following years. However, one thing remains the same: regardless of a new tool, states will continue to use it as an additional instrument alongside existing ones to achieve their objectives.

Accordingly, in this study, "*cyber tools are considered as evolutionary and complementary tools"*, rather than revolutionary and substitutive tools of war, as the second group suggests. In other words, *cyber-attacks are considered contemporary tools of statecraft that are used alongside other tools in a tailored manner to accomplish a country's particular objectives.* However, in contrast to the analysis of individual cyber-attacks, this study, similar to the third school of thought, will also adopt the perspective that cyber tools should also be examined based on their long-term use in interstate relations. In this respect, states may employ cyber-attacks in various ways, including a) exploiting to gain a long-term advantage without resorting to force, b) as a coercive diplomatic tool in response to an undesired situation caused by an adversary state, and c) to inflict damage on an adversary in the event of war. An analysis of open-source datasets (Valeriano, 2022; Center for Strategic and International Studies, 2023; Council on Foreign Relations (CFR), 2023) also underlines the fact that states use different forms of cyberattacks against different targets at different times and for different purposes.

When these data sets are examined, another factor can also be noticed: The majority of cyber-attacks occur between rival states within the same region or when a state out of the region interferes with regional affairs. If we consider the great powers as actors in a region where they operate beyond their territories, either by forming alliances or the presence of the military, the regional scope of cyber-attacks even more expands. For instance, when assessing the relations between the United States and Iran, taking into account the US as an actor in the Middle East would significantly amplify the role of cyber-attacks in the regional dimension. According to Stephen Walt (1985), states seek to balance perceived threats, with geographic proximity as a key factor in shaping those perceptions. Similarly, Barry Buzan and Ole Weaver (2003, p.11) argue that political and military threats travel more easily over short distances, thereby linking insecurity to proximity and the tendency for states to fear their neighbours more than distant powers. It is also possible to extend their view through including that states feel more threatened by a great power when it intervenes in their regional affairs. In this respect, even if cyberspace is a dimension with no geographical limitations or physical limits, the datasets demonstrate that cyber-tool usage is also shaped by regional mindset. Moreover, the fact that cyber-attacks are used in a regional framework also indicates that hybrid tools such as cyber-attacks are not used by

revisionist states in their systemic struggle, but as a foreign policy tool in regional and bilateral level. In this regard, as Lonergan and Lonergan (2023, p. 111) and Valeriano et al. (2018, p. 6) argue, this study also posits that *"cyber tools are utilised as foreign policy instruments by states, especially in regional affairs, to coerce and leverage concessions, with the eventual goal of gaining a strategic advantage over rivals".*

Furthermore, it is important to note that a third party may become the target of cyber-attacks or may be responsible for carrying them out due to the existing tension between the two states. For instance, the tension between the US and Iran may lead to Iran directing cyber-attacks toward the US's regional allies, like Israel or Saudi Arabia, instead of directly targeting the US. Furthermore, two states' rapprochement may be interpreted by a third as a potential threat, leading to retaliatory cyberattacks on both states. For example, following the diplomatic rapprochement between Saudi Arabia and Israel, it is reasonable to expect a decrease in the number of cyber-attacks between the two countries. However, this rapprochement could be perceived as a potential threat by Iran, and both Saudi Arabia and Israel could find themselves in Iran's targets. In this regard, the two countries' relations and the number of cyber-attacks they faced are influenced by various factors, including region-specific factors, the distribution of power in the region, and the historical amity-enmity relationships among states. Therefore, when case studies or quantitative research examine the effect of cyber tools through the dyadic relations of rival states, the role of the third countries, especially the strategically important ones for both rival states, should be included in the analysis.

This research examines how "usual suspects" – Russia, China and Iran –utilise cyber disruption operations as instruments of foreign policy, particularly as a form of tacit bargaining, against the United Kingdom (UK) when the UK increases its cooperation with Ukraine, Hong Kong, and Israel, which are strategic actors for both the UK and the "usual suspects", will be examined. By examining these relations, this study will test the following hypotheses:

H1a: *As the level of conflict between two rival states increases, the likelihood of utilising cyber-disruption operations as a tool of hybrid threat also increases.*

H1b: *There is no relationship between the level of conflict between two rival states and the likelihood of utilising cyber-disruption operations as a tool of hybrid threat.*

H2a: *When one of two rival states increases its cooperation level with a strategically important third country for both rival states, the likelihood of the other rival state launching cyber-disruption operations against its rival increases.*

H2b: *There is no relationship between one of the two rival states increasing its level of cooperation with a strategically important third country for both rival states and the likelihood of the other rival state launching cyber-disruption operations against its rival.*

In the next chapter, the methodology for testing these hypotheses will be explained in detail. In addition, based on results of these hypotheses, how an early warning system for politically motivated cyber-attacks can be developed, will also be discussed in the next.

3. METHODOLOGY: COMPREHENSIVE APPROACH FROM DATA COLLECTION TO ANALYSIS

> *"Once upon a time the expert in International Relations (IR) did not need many skills beyond an ability to speak with suavity and distinction in more than one language and to know a bit of the history and customs of a few countries besides his own. But times have changed and now the student of IR should be not only a gentleman and a scholar but also, of all things a scientist"* (Deutsch, 1958, p. 278).

This study uses "quantitative research methods" to examine how the UK's trilateral relations with "Russia-Ukraine", "China- Hong Kong" and "Iran-Israel" affect the likelihood of cyber disruption operations being used against the UK as a modern foreign policy instrument. Quantitative methodology principally collects data and uses statistical analysis techniques to test related hypotheses or theories (Mertler, 2021, p. 107). This basic definition underlines two important factors in quantitative research: "*Data*" and "*Analysis*". Therefore, this chapter will explain which data will be used, from which sources and how these data will be collected, and the methods for analysing those data. In this regard, this chapter will first discuss which kind of cyberattacks will be used collected. As mentioned in the previous chapters, there are different kinds of cyber-attacks. Classifying all these activities in the same category and analysing them through the same perspective could lead researchers to inaccurate conclusions. Each cyber-attack is executed using distinct methods and employed by various threat actors with varying motivations. Therefore, it will be discussed which kinds of cyberattacks are useful for the purpose of this study. Secondly, the sources and methods of collecting data on cyber-attacks will be explained. After the cyber-attack dataset is prepared, thirdly, the methods of quantitatively analysing the state's dyadic relations will be discussed. In this respect, "Event Data" which is used as both "process" and "specific data type" in the generation of quantitative political data in the Political Science and International Relations disciplines, will be discussed. Fourthly, to analyse these datasets by quantitative methods, Binary Logistic Regression and Pearson Correlations will be addressed. Lastly, to enhance the detection capacities of

the states regarding the second main research question, how to develop an AI-based early warning system to detect politically motivated cyber disruption operations based on the analysis of the complex dynamic relations of states will be discussed.

3.1. Choosing Cyber-Attacks: DDoS Attacks as Tools for Geopolitical Upheavals

According to the United Kingdom National Cyber Security Centre (2023), a cyber-attack is an intentional attempt to "damage, disrupt or gain unauthorised access to computer systems, networks or devices". In the same way, Salih Bıçakcı (UIK, 2019) defines cyber-attacks as someone who does not have the user right to access the data within the computer network and wants to 1) access, 2) disrupt the integrity of data, or 3) add information that is not there, is called a cyber-attack. Both definitions underline the same points: In principle, all cyber-attacks pose a potential risk to one of the fundamental elements of security controls in information systems, which are *confidentiality, integrity and availability (CIA Triad)* (Samonas & Coss, 2014, pp. 21–24). Therefore, although different kinds of cyber-attacks employ different techniques and require different capacities, all these cyber-attacks threaten at least one element of the CIA Triad. In this regard, it is possible to categorise all cyber-attacks according to their potential risks on the CIA Triad. For instance, cyber espionage attacks pose a risk to the target's confidentiality because these types of cyber-attacks aim to gain unauthorised access to the target's computer systems, networks, or devices. The information that is retrieved by unauthorised access can be used for different purposes according to the threat actor's motivation. While this information can be about the personal information of political leaders to cause reputational harm by exposing private information such as e-mails, it can also be classified data, trade secrets or intellectual property (IP), which is used to create an economic or political advantage (Baker, 2023). As an example of cyber espionage, the leaked e-mails of Hillary Clinton to damage her campaign for the US Presidential Election (D. Smith, 2016) and the accusation of China stealing trade secrets of various US companies in different sectors to gain economic and political advantage (Siddiqui, 2023) can be given. These examples indicate that the type and the target of the cyber-espionage attacks differ with respect to the attacker's motivation.

Secondly, cyber sabotage attacks threaten the integrity of the target's security because they entail the deployment of malicious software to prevent normal operation of the target's systems, network and devices either by deleting or changing code (CFR, 2023; CISA, 2023). From causing a power outage by attacking the power grid to changing the code that adjusts the spinning speed of the centrifuges, all these cyber-sabotage attacks damage the integrity of the devices, networks and systems. Any sabotage attack that can cause harm to critical infrastructure directly hampers daily life in modern societies. In this respect, cyber-attacks that threaten integrity are considered to pose the most threat to states. However, as datasets demonstrate (e.g. CFR, 2023; Valeriano, 2022), these cyber-attacks rarely occur. It is because these kinds of cyber-attacks require detailed information about the target's systems and devices so that they are costly in terms of time, know-how and development. In addition, states pay great importance to the security of their critical infrastructure and important devices and systems so that it increases the cost of employing successful this kind of cyber-attack.

Also, measuring the impact of these kinds of cyber-attacks after their use is difficult. While they can remain limited, on the other hand, it can lead to unintentional damage to the target, which increases the possibility of escalation. Lastly, these types of cyber-attacks have a unique "*use it and lose it*" character (B. Jensen & Banks, 2021). Therefore, developing unique cyber weapons for each target increases the cost of establishing an arsenal of offensive cyber capabilities (Linn, 2016). For all these reasons, while developing these kinds of cyber tools is costly, the states with the capacity and capability to develop such tools are reluctant to use them. Thus, although cyber-attacks which target the integrity of the target's systems and computers pose a significant threat and their impacts can be substantial, states rarely carry out such cyber-attacks due to their complex nature.

Lastly, Denial of Service (DoS) and Distributed Denial of Service (DDoS) can be given as example of cyber-attack that threatens the *availability* of systems and computers. DoS is a malicious attempt to deliberately disrupt the normal flow of traffic to a specific server, service, or network so that making these targets temporarily or indefinitely unavailable to authorised users. As a type of DoS attack, DDoS attacks, on the other hand, use multiple sources (computers, machines) to flood servers or computers with information to force malfunction or bring them down (Klimburg,

2017, p. 76; Microsoft, 2023). In other words, the main difference between DoS and DDoS is the source of the attack. While DoS attacks are carried out from a single source, DDoS attacks involve flooding the target with a large volume of data simultaneously generated by numerous individual devices (CFR, 2023). The objective of the attacker is to overwhelm the target's capacity to handle the influx of requests, thereby impeding its normal functioning (Kaspersky, 2023). These sources can be all over the world. Therefore, it is rather difficult to prevent these attacks and attribute them to a single actor.

However, a vast number of the sources can be directed from a single actor as depicted in Figure 3.1 below. In general, DDoS attacks are carried out by using a network of compromised computers known as a botnet. These computers, often referred to as bots or zombies, have been infected by threat actors without the knowledge or consent of users (Cloudflare, 2023). The compromised devices are then utilised to participate in the attack, allowing the perpetrators to coordinate and orchestrate a massive influx of traffic toward the target. It is important to note that the users whose devices are part of a botnet are typically unaware that their devices are being used in such attacks. However, there are also instances in which individuals voluntarily allow their computers to be used as zombie computers so as to support the attacks. For instance, during the DDoS attacks on Estonia, instructions to attack Estonian targets were spread in various Russian language websites and forums (Ottis, 2008, pp. 2–3).

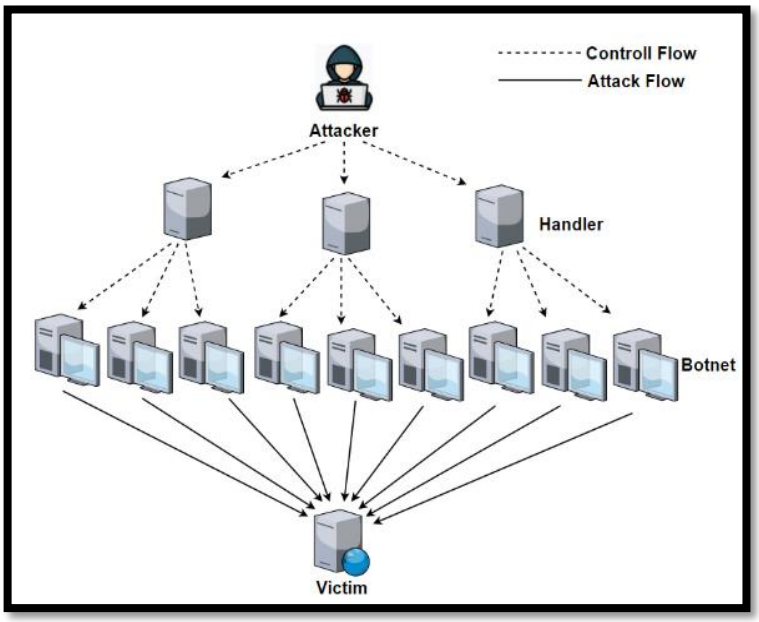

Figure 3. 1: DDoS Attacks with a Botnet

Source: (Shieh et al., 2021, p. 2)

DDoS attacks are also considered a part of disruptive cyber operations along with defacement of the websites (Kostyuk & Gartzke, 2019; Valeriano et al., 2018). Disruption attacks are low-cost cyberattacks that require fewer resources and skills and are aimed at creating disturbance following an incident. Therefore, disruptive cyber operations are defined as "*cheap signals*" that are used to pressure adversaries by threatening them as if to escalate the crisis (Valeriano et al., 2018). In other words, they are used to test the resolution of the adversaries.

The impacts of disruptive cyber operations can change according to the scope of the operations. Although disruptive cyber operations generally cause limited impact and cause only annoyance, their impact can be dramatic as well. For instance, the DDoS attacks that targeted Estonia in 2007, lasted three weeks and disrupted numerous government ministries' websites and systems, as well as two major banks (Herzog, 2011, pp.49-51; Ottis, 2008, p.1).

> "*The result for Estonians citizens was that cash machines and online banking services were sporadically out of action; government employees were unable to communicate with each other on email; and newspapers and broadcasters suddenly found they couldn't deliver the news"* (McGuinness, 2017).

The impacts of the DDoS attacks were mitigated by “restricting internet traffic in and out of the country” which was similar to “cyber siege” (Kingsley, 2012). Due to DDoS attacks' widespread impact on Estonia, it is generally regarded as the first cyber-war in history. Nevertheless, despite the potentially severe impacts of DDoS attacks, most cyber disruption attacks are conducted at a low cost that causes limited pain to a targeted state (Valeriano et al., 2018, p.36). In this study, to analyse the role of cyber tools as modern foreign policy instruments, DDoS attacks, which consist of the majority of the disrupting cyber operations, will be examined. There are four main reasons to include DDoS attacks for analysis:

First of all, DDoS cyber-attacks are access agnostic. This means that an attacker does not need an early reconnaissance or back door (a vulnerability that the attacker can access systems or networks) to facilitate an attack (Borghard & Lonergan, 2017, pp. 468–469). The more complex cyber-attacks, such as sabotage and espionage, require reconnaissance to find any vulnerability in the target. Through that access, the attacker can either retrieve the information from the source or change the code to damage the integrity. Nevertheless, these cyber-attacks cannot be facilitated if the attacker loses access to the target of the pre-discovered vulnerability. However, during a crisis, states have no time for reconnaissance to find a vulnerability in the adversaries' systems. Even if they try to use the previously discovered vulnerabilities to conduct cyber-attacks, there is no guarantee that vulnerability is still present. The targeted state might have discovered its own vulnerabilities and fixed them. On the other hand, a DDoS attack does not require a back door (although more advanced DDoS attacks may require it) because regardless of the target, the same method and same sources can be utilised to disrupt the flow of traffic to a specific server, service, or network by creating excessive traffic. In this regard, during a crisis between states, DDoS attacks become useful tools for states to signal their disturbance about an incident and to test rivals’ resolution.

Secondly, DDoS attacks are one of the least complex types of cyber-attacks due to the requirement of less technical knowledge and resources compared to other cyber-attacks (Brantly, 2018, p. 42). Therefore, DDoS attacks can be conducted regardless of the capacity of the state actors. In the literature, there is a fear of Stuxnet-like cyber-attacks; however, only a limited number of states have the capacity and capability to

develop them. On the other hand, DDoS attacks can be carried out easily by even non-state actors. Therefore, this method can be utilised by states that have not developed technical capacity and capability. Furthermore, even in the absence of available cyber tools, state-sponsored actors can easily conduct a DDoS attack by purchasing from the black market for around $400-800, according to the scale of the botnet that is being deployed (Borghard & Lonergan, 2017, p. 468). Hence, during a crisis, states can easily conduct DDoS attacks even if they do not have a cyber tool available at that time.

Thirdly, DDoS attacks are often driven by geopolitical, regional, and socio-political motivations. According to prominent studies, researchers observe a correlation between DDoS attacks and political events as well as military incidents. For instance, Maness and Valeriano (2016, p. 317) observe that while DDoS attacks have a negative impact on the relations between two states, they could not observe such relationship for other cyber-attacks. They argue that since people can experience the impacts of DDoS attacks, DDoS attacks negatively affect the relations between two states (Maness & Valeriano, 2016, p. 317). The primary reason is that DDoS poses a risk for states, causing people to feel insecure and lose their trust in their states or governments. While a state may be able to hide an attack on military or government sources, it becomes much harder to conceal a DDoS attack on public targets. Therefore, DDoS attacks' psychological effect on societies, rather than their physical effects, led states to react to DDoS attacks. In other words, DDoS attacks are also used as tools for "influence operation" to exert influence on society and cause disruption for political purposes. As an influence instrument, DDoS attacks are particularly deployed to degrade the morale of countries embroiled in socio-political upheaval (Hummel & Dobbins, 2022, p. 11). I

In addition to DDoS attacks' disruption and physiological impact, Philipp M. Lutscher (2021) argues that DDoS attacks are also used as a digital retaliation tool in response to the imposition of sanctions. According to Lutscher (2021, pp. 9–10), if a sanctioned country has a certain level of technological advancement or development, that state retaliates with DDoS attacks on a state that imposed the sanctions. Moreover, Kostyuk and Gartzke (2019, p.17,23) contend that while cyber espionage and degradation campaigns are used in isolation, disruptive operations are used to

complement fighting on the ground. With these attacks, states try to disrupt the command and control of systems of their enemies in the conventional kinetic war. In particular, powerful states tend to use disruptive cyber-attacks against their adversaries, in addition to traditional kinetic warfare on land, sea, air and space, due to their advantages in technology and available resources. (Kostyuk & Gartzke, 2019, p. 3,17).

Fourthly, in addition to the inherent characteristics of DDoS attacks, the challenges of analysing other cyber-attacks also play a significant role in the choice of DDoS attacks for analysis. As noted above, states have rarely used integrity attacks due to various factors, including their unpredictable nature, the risk of escalation and the capacity and cost of developing them. In this regard, limited data available to researchers for integrity attacks makes it difficult to analyse these attacks, especially with quantitative methods. On the other hand, espionage attacks, which pose a threat to confidentiality, take place regardless of the crisis or war. As the director general of the Australian Security Intelligence Organization, Mike Burgess underlines that "*all nations spy, all nations seek secrets, and all nations seek strategic advantage*" (Barnes, 2023). Due to this fact, states consider cyber espionage attacks as a part of statecraft and do not share the details about these attacks or publicly renounce them unless cyber espionage activities go beyond traditional espionage. Besides, big companies and corporations also try to conceal cyber-attacks for fear of losing customers. Especially in sectors where trust and confidentiality are important, such as finance and telecommunications, sharing details of the cyber-attacks can create a sense of insecurity in their customers and lead them to turn to alternative companies. In order to avoid this situation, companies generally hide such attacks from the public. Moreover, states and companies may not even realise that they have been under attack. Even if they discover the attack, they cannot be sure when it started or which information are retrieved by attackers. Therefore, conducting studies on the relationship between political events and cyber-espionage activities is challenging. In the next chapter, the data sources and methods of collecting DDoS attacks will be discussed.

3.1.1. Collecting DDoS Attacks Data: Sources and Methods

In the literature, there are limited number of datasets about cyber-attacks. These datasets (e.g. CFR, 2023; Valeriano, 2022) are updated in a period of time and show the source of the target, attacker, type of the target, time and the target sectors. These datasets do not include all cyber-attacks but the state-sponsored and significant cyber-attacks between states. In this study, these datasets will also be utilised for pre-analysis; however, to analyse the geopolitical events and their impacts on the increase or decrease of DDoS attacks, there is a need for more available and timely data on cyber-attacks. Particularly, to develop an early warning model for cyber-attacks that predicts the increase in the frequency and volume of cyber-attacks, more data is required. The available datasets also offer lots of analysis; however, the aim of the study necessitates additional new dataset.

There is a substantial number of cybersecurity companies that actively monitor servers and network traffic, analysing various cyber-attacks, including DDoS attacks. Some of these companies also share their data and publish regular reports, providing valuable insights into the global cyber threat landscape. In this study, the data for DDoS attacks will be received from the "NETSCOUT Omnis Threat Horizon". It is a free tool that offers real-time DDoS attack monitoring service that allows researchers to access data on real-time attacks worldwide. With filter options, researchers can parse the data according to target country, region and DDoS attacks' frequency, volume, speed, and duration. Also, it provides attack states based on daily/monthly/yearly trends for each country and region to increase awareness of global cyber threats.

Moreover, NETSCOUT's experts also offer country/region-based analyses to elucidate political and cyber trends and give insights about different regions. For instance, in 2022 DDoS Threat Intelligence Report, experts (Hummel & Dobbins, 2022) emphasised the role of the Russia-Ukraine War on global DDoS attacks. In this report, it was highlighted that many high-profile DDoS attack campaigns coincided with national or regional conflicts that generated worldwide reactions. Hence, they underlined the importance of both regional and global dynamics in cyber-attacks. In their 2023 report, experts examined how geopolitical influences play a dominant role

in the DDoS threat landscape, citing Sweden's bid to join NATO (Hummel et al., 2023, p. 13). In addition, NETSCOUT is also cited in reports by prominent institutions such as The European Union Agency for Cybersecurity (ENISA) (2022, p.70). ENISA relies on NETSCOUT's reports as a primary source of information for understanding the trends in cyber-attacks. Hence, by choosing NETSCOUT as a reference, this study's overall validity and credibility will increase.

Although the Omnis Threat Horizon of NETSCOUT allows researchers to view all data for a specific country, time period, and additional filtered options, it does not provide an option to extract or download all datasets. If a researcher wants to work on the data, they can collect all data manually. In this regard, the daily frequency and volume of DDoS attacks on countries will be collected manually from NETSCOUT's Omnis Threat Horizon, while strictly adhering to data privacy regulations.

Table 3. 1: Dataset Example: DDoS Attack Frequency and Volume

Date	**Frequency of DDoS Attacks to Country A**	**Volume of DDoS Attacks to Country A**	**Frequency of DDoS Attacks to Country B**	**Volume of DDoS Attacks to Country C**
01.01.2015	560	12	120	14
02.01.2015	810	24	340	28
03.01.2015	900	30	200	18

As illustrated in Table 3.1. above, the attacker state will not be included in the dataset. This is a different approach and may be criticised by many scholars. This study acknowledges that these criticisms have some merit. However, as discussed in the previous chapter, this study argues that analysing cyber-attacks through dyadic relations can lead researchers to overlook complex dynamics. Conducting an analysis only based on the two countries may prevent the researcher from making a more comprehensive analysis. In the tension between two countries, a third country may also perceive a threat from the crisis and conduct a cyber-attack on the parties involved in the tension. On the other hand, a state may perceive a threat from the rapprochement of two countries and may signal its disturbance by carrying out a cyber-attack on both states at the same time. Instead of analysing only the cyber-attacks between two countries and their bilateral relations, it would be more insightful to examine how the changing complex relationship of countries within the same region affect the trends of

cyber-attacks on a country. This approach will provide a better understanding of the relationship between cyber-attacks and geopolitical and regional dynamics. To perform this analysis, it is required to have a dataset that shows the level of relations between countries alongside the cyber-attack dataset. The next section will explain the method used to analyse the dyadic relations quantitatively in detail.

3.2. Quantitative Analysis of Bilateral Relations: Event Data

Following the Second World War, social science disciplines experienced a behaviourist revolution. Alongside technological advancements, the ideological rivalry between the two superpowers played a vital role in the behaviourist approach in the 1950s. In the United States, the academic community emphasised scientificness through the behavioural approach in social science disciplines. The scientific theme was critical in these studies because the researchers believed that by utilising scientific methods that were based on objective and universal truths, their studies were more reliable than the ideological work of the socialist camp (Tanrısever, 2015, p. 91). In this regard, many social sciences disciplines had been significantly influenced by American *Warrior Academics*[2] (Robin, 2003, p. 5) in terms of methodology and the context of the studies. Although IR as an academic discipline was born in Europe after World War I, following World War II, especially with the power struggle between the US and the Union of Soviet Socialist Republics (USSR), IR became one of the disciplines most affected by American scholars, as well as behaviourist turn.

In this respect, behaviourist researchers assumed that *history and law*, which were the main interest areas of the traditionalists, were not sufficient to understand and analyse the *causes of wars* (Şatana, 2015, p. 19). Throughout history, science has found cures for many illnesses and problems. In that vein, a social scientist could find cures for *social illness* (Özlük, 2009, p. 202) - war- through scientific methods. Therefore, behaviouralists use research techniques in natural sciences to analyse the patterns and trends in international affairs and to make predictions (McClelland, 1969, p. 4). As Hayward R. Alker echoed that behavioural analyst believed that these techniques would "*increase the explanatory power of our theories without escaping from or dismembering international reality*" (1966, pp. 654–655).

[2] Ron Theodore Robin (2003, p. 5) labelled those academics who use the discourse of scientificness against communist ideology.

In this respect, behavioural scholars have started to collect historical data and make analysis based on their dataset. For instance, David J. Singer initiated "*The Correlates of War Project*" to examine conditions under which international conflicts turn to war, which elements prolong and shorten the war, and whether there is a relationship between starting and succeeding in the war (1972, p. 243). Moreover, to bridge between new quantitative analysis of international politics and traditional approach of diplomatic history, Charles McClelland develop "political event data" that structured records events in the format of "who-did-what-to-whom" (McClelland, 1978; Gerner et al., 1994, p. 92). According to McClelland (1978, p.1) "*states act consistently enough that their past behaviour is a source for predicting their present and future actions"*. In this regard, under his directorship, the *World Event/Interaction Survey (WEIS) project* began collecting large amounts of event data to determine "whether these theoretically expected patterns occur regularly in international relations". This method has been adopted by many researchers and many different studies have been conducted. In this study, the state's dyadic relations will be analysed quantitatively through Event Data.

Event data is both a "*process"* and a "*specific data type"*. As a process, it contains the basic three steps that researchers follow to conduct an analysis respectively: 1) Obtaining stories, 2) Coding stories for relevant information, and 3) Aggregating and analysing the outputs through quantitative methods to understand trends and generate predictions. On the other hand, as a specific data type, an event is coded through the *who | did what | to whom | when | [and sometimes] where* (Schrodt & Yonamine, 2016, p. 7)

During the early stage of the event data, the whole process was conducted manually. The newspapers were collected and read, and the stories in the news articles were coded manually according to codebooks. Then, the aggregated data were created. However, this process was labour-intensive and required significant time, effort and budget for personnel and training. Also, manual coding consists of mistakes due to basic human errors and subjective judgment. However, in the 1990's, the event data coding process was automatised by two developments: Initially, with the advent of the Internet and large-scale aggregated online data sources such as LexisNexis,

researchers could obtain large-scale machine-readable data, which makes conducting analysis easier. Secondly, the advancement in computational capacity and Natural Language Processing (NLP) methods, made it possible to use personal computers to process large amounts of data (Schrodt & Yonamine, 2016, p. 8). Since then, many researchers adopted this automated coding system to generate large-scale event data.

Two tools are needed to automate the extraction of stories and convert them into structured event data: 1) Coding ontologies/frameworks and 2) Computer programs that use coding ontologies/frameworks to create a structured dataset. In event coding, the "*source"* of the event is the subject of the sentence, *the event code* is determined by the verb, and the *target* is the object of the verb (Schrodt et al., 1994, p. 563). In this respect, the coding ontologies are the rules that identify which source, object and verb in the texts are converted into event codes and categorical actors (Schrodt & Yonamine, 2016, p. 10). In other words, coding ontologies are the basic dictionaries/codebooks that indicate which actors and actions correspond to what. For the event data, there are specific coding ontologies such as "*World Event Interaction Survey (WEIS)*" (C. McClelland, 2006), "*Conflict and Mediation Incident Observations (CAMEO)*, (Gerner et al., 2002) and *Political Language Ontology for Verifiable Event Records (PLOVER)* (Halterman, Bagozzi, et al., 2023). These ontologies have been developed over the shortcomings of existing ones. Therefore, it would be more accurate to see them as upgraded versions rather than completely distinct ones.

Secondly, to code automatically stories in the news, there are various computer programs such as *Kansas Event Data System (KEDS)* (P. A. Schrodt et al., 1994), its successor "*Textual Analysis By Augmented Replacement Instructions (TABARI)*" (Schrodt, 2011) and its successor "*Python Engine for Text Resolution And Related Coding Hierarchy-2 (PETRARCH-2)* (Norris et al., 2017)". Although different techniques are used in these programs with advancements in technology, they are primarily based on a syntactic constituency parse to extract political event data from news stories, determining "*who"*-"*did what"*-"*to whom"* as well as general attributes "where" and "when" (Norris et al., 2017, p.1). In other words, these programs automatically identify and code the *source* and *recipient actors* (person, organization, or entity), time and *location* based on extensive dictionaries of verb and noun patterns, as demonstrated in below Table 3.2

Table 3. 2: An Example of Event Data Format

March 12, 1998 – Israeli troops launched offensive attacks against Palestinian insurgents on Monday, in the first of what is expected to be a new wave of counter-terrorism efforts.

Date	Source	CAMEO Code	Target	CAMEO Event
19980312	ISRMIL	190	PALINS	(Use conventional military force)

Source: (Schrodt & Yonamine, 2016, pp. 12-13).

However, since these programs work with the dictionaries, there is a limit to coding, such as if the verb phrase or actor is not included in the dictionaries. With the recent advances in NLP these problems tried to be overcome. In this respect, there is a novel approach to generating event data without hand-coded dictionaries (Halterman et al., 2023). This innovative approach identifies source actors and recipients of the event through the utilisation of extensive language models, traditional machine learning classifiers, and pre-trained "question-answering" models from NLP. The method further categorises these individuals by matching them to their corresponding Wikipedia articles (2023, p.1). The figure 3.2 below illustrates how this novel approach works.

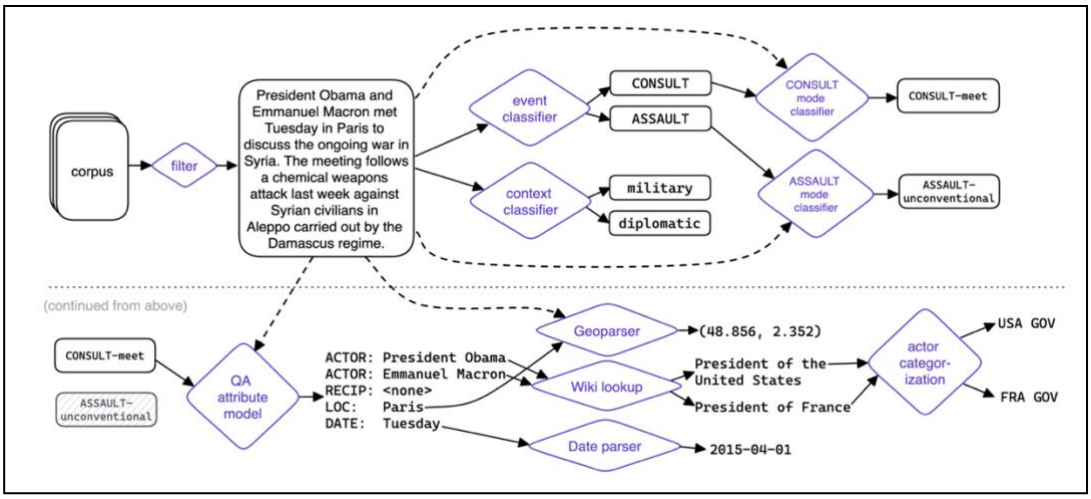

Figure 3. 2: Event Coding Pipiline

Source: (Halterman et al., 2023, p.6)

After finalising the process of event data, researchers can aggregate events and make analyses based on their specific objectives. While some researchers can analyse the relationship between two states through types of events, others can use quantitative

methods to analyse trends. In general, for the quantitative analysis, the events are coded based on the different scales. In this way, the dyadic relations for certain periods of time can be measured quantitatively. In general, researchers use the "*Conflict-Cooperation Scale for Event Data",* which was developed in an IR panel organised with the initiative of Joshua Goldstein (1992). IR scholars who participated in the panel, scored the events between -10 and +10 (-10 indicating the most conflictive and +10 representing strong cooperation). Based on scholars' scoring of the events, Joshua Goldstein created a scale for the Conflict and Cooperation which is presented below in Table 3.3.

Table 3. 3: Conflict-Cooperation Scale for (WEIS) Events Data

Event Type	**Weight**	**Event Type**	**Weight**
Military attack; clash; assault	-10.0	Explicit decline to comment	-0.1
Seize position or possessions	-9.2	Request action; call for	-0.1
Nonmilitary destruction/injury	-8.7	Explain or state policy; state future position	0.0
Noninjury destructive action	-8.3	Ask for information	0.1
Armed force mobilization, exercise, display; military buildup	-7.6	Surrender, yield to order, submit to arrest	0.6
Break diplomatic relations	-7.0	Yield position; retreat; evacuate	0.6
Threat with force specified	-7.0	Meet with; send note	1.0
Ultimatum; threat with negative sanction and time limit	-6.9	Entreat; plead; appeal to; beg	1.2
Threat with specific negative nonmilitary sanction	-5.8	Offer proposal	1.5
Reduce or cut off aid or assistance; act to punish/deprive	-5.6	Express regret; apologize	1.8
Nonmilitary demonstration, walk out on	-5.2	Visit; go to	1.9
Order person or personnel out of country	-5.0	Release and/or return persons or property	1.9
Expel organization or group	-4.9	Admit wrongdoing; apologize, retract statement	2.0
Issue order or command, insist, demand compliance	-4.9	Give state invitation	2.5

Threat without specific negative sanction stated	-4.4	Assure; reassure	2.8
Detain or arrest person(s)	-4.4	Receive visit; host	2.8
Reduce routine international activity; recall officials	-4.1	Suspend sanctions; end punishment; call truce	2.9
Refuse; oppose; refuse to allow	-4.0	Agree to future action or procedure, to meet or to negotiate	3.0
Turn down proposal; reject protest, demand, threat	-4.0	Ask for policy assistance	3.4
Halt negotiation	-3.8	Ask for material assistance	3.4
Denounce; denigrate; abuse	-3.4	Praise, hail, applaud, extend condolences	3.4
Give warning	-3.0	Endorse other's policy or position; give verbal support	3.6
Issue formal complaint or protest	-2.4	Promise other future support	4.5
Charge; criticize; blame; disapprove	-2.2	Promise own policy support	4.5
Cancel or postpone planned event	-2.2	Promise material support	5.2
Make complaint (not formal)	-1.9	Grant privilege; diplomatic recognition; de facto relations	5.4
Grant asylum	-1.1	Give other assistance	6.5
Deny an attributed policy, action, role or position	-1.1	Make substantive agreement	6.5
Deny an accusation	-0.9	Extend economic aid; give, buy, sell, loan, borrow	7.4
Comment on situation	-0.2	Extend military assistance	8.3
Urge or suggest action or policy	-0.1		

Source: (Goldstein, 1992, pp. 376–377)

Researchers can generate their own event datasets by following the aforementioned steps. However, instead of creating a new dataset, this study will utilise the open-source datasets that are already available. Although the author of this

study can produce datasets for a limited number of countries, the event data of many countries is required for this study. Therefore, the open-source datasets created by distinguished scholars and experts in event data methodology will be used as a primary event data source. Using these datasets instead of generating a new one will ensure a more reliable and credible analysis. As an open-source event dataset, The US Defense Advanced Research Projects Agency (DARPA)-funded *"Integrated Conflict Early Warning System"* (ICEWS)[3] (Boschee et al., 2023) and "*Global Data on Events, Location and Tone"* (GDELT) (Leetaru & Schrodt, 2013) are the largest event data collections (Ward et al., 2013, p.2).

These two datasets consist of millions of event data collected over long time periods. Nevertheless, the main difference between ICEWS and GDELT is the sources from which they extract the data. ICEWS retrieves articles from both international and regional news sources, while GDELT collects all articles from hundreds of smaller news sources in Google News (Schrodt & Yonamine, 2016, p.8). Instead of choosing one of them, both data sets will be used in this study. Since the two data sets use different sources, if there is missing data in one of the data sets, missing values will be completed with the other data set. This will allow for a more holistic and accurate analysis.

However, there is no single document available for these datasets. Instead, they generally share weekly or daily datasets. This means that researchers must merge those documents in an order. Since each document contains millions of news events, merging large datasets using basic programs like Microsoft Excel can be quite challenging. This is because merging or editing such files requires significant computing power. However, researchers can use open-source libraries of the Python programming language, such as Pandas and NumPy, to work on large documents. By using these libraries and Python, the event data datasets will be merged. Once the data is merged, to make a compatible quantitative analysis with the cyber-attack dataset, the merged event dataset will be filtered based on the following categories: "*Event Date"*, "*Source Country"*, "*Target Country"* and "*Goldstein Score*".

[3] Starting from May 2023, "*The POLitical Event Classification, Attributes, and Types" (POLECAT)* dataset, produced by the Program on Geostrategic Risk and funded by the Central Intelligence Agency (CIA), substituted the *ICEWS* (Scarborough et al., 2023).

Although both datasets will be used to collect data, there may still be missing values. The Event Data is created based on events reported in the news, so if there is no development or interaction between two states during a specific period of time, the datasets are coded with missing values for that day. For instance, if a researcher wants to analyse the dyadic relations between Turkey and Ecuador, the researcher will face a great challenge to find a development between the two states. The missing value is also an important indicator of dyadic relations; however, the lack of data in such cases makes it difficult or impossible to conduct a quantitative analysis of the relations between these countries. Therefore, in some cases, the dyadic relations have to be excluded from the analysis to have a better and correct analysis.

On the other hand, in some cases, the number of missing values may be limited, but they can still have a negative impact on the overall quantitative analysis. In the field of data science, there are various imputation methods to address this issue. The choice of imputation method depends on factors such as the data type, structure, and topic of the study. One popular approach for imputing missing values is to use a model to predict these values (Brownlee, 2020). This involves creating a model for each input variable that has missing values. While different models can be used for this purpose, in this study, the K-Nearest Neighbor (KNN) algorithm is employed for imputation. In KNN imputation, to fill in the missing value, a new sample is imputed by identifying the samples in the training set that are "closest" to it and averaging the values of these nearby points (Kuhn, 2013, p.42) Configuration of KNN imputation often involves selecting the distance measure (e.g. Euclidean) and the number of contributing neighbours for each prediction, the k hyper-parameter of the KNN algorithm (Brownlee, 2020). With this imputation process, the last step before the analysis is completed and the quantitative level of the dyadic relations can be obtained. For instance, Figure 3.3 below shows the trend of the dyadic relations between Turkey and Russia from 2015 to the end of 2022. By following these steps, the UK's relations with Russia, Ukraine, China, Hong Kong, Iran and Israel between 2014-2023 will be quantified. In the following section, how to analyse these datasets through quantitative methods will be discussed.

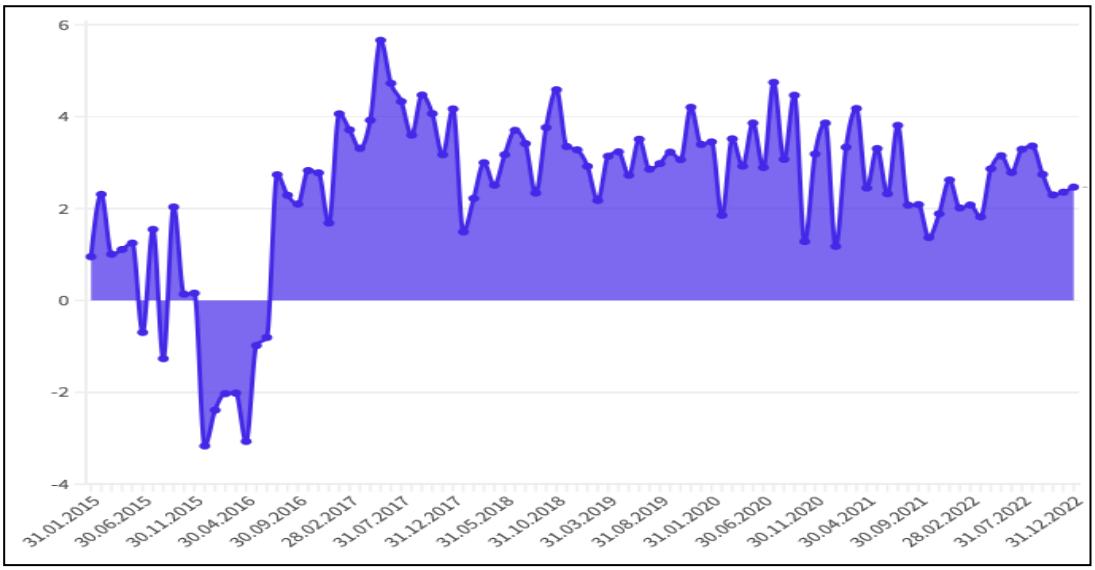

Figure 3. 3: The Trend of Türkiye and Russia Dyadic Relations with Event Data Dataset (2015-2022)

3.3. Methods for Analysing Impacts of Dyadic Relations on Cyber Disruption Operations

In general, it is expected that when there is a crisis between two countries, they carry out cyber-attacks against each other. For this reason, cyber-attacks between two states against each other are being studied. In this context, the general tendency is to examine reciprocal cyber-attacks and their dyadic relations. Although this approach is not wrong, it overlooks the fact that states engage in simultaneous conflictual and cooperative relationships with multiple actors simultaneously. Even though the crisis occurs between two states, it generally also affects the other states, especially the ones in the same region. In other words, a third actor may become the target or sponsor of cyber-attacks even if it is not directly involved in the crisis. Moreover, a rapprochement between two states may be interpreted by a third state as a potential threat, leading to retaliatory cyber-attacks against both states. Indeed, cyber-attacks - one of the tools that allow states to operate in grey areas, mainly because of the advantages of creating ambiguity and offering plausible deniability - are useful tools in such situations.

This is because when dyadic relations deteriorate, states have a variety of tools at their disposal However, when a rival state improves its relations with a strategically important country, states have relatively fewer foreign policy tools. At this point, cyber

disruption operations could be alternative tools for different purposes, whether to pressure rivals and create uncertainty among the public of a rival state during crises or to allow states to show their response without resorting to kinetic means. Thus, for states that are reluctant (or unable) to use other tools and that want to "do something" rather than "do nothing", cyber-attacks offer strategic utility.

Accordingly, this study will test the hypotheses discussed in the final part of Chapter 2.4. In order to test these hypotheses, a method which tests whether "A causes B or not" is necessary. By employing statistical methods, researchers can test whether an independent variable causes a dependent variable and, if so, to what extent. Thus, researchers must first identify their independent variable(s) and dependent variable. In this context, this study examines the relationship between the following dependent and independent variables:

- Independent Variables: *Cooperation-Conflict Scores of a country's bilateral relations*

Instead of including numerous variables like whether there is war, conflict, diplomatic crisis, and military cooperation agreements, only the cooperation-conflict scores between states are preferred. The primary reason for selecting the cooperation-conflict score as an independent variable is because this score encompasses all of the variables and offers an overview of all the events between the two countries.

- Dependent Variable: *Do the frequency and volume of DDoS attacks in the country simultaneously exceed the threshold? (Yes/No)*

Indeed, in the dataset that is collected from "Event Data" and the "frequency and volume of DDoS attacks", there is no variable as "*exceeding threshold level".* To obtain such a variable, the linear frequency and volume data will be converted into one binary category (Yes/No). In general, it is not preferred to convert linear data to binary data because it results in the loss of many features. However, in this study, it is necessary to convert it because there is a need to incorporate both volume and frequency variables simultaneously. Each country encounters numerous hundreds/thousands of cyber-attacks every day, depending on their population, the

prevalence of information and communication technologies and internet usage. The majority of these cyber-attacks are low-level. For this reason, while the frequency of cyber-attacks may be high, they might be low-level and ineffective. On the contrary, when the state or state-sponsor actor conducts a series of cyber operations, both the volume and frequency of the DDoS attacks increase significantly. In this regard, to detect cyber-attacks in the systems and networks, researchers try to find the anomalies in the flow of the data (Al-amri et al., 2021; Dutta et al., 2020; Karimipour et al., 2019). To find the anomalies/outliers, they adjust a level (threshold) that identifies what can be accepted as normal and different from the majority of the data (Bajaj, 2020). In other words, a threshold is used to find out the outliers/anomalies in the dataset. Hence, adjusting the threshold based on both the frequency and volume of the DDoS attacks in a country offers to detect the severe cyber disruption operations in countries that are most likely to be carried out by states or state-sponsored actors.

Since the frequency and volume of cyber-attacks will be converted into a single binary category, setting the optimal threshold for both variables is crucial step for both analysis and development of the early warning system, as will be discussed in the next section. To find the optimum threshold for both the frequency and the volume of DDoS attacks, "*unsupervised machine learning techniques*" will be used. Machine learning (ML) is a branch of Artificial Intelligence (AI) that uses self-learning algorithms to gain knowledge from data to make predictions. Instead of manually deriving rules and building models through analysing large amounts of data, Machine Learning presents an efficient alternative to capture the information in the data to improve the performance of predictive models progressively and make data-driven decisions (Raschka, 2015, p. 2). In other words, ML enables computers to learn from the data and make predictions. Machine learning algorithms are categorised generally into four groups that are "supervised learning" "unsupervised learning", "semi-supervised learning" and "reinforcement learning", as shown in the Table 3.4 below.

Table 3. 4: Four Types of Machine Learning Techniques with Examples

Learning type	Model building	Examples
Supervised	Algorithms or models learn from labeled data (task-driven approach)	Classification, regression
Unsupervised	Algorithms or models learn from unlabeled data (Data-Driven Approach)	Clustering, associations, dimensionality reduction
Semi-supervised	Models are built using combined data (labeled + unlabeled)	Classification, clustering
Reinforcement	Models are based on reward or penalty (environment-driven approach)	Classification, control

Source: (Sarker, 2021, p. 4)

Since there is no labelled/classified data of frequency and volume of DDoS attacks to train the ML model, the threshold will be set based on the DDoS attacks dataset. Therefore, to determine the threshold using unlabelled data, unsupervised machine learning models are necessary. For this aim, there are different unsupervised models such as "*clustering methods* (e.g. K-means clustering, density-based clustering)", "*Isolation Forest (iForest)"* and "*One-Class SVM (Support Vector Machines)".* Each technique uses different unique features to find the outliers/anomalies in the given dataset. However, some of them are more preferred by researchers. For instance, "*K-means"* -one of the most popular clustering methods- (Sinaga & Yang, 2020, p. 80717) divides a dataset into specified number (K) clusters based on squared Euclidean distance (Vanem & Brandsæter, 2021, p. 219). On the other hand, some data scientists consider "*Isolation Forest Algorithm"* as the best anomaly detection method for binary classification in big data (Young, 2021). It is fundamentally different from most of the other anomaly detection algorithms. Most of the algorithms first identify the normal instances in the dataset and then identify instances that do not conform to the normal instances in the dataset. On the other hand, Isolation Forest algorithm explicitly isolates anomalies from normal instances (F. T. Liu et al., 2008). This means that iForest detects the anomalies without employing any density or distance measure, which makes it different from other methods (F. T. Liu et al., 2012, p. 1). However, some of them are more preferred by researchers. In this study, "K-means" -one of the most popular clustering methods- (Sinaga & Yang, 2020, p. 80717) that divides a dataset into specified number (K) clusters based on squared Euclidean distance (Vanem & Brandsæter, 2021, p. 219) will be used. To use these models, Python Programming Language and "*Scikit-learn"* (Pedregosa et al., 2012), an open-source machine learning library in Python, will be used.

Following this process, a new binary category that variable indicates whether the volume and frequency of DDoS attacks simultaneously exceed the threshold or not, will be added to a dataset, as shown above in Table 3.5.

Table 3. 5: Adding Binary Category (Threshold) to Dataset

Date (Weekly Date)	**Conflict-Cooperation Score Between Country A and Others**		**Cyber-Attacks to Country A**		**Serious Cyber Disruption Operations**
	Country A & Country B	**Country A & Country C**	**Frequency**	**Volume**	
4.01.2015	-1,63913	-2,56154	529,2857	28,13258	True
11.01.2015	-1,312	-1,50667	250,5714	2,3268	False
18.01.2015	-1,30476	-1,04286	150,1429	6,3861	False
25.01.2015	-2,2	-3,35294	780,2857	40,06502	True

Before the analysis, the last step is to create a "sliding window" to capture the lagged effects of dyadic relations' impact on disruptive cyber operations. The created dataset with event data and cyber operations matched based on the occurring date. However, the impact of each political development might not be immediate on the cyber-attacks. The time of the state's response can be changed based on the events, situation, or country. Therefore, the lagged effects of political events on the frequency and volume of cyber-attacks should be taken into consideration. To catch the possible lagged effect of the political events, the "*Sliding Window Technique*" will be used. This technique allows to evaluate each value together with its previous values. For instance, if the window size is set as three, this technique evaluates each value together with the previous two values. In this study, to prevent to overlook of lagged effects of the political events on cyber-attacks, the window size will be chosen as four. The main reason for choosing a size of four is to capture monthly trends in political events since most political events' impact can be understood within a month. To use the Window Sliding Technique, the open-source data analysis and manipulation tool in Python, "*pandas"* will be employed. After these processes are finalised, the final dataset, as shown in Table 3.6 below, will be obtained.

Table 3. 6: Adding Lagged Conflict-Cooperation Scores to Dataset

Date (Weekly Date)	Conflict-Cooperation Score Between Country A and Others		Lagged Conflict-Cooperation Score Between Country A and Others (Window Size=3)		Serious Cyber Disruption Operations
	Country A& Country B	Country A& Country C	Country A& Country B	Country A& Country C	
4.01.2015	-1,63913	-2,56154	-	-	True
11.01.2015	-1,312	-1,50667	-	-	False
18.01.2015	-1,30476	-1,04286	-1,48596	-1,7034	False
25.01.2015	-2,2	-3,35294	-1,93824	-1,7997	True

After data processing is concluded, to test the hypothesis, the *binary logistic regression* will be used. In general, regression models are used to analyse the "*weighted sum of a set of independent (predictor) variables on the dependent (response) variable* (Harrell, 2001, p. 11). In other words, regression analysis is used to infer the causal relationship between the independent variable(s) and the dependent variable. By revealing this causal relation, regression analysis is also used to predict future values of the dependent variable (Arnab, 2017, p. 673). According to the data format, the number of the independent variable (single or multiple) and the type of the dependent variable (ordinal, binary, quantitative), there are different types of regression models such as Simple Linear Regression, Multiple Linear Regression and Logistic Regression. While Linear Regression is used when the dependent variable is continuous, logistic regression is used when the dependent variable is categorical (Fritz & Berger, 2015, p. 271). If the dependent variable consists of two categories (Yes/No - 0/1), to analyse the independent variables' relations to *a dichotomous response variable*, binary logistic regression is applied (Harrell, 2001, p. 215), regardless of the independent variables are continuous or categorical (Faizi & Alvi, 2023, p. 238).

Since the dependent variable in this study is classified based on whether cyber disruption operations exceed the threshold on a given date or not, this study will apply *Binary Logistic Regression.* In this context, this study will analyse the causal relationship between a country's dyadic relations and the disruptive cyber operations directed against it. However, it should be noted that if a country's dyadic relations have a statistical significance on the model, this study does not directly imply that the country is the perpetrator of the cyber operations. This study does not test it. This

analysis only tests which countries' relations have an impact on the increase or decrease of cyber-operations toward a given country.

Lastly, to uncover patterns, trends, and correlations between cyber disruption operations towards different countries in different times, Pearson Correlation analysis will also be used. Pearson Correlation basically measures the strength and direction of the linear relationship between variables. The correlation coefficients range from -1 to +1. When the correlation coefficient is close to either -1 or +1, it indicates a stronger correlation between variables (Sarker, 2021, p. 11) If the coefficients are positive, it indicates there is a positive linear relationship or vice versa, as seen in Figure 3.4 below.

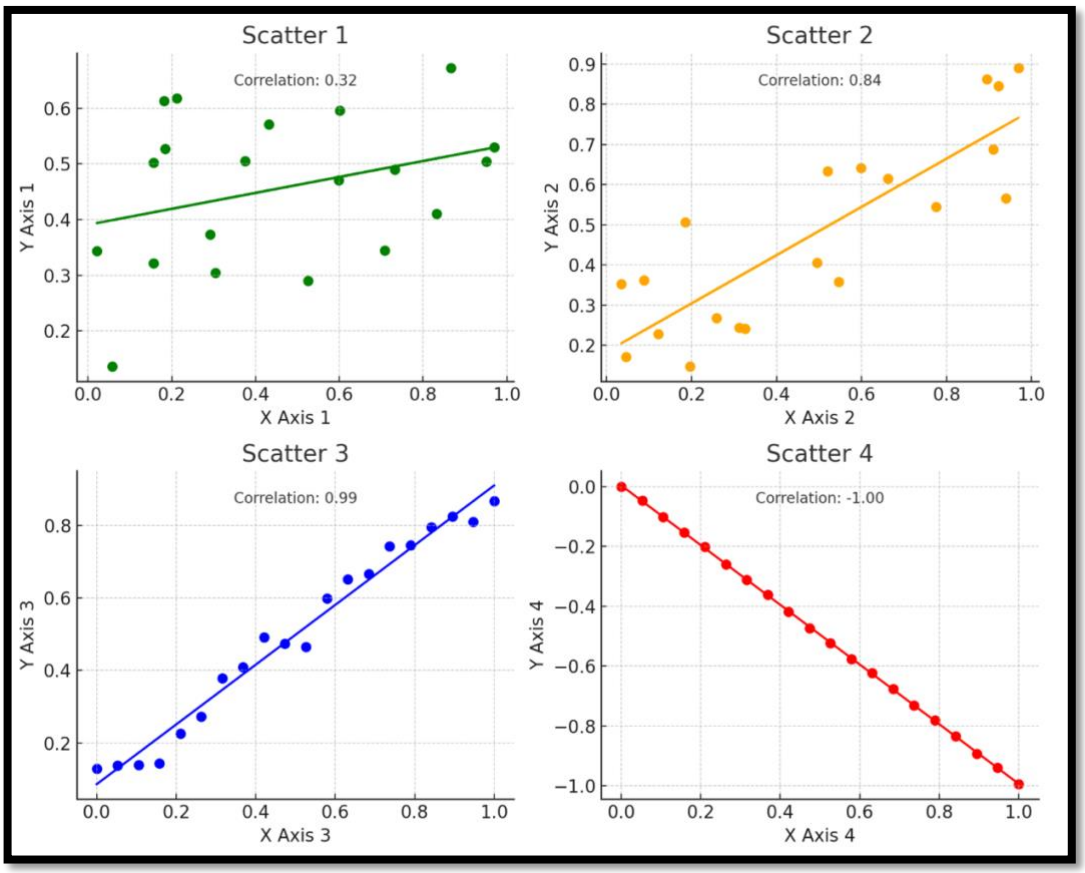

Figure 3. 4: Pearson Correlation Coefficient

In this regard, by using correlation analysis, it can be determined which countries are subject to cyberattacks with similar trends. The technological infrastructure of each country differs. If a country has an underdeveloped infrastructure, it is likely to be the target of a limited number of cyber-attacks (e.g., South Sudan, Yemen). Since

correlation analysis measures the linear relationship between two variables rather than the magnitude of the value, it allows us to analyse cyber-attack trends against countries. Thus, cyber-attacks on countries can be analysed comparatively via Pearson Correlation analysis.

3.4. Methods of Developing an Early Warning System for State-Sponsored Cyber-Disruption Operations by Machine Learning Models

One of the main aims of this study is to develop an early warning system to detect politically motivated cyber disruption operations based on the analysis of the complex relations of states. To develop this model, the supervised machine learning algorithms will be used in this study. In the previous section, how the optimum threshold value could be measured through the unsupervised machine learning models was discussed. With this technique, the threshold value will be determined, and a labelled dataset will be obtained. In other words, a dataset that shows when a country is subject to significant cyber disruption operations, will be obtained by unsupervised machine learning models.

In supervised machine learning techniques, researchers train models using labelled datasets. Based on this training, artificial intelligence models can classify the new test datasets. Therefore, this technique is called as “supervised” machine learning model. This technique is generally preferred in order to make a more accurate classification, especially in areas where many factors need to be taken into account simultaneously, and therefore it is challenging to make the classification. In this regard, it is used in different sectors, from detecting anomalies in networks (Elmrabit et al., 2020; Nawir et al., 2018) to disease diagnosis (Sokoliuk et al., 2020). For the same purpose, to predict/classify whether there will be cyber operations that exceed the threshold when new conflict-cooperation scores between countries are obtained, this study aims to develop a model using supervised machine learning techniques. The model will be trained with the dataset presented above in Table 3.4.

For classification, several supervised machine learning algorithms exist, such *Random Forest (RF)*, *Support Vector Machines (SVM)*, *Gradient Boosting* and *K-Nearest Neighbors (KNN)*. Each model classifies the instances based on a different

approach. In this respect, firstly, the Random Forest model is designed to predict a value or class by combining the results of multiple decision trees to solve classification and regression problems. This model is used for various applications, including cybersecurity for its suitability for nonlinear problems, high accuracy, and efficient computation (Singh et al., 2023; Y. Liu et al., 2012, p.246). Secondly, the SVM is an important model for solving complex classification, regression, and outlier detection problems. This model works by constructing a hyperplane that separates data points into different classes (such as anomalies and normal instances). In this regard, the model tries to find the hyperplane that has the maximum margin between the classes (Ioannou & Vassiliou, 2021; Awad & Khanna, 2015, p. 43). Thirdly, Gradient boosting is an ensemble learning approach that improves prediction accuracy by combining multiple weak models to create a stronger prediction model. In this machine learning model, each successive model corrects the errors of the previous models by focusing on the residual errors, gradually increasing the accuracy of the ensemble prediction (Natekin & Knoll, 2013). Last but not least, KNN is a non-parametric algorithm which classifies data points based on their proximity and association with other available data. The KNN model calculates the distance between data points, and based on the proximity of data points, it assigns a class using the most frequent class or average (Martinasek et al., 2016).

Since these models have different approaches to classification, each has different strengths, affecting their classification performance (Chen et al., 2020, p. 2). In this respect, instead of using specific machine learning models, this study will train these models separately and compare their prediction performances. To measure these models' performance, there are different metrics such as *accuracy, precision, sensitivity, specificity* and *F-score values, Root Mean Square Error (RMSE) and Area Under Curve (AUC).* Indeed, the basis of these metrics is the Confusion Matrix because these metrics are measured through the Confusion Matrix, as seen below in Table 3.7.

Table 3. 7: Confusion Matrix

		Actual Class
Predicted Class	TRUE POSITIVE (1)	FALSE POSITIVE (0)
	FALSE NEGATIVE (0)	TRUE NEGATIVE (1)

- True Positive (TP) indicates the prediction is positive when it is also actually positive.
- True Negative (TN) indicates prediction is negative when it is actually negative.
- False Positive (FP) indicates prediction is positive when it is actually negative.
- False Negative (FN) indicates prediction is negative when it is actually positive.

In these regards, the metrics can be measured as indicated in below (Sharma et al., 2022, pp. 37–39; Itoo et al., 2021, pp. 1507–1508; Elmrabit et al., 2020, pp. 5-6):

Accuracy is the proportion of total number of correct predictions.

$$\text{Accuracy} = \frac{TP + TN}{TP + FP + TN + FN}$$

Precision is the proportion of correct predictions of the positive values.

$$\text{Precision} = \frac{TP}{TP + FP}$$

Sensitivity (Recall) is the proportion of correct positive observations out of total positive instances. Therefore, it is also called as *True Positive Rate (TPR)*.

$$\text{Sensitivity (Recall)} = \frac{TP}{TP + FN}$$

Specificity is the proportion of correct negative observations out of total negative instances. Therefore, it is also called as *True Negative Rate (TNR)*.

$$\text{Specificity} = \frac{TN}{FP + TN}$$

The F1 score, or *F-score*, indicates the accuracy of the test. The value of the F1 score ranges from 0 to 1. Therefore, as the score is closer to 1, the accuracy of the test increases.

$$\text{F-measure} = 2.\frac{Precision.Recall}{Precision + Recall}$$

The Area Under Curve (AUC) measures the classification performance of the model across all potential classification thresholds.

$$\text{AUC} = \frac{1}{2}.(Sensitivity + Specificity)$$

The Root Mean Square Error (RMSE) measures the average differences between the values predicted by a model and the values actual observed values. The RMSE value can range from zero to positive infinity, with lower values indicating a better model.

$$\text{RMSE} = \sqrt{\frac{\sum_{i=1}^{N}(\text{Predicted}_i - \text{Actual}_i)^2}{N}}$$

It is important to note that a machine learning model's good performance is indicated by higher values of accuracy, precision, sensitivity, F1-score, and AUC and lower values of RMSE. To evaluate the performance metrics of the model, this study will focus on five metrics: "Accuracy," “Precision”, "F1 Score," "Recall," and " AUC." By comparing different machine learning models, this study also will be escaped from the falling into the famous trap that British statistician George Box emphasises: “*Statisticians, like artists, have the bad habit of falling in love with their models*” (Gorunescu, 2011, p. 36).

4. BEYOND BILATERAL RELATIONS: ANALYSING TRILATERAL RELATIONS OF THE UNITED KINGDOM AND CYBER ATTACKS

In this study, cyber-attacks are considered as contemporary tools of statecraft, used alongside other tools to achieve countries' particular objectives. However, in contrast to the analysis of individual cyber-attacks, this study also asserts that the role of cyber tools should also be examined based on their long-term use in the context of trilateral relations. This is because, as Valeriano et al. (2018, p.11) stated, cyber strategy does not necessarily aim to obtain direct concessions. Rival states use indirect cyber tools to shape long-term rivalry rather than to obtain immediate concessions. By analysing long term impacts, how states use cyber instruments as foreign policy instruments can be evaluated from a more holistic perspective. It is also possible to better determine when and in what situation state cyber-tools become more applicable tools for states. In this way, the use of various cyber tools by different states for different motivations at different times can be more explicitly shown.

Nevertheless, this study will not include every state or type of cyber-attack. Instead, it will concentrate on DDoS attacks for reasons discussed in detail in the previous methodology section. DDoS attacks are considered disruptive cyber operations (Kostyuk & Gartzke, 2019; Valeriano et al., 2018). Disruption attacks are low-cost cyberattacks that require fewer resources and skills and are aimed at creating disturbance following an incident. Therefore, disruptive cyber operations are defined as "*cheap signals*" that are used to pressure adversaries by threatening them as if to escalate the crisis (Valeriano et al., 2018). In other words, they are used to test the resolution of the adversaries. In this regard, this study will first test the following hypotheses:

H1a: *As the level of conflict between two rival states increases, the likelihood of utilising cyber-disruption operations as a tool of hybrid threat also increases.*

H1b: *There is no relationship between the level of conflict between two rival states and the likelihood of utilising cyber-disruption operations as a tool of hybrid threat.*

Furthermore, this study also posits that cyber-attacks serve as important foreign policy tools, particularly for states that are uncomfortable with the rapprochement of two states. While states possess a broader array of foreign policy instruments when their relations deteriorate, they are less equipped to respond when a state, particularly one of strategic importance, establishes good relations with a rival state. In this context, cyber-attacks become a viable option for states to convey signals without triggering a significant response. So, states might employ cyber tools to pressure rivals and create insecurity among the public of a rival state during crises or to allow states to show their response without resorting to kinetic means, thereby de-escalating crises. Therefore, for states who are reluctant to use (or unable to use) other tools but want to do "something" "rather than doing nothing"; cyber-attacks offer strategic utility. In this sense, cyber disruption operations are employed as instruments for tacit bargaining against rivals when the rival increases its cooperation with a strategically important state. In other words, in contrast to explicit bargaining, which relies on informal or formal diplomat exchanges, by using cyber disruption operations as an instrument of tacit bargaining, states try to influence the policy choices of rivals through behaviours". In this regard, this study will also test the following second hypotheses:

H2a: *When one of two rival states increases its cooperation level with a strategically important third country for both rival states, the likelihood of the other rival state launching cyber-disruption operations against its rival increases.*

H2b: *There is no relationship between one of the two rival states increasing its level of cooperation with a strategically important third country for both rival states and the likelihood of the other rival state launching cyber-disruption operations against its rival.*

In order to test these hypotheses and examine the complex relations between the changing dyadic relations of countries and the use of cyber disruption operations as a complementary foreign policy tool, the United Kingdom and its dyadic relations are

chosen as a case study. There are four key reasons for choosing the UK as a model country. First of all, according to DDoS attack data extracted from NETSCOUT, the UK has been the most targeted European country. As shown in the table below, from 2015 to 2022, the UK has always been the most targeted European country (annual average).

Table 4. 1: Frequency of DDoS Attacks on Several European Countries Between 2015-2022 (Yearly Average)

Date	United Kingdom	Germany	France	Italy	Belgium	Poland
2015	1155.99	639.95	953.68	272.41	170.12	165.90
2016	815.58	403.12	567.25	237.01	116.21	263.39
2017	872.51	415.86	760.69	195.85	113.14	233.88
2018	808.76	351.93	436.38	343.12	120.64	237.66
2019	1065.05	445.02	374.24	476.78	164.81	436.02
2020	1634.02	1215.32	487.18	525.92	341.48	407.99
2021	1323.04	779.44	270.10	445.61	274.31	408.66
2022	697.82	424.62	596.55	222.05	189.81	533.22
	Norway	**Sweden**	**Finland**	**Estonia**	**Latvia**	**Lithuania**
2015	130.46	376.43	51.12	11.05	8.97	19.01
2016	80.73	312.24	23.12	4.09	5.55	11.25
2017	69.07	341.15	22.22	4.60	19.42	7.92
2018	38.22	60.88	25.36	4.47	3.02	18.09
2019	61.88	128.97	36.41	3.72	6.73	91.42
2020	85.00	242.33	68.67	8.52	3.94	65.41
2021	92.60	251.55	196.00	15.19	2.16	53.73
2022	87.90	199.56	121.57	10.95	6.53	50.90

There are different reasons why the UK has been attacked so frequently. One of the main reasons is that the UK has one of the most advanced information and communication infrastructures in Europe. Indeed, there is a correlation between technological development and the likelihood of a country being the target of cyber-attacks. This is because if a country has a limited level of technological development and a limited number of users of these technologies, it means that attackers also have limited alternatives to attack. Therefore, these countries have become less of a target for cyber-attacks. On the other hand, cyberattacks are more prevalent in countries (e.g., the UK) where ICTs and IoTs are widely used and have a substantial number of users. In addition, since London is one of the prominent capitals in the world, the UK hosts a great number of major companies, especially in the finance sector. The existence of such companies substantially increases the severity and number of cyber threats.

However, it is noteworthy that Germany and France also have a similar level of internet infrastructure and host many companies. For instance, 97% of the UK population uses the internet, and its infrastructure score, which indicates the “existence and availability of physical infrastructure that provides internet connectivity” (Mitchell, 2023) is 78 (out of 100) (Internet Society, n.d.). Furthermore, its overall internet resilience index, which measures the acceptable level of service in the face of faults and challenges to normal operation, is 60 (out of 100) (Internet Society, n.d.). On the other hand, while Germany's 92% of the population uses the internet and its infrastructure score is 74, its overall internet resilience index is 66. Similarly, France's 85% of the population uses the internet, and its infrastructure score is 67, with an overall the internet resilience index of 64 (Internet Society, n.d.). Furthermore, according to the National Cyber Power Index, which measures countries' cyber power through "29 capability indicators across eight objects" by Harvard University's Belfer Center, the UK ranked fourth, France ninth and Germany eleventh in the overall ranking for 2022 (Voo et al., 2022, p. 10). Similarly, in terms of “defence” - one of the subjects of the National Cyber Power Index - the UK ranks fifth, while France and Germany rank and tenth respectively (p. 12).

Despite these approximate levels, as Table 4.1 above demonstrates, no country shares a similar level of experience with cyber-attacks as the United Kingdom. Therefore, it is not convenient to explain this phenomenon only by the level of its developed infrastructure. There are many other factors besides technological reasons. In this regard, this study posits that the United Kingdom's foreign policy is a significant causal factor in the UK's higher frequency of being subjected to cyber-attacks than other European countries.

This brings us to the second reason for choosing the United Kingdom as a model country: The United Kingdom has undergone shifting foreign policy due to both internal and external factors such as the Russia-Ukraine crisis, Brexit, the election of Donald Trump as US President and China’s more assertive and nationalist stance under the administration of Xi Jinping. This situation offers a good opportunity to analyse the relationship between changing diplomatic relations and being the target of cyber-attacks. Thirdly, the UK has been a significant actor in the major international organizations and alliances such as NATO, Five Eyes (FVEY) AND AUKUS. The

significant positions in these organizations and alliances make the UK the target of the various actors even if it has not directly been part of the events. Lastly, due to imperial and colonial history, the UK has historical ties in many parts of the world. Consequently, the United Kingdom's foreign policy towards countries and regions has been perceived differently from that of any other country in its relations with these countries. In these respects, the United Kingdom has been chosen as a model country.

On the other hand, to test these hypotheses, dyadic relations of the United Kingdom with Russia, Ukraine, China, Hong Kong[4], Iran and Israel between 2014-2023 were chosen. There are six reasons for choosing these dyadic relations. First of all, in the United Kingdom Government's Integrated Review of Security, Defence, Development and Foreign Policy Report (2021, p. 69), the UK describes its first goal as to "*counter state threats*". Accordingly, the UK underlined that as systemic competition intensifies, state threats against it intensify and diversify. As key factors in the deterioration of the security environment and the weakening of the international order, the United Kingdom considers great power competition [with China] and the opportunist states such as Russia and Iran (United Kingdom Government, 2021, p. 70). In this regard, for the United Kingdom, China poses an increasing threat to the UK's interest due to "its military modernisation and growing international assertiveness"; Russia poses a direct threat to European security, and Iran undermines the UK's interest by its destabilising activities in the Middle East (United Kingdom Government, 2021, p. 29). Moreover, according to the UK National Cyber Strategy 2022 Annual Progress Report (2023), Russia, China, and Iran were identified as top three cyber threat actors for the UK. Also, in the report, it was highlighted that there has been a deepening and growing partnership between these three countries, which makes international security dynamics more complex (2023, p.10). Furthermore, in the hybrid warfare/threat and grey zone warfare conflict, these three countries are regarded as the main applicants for the hybrid technique. For instance, according to Michael Mazarr, these three countries are "measured revisionists" that benefit from this system but are not satisfied with the existing system. In this context, they aim to shift the distribution of power in the international system, as well as international rules and norms, without going to war by using non-conventional tools below the threshold of

[4] Hong Kong was part of British colony until 1997. Since that time, it has been a Special Administrative Region of the People's Republic of China under the "One Country-Two Systems" framework.

war (2015, p. 28). Therefore, including these three states' relations with the UK in the analysis will also provide important clues about how cyber tools are employed.

Secondly, the United Kingdom's relations with Russia, China and Iran have generally been influenced by its relations with Ukraine, Hong Kong and Israel. Thus, it is more accurate to consider the UK's relations with those countries from a trilateral perspective rather than dyadic relations. Thirdly, whereas Russia was described as the "most acute threat" to its society (United Kingdom Government, 2021, p. 18), the UK has been one of the main supporters of Ukraine in terms of military, diplomatic and political instruments since 2014. Also, when the Russian-Ukraine War erupted in 2022, the UK dramatically increased its support for Ukraine, which has made the UK almost a part of the ongoing war in Ukraine. In this regard, Ukraine has a significant role in Anglo-Russian relations, especially since 2014.

Fourthly, the United Kingdom has strategic and historical relations with Israel. The Balfour Declaration (1917) - British Foreign Secretary Arthur James Balfour's statement of British support for "the establishment in Palestine of a national home for the Jewish people"- is regarded as the founding document of the state of Israel that was established in 1948 after the UK withdrew from Palestine in 1948. Since then, although the relationship between the two states has been volatile, the UK has been one of the most important supporters of Israel. In recent years, with the strengthening economic, military and diplomatic relations between the UK and Israel, the two countries' relations "had never been better, and all past tiffs felt long forgotten" as Stephen Oryszczuk stated (2020). On the other hand, this increasing cooperation between the two states has negatively affected the UK relations with Iran, the archenemy of Israel in the region. Therefore, the UK government's unequivocal support to Israel, particularly since the Israel-Hamas War, which began on 7 October 2023 (Helm, 2023), has made the trilateral relations between Israel, Iran and the UK more evident.

Fifthly, Hong Kong was part of the United Kingdom from the "First Opium War" in 1841 until 1997, when the UK handed Hong Kong to China on the condition that 50 years of self-government (Soo, 2022). However, China's gradual expanding influence and control over Hong Kong have hampered the "one country two systems" framework in the last decades. In response to China's assertive policy, the UK has

increased its cooperation with Hong Kong. The policies of both countries towards Hong Kong have caused them to criticize each other more, making UK-China-Hong Kong trilateral relations a significant case for this study. Moreover, in the 2010s, there was a golden era in the China-UK bilateral relations. However, bilateral relations began to deteriorate in the latter part of the 2010s and severely worsened in the 2020s. These developments provide important insights into the relationship between changing bilateral relations and cyber disruption operations. Lastly, these three trilateral relations take place in three different regions. Examining these relations across three regions allows testing the hypotheses in various regional dynamics and broadens the scope and applicability of this study. As a result, this case selection enhances both the internal and external validity of this research.

In this regard, the impact of these trilateral relations on cyber disruption operations against the United Kingdom will be examined in the following chapters. As a period, the analysis will focus on the era between 2014 and 2023. The primary reason for selecting this period is to present a holistic assessment that includes key events for UK's trilateral relations, from the Russian-Ukrainian Crisis in 2014 to Brexit, Pro-Democracy Protests in Hong Kong in 2019-2020, the Huawei crisis in 2020, the UK’s tilt towards the Indo-Pacific policy, major protests in 2022 in Iran, and the Israeli Gaza war in 2023.

Thus, in the next section, it will be first examined the UK's relations with Russia, China and Iran from the historical perspective to the present day (2024). In doing so, the strategic role of Ukraine, Hong Kong and Israel in the UK's bilateral relations with Russia, China and Iran will be discussed respectively. Secondly, impact of these three trilateral relations on the cyber disruption operations will be analysed with quantitative methods. This analysis will address how and why the UK becomes the target of cyber disruption operations in relation to Russia-Ukraine, China-Hong Kong, and Iran-Israel. After these three trilateral relations will be examined, lastly, it will be addressed why artificial intelligence (AI) offers significant potential for detecting, which is one of the most important elements in the countering of hybrid threats. In this regard, this study will introduce early warning systems based on different Machine Learning models. Then, which model is better in which aspects and which model holds the most

promise for developing an early warning system for politically motivated cyber disruption operation, will be evaluated by AI performance metrics.

4.1. The Trilateral Relations of the United Kingdom, Russia and Ukraine

In the United Kingdom's 2021 strategic report that outlined UK's long-term foreign policy strategy, Russia was described as "*most acute threat to [its] security"* (United Kingdom Government, 2021, p.18). Two countries relations have not deteriorated in a day. To understand two countries contemporary relations, it is important to examine the history of bilateral relations. Indeed, throughout the ages, two countries have been their main rivalries not only in the European continent but in different regions in eras. In this respect, the brief historical perspectives will shed light into the two countries current relations and the future as well.

Accordingly, the history of the United Kingdom and Russian relations goes back to 1553 when British navigator Richard Chancellor's ship escaped from the great storm and entered the White Sea. Tsar Ivan the Terrible, who was the ruler of Russia at that time, welcomed this arrival with more than the traditional diplomatic protocol and hospitality (Lobanov-Rostovsky, 1948, p.41). "Ivan gave the trading monopoly to the British-established Muscovy Company" and sent Chancellor back with an ambassador to initiate diplomatic relations, to have new trade routes and gain a new ally against other powers. As Lobanov-Rostovsky (1948, p.42) underlined that Ivan's political motivation for this friendly diplomatic relation was more acute than Queen Elizabeth. It is because to maintain the balance of power in Europe, Tsar Ivan the Terrible was seeking a military alliance with England by revealing the complementary need of the "bear" and "whale". However, since then, "whale" and "bear" have come together only when a power that endangers both countries arose, such as Napoleon's France and Hitler's Germany. Apart from the rise of such a power, Europe has witnessed the inevitable Anglo-Russian rivalry.

As Halil İnalcık (2016, pp. 266–267) summarised that Russia became a major state in Europe, especially during the reign of Catherine the Great, with the war of 1768-1774 and the subsequent invasion of the Crimean Khanate and the Northern Black Sea. In the 19th century, when Russia threatened to expand into the Baltics and

Poland and to invade the capitalist Western market, Europe had begun to see Russia as a major threat. In this regard, Russia had become a major threat to European markets in the Caucasus, the Middle East, Afghanistan-India, as well as in the Europe with its policy of landing in the warm seas. However, as Campbell underlined (1992, p.693) Russia was not a concern for Britain until the late 1820s when Russia's influence over the Ottoman Empire expanded, and there were no serious threats from France over the domination of Europe. Therefore, Anglo-Russian rivalry did not become overt until the 1850s. As Campbell stated that (1992, p.693) there was no arms race, competition for colonies and even in some cases (e.g., the Russian-Ottoman War between 1826 and 1829), they became close partners. Nevertheless, after the Crimean War (1853-1856), the rivalry between the two states had become overt. For years, Russia's ambitions to access the Eastern Mediterranean through the Turkish Straits and Aegean Sea was the main discord between the two countries; however, after this war, the competition shifted towards Asia (Sergeev, 2014, p. 15).

From the mid-nineteenth century until the "Anglo-Russian Entente Pact (1907)", in which Britain and Russia settled their colonial disputes in Persia, Afghanistan, and Tibet" (Encyclopaedia Britannica, n.d.) two countries had been involved in a major geostrategic rivalry called the "Great Game" for control of Central Asia (Sergeev, 2014, p. 2). One of the most important factors that fuelled the rivalry was the unification of Germany after the 1870-1871 Franco-Prussian War. In this period, as Halil İnalcık (2016, p.294) states, the most important problem for Great Britain was that after the establishment of The German Empire, the Germans disrupted the European balance of power and became a danger to the British colonies, which led to radical changes in the foreign policy of the British Empire (İnalcık, 2016, p.294). Former British Prime Minister Benjamin Disraeli underscored this change in his speech a few weeks after the proclamation of the German Empire in the Hall of Mirrors at Versailles on 18 January 1871:

> *"This war represents the German revolution, a greater political event than the French revolution of last century […] Not a single principle in the management of our foreign affairs, accepted by all statesmen for guidance up to six months ago, any longer exists. […]The balance of power has been entirely destroyed, and the country which suffers most, and feels the effects of this great change most, is England"* (United Kingdom National Archives, 2021).

However, Germany did not pose a direct threat to the United Kingdom. Germany was a long-term threat, and the main reason for this threat was the establishment of a state in Germany, which had been a power vacuum for years, and would disrupt the balance of power in Europe in the long term. As stated in the archives of the United Kingdom:

> *"[New Germany's] armies, victorious against continental enemies, could not reach the British Isles because it had no navy of any size; nor could they threaten Britain's overseas empire. And rivalry with Britain had no place in Bismarck's plans… Yet the German Empire posed a different kind of threat – the one Disraeli had identified – to the European balance of power"* (United Kingdom National Archives, 2021).

In this respect, historian Christopher Clark (2017, p. 132) put forward that the German threat was an invention and a panorama for Britain. The main issue was not the rise of Germany, but the fact that Russia had been freed from the conditions imposed on it after the 1853-1856 Crimean War. However, with the defeat of France, Britain could not restrain Russian ambitions alone. It soon became clear that these fears were not unfounded. As feared, Russia started to build a new Sevastopol in the 1870s and it was considered by Britain as the beginning of a new Russian expansionism. Hence, as Christopher Clark underscored that the most serious long-term threat to Britain was not Germany but Russia and Russia found the legitimate source of access to the coasts with the unification of Germany in 1871 (Clark, 2017, p. 132).

Moreover, Russia also posed a severe threat to India. Given Russia's geographical position and land power, it also had the upper hand over Britain. Hence, when the Russian railroad network was extending into Central Asia so that Russia could have better access to India, Britain significantly alarmed (Clark, 2017, p. 133). At that point, the alliance between Russia -the UK's rival in Central Asia and the Far East- and France - its main rival in Africa- exaggerated the concern of the United Kingdom. Accordingly, to balance Russia, Britain had two options: Either to support Japan in Asia against the increasing influence of Russia in the region or to find a way to reach an agreement with Russia. Indeed, the United Kingdom adopted both options. Initially, Japan was supported. However, after Russia suffered a significant military loss in Asia after the Russo-Japanese War in 1904-5 and turned its direction to the Balkans, it came across Germany, which was getting significantly stronger in Europe.

In this regard, in 1907, two states signed a treaty that resolved the issues between them in Iran, Afghanistan, and Tibet. Indeed, Christopher Clark (2017, p. 153) asserts that this agreement was not motivated by the fear or hostility towards Germany but rather by the fact that Russia was a much greater threat to Britain on many issues, and therefore, Russia was to be welcomed, and Germany was to be opposed. This was, therefore, the main idea behind the rapprochement between the two states in the 20th century Thus, Russian pressure in Asia, which was very important for the empire, was relieved and the Great Game was over.

For Russia and Britain, which fought together (Triple Entente) in the First World War, the rivalry seemed to be over for a moment. However, diplomatic relations deteriorated once again with the Russian Revolution of 1917. Against the Bolsheviks, Britain supported *'Whites'* and became the part of the Russian Civil War. Although diplomatic ties re-established in 1924, the Soviet Union continued to be the object of suspicion and hostility for Britain in the 1930s (War, 1996, p. 293). Also, at the beginning of the Second World War, the non-aggression pact between Germany and the USSR, the occupation of Eastern Poland, and the invasion of Finland, significantly increased the suspicions over the Soviets (War, 1996, p. 293). What brought "whale" and "bear" together once again was Hitler turned the barrel of the Panzers towards Moscow in 1941. With the start of Nazi Germany's invasion of the Soviet Union in 1941, two countries once again came together to fight against the candidate of the hegemon of Europe. In the immediate aftermath of World War II, increasing scepticism toward the Soviet Union and the famous "Iron Curtain speech" delivered by former British Prime Minister Winston Churchill in 1946, (Encyclopaedia Britannica, 2024c), the two countries' rivalry once again started. However, this time, the great game was not between the two countries but between the Soviets and the United States. Thus, since then, Anglo-Russian relations have significantly shaped the US-USSR rivalry. After the end of the Cold War, Russia's pursuit of integration with the West was welcomed by Britain, and it seemed that half a century of tension had finally been resolved. However, as in history, this period of rapprochement once again lasted very short and began to gradually deteriorate after Vladamir Putin became the president of the Russian Federation in 2000.

Duncan Allan and Ian Bond (2022) -associate fellow of the Russia and Eurasia Programme at Chatham House and the director of foreign policy at the Centre for European Reform (CER), respectively- asserted that "UK-Russia relations have moved through five phases since 2000". These five phases are 2000-mid 2003, 2003-2006, 2007-2014, 2014-2018, and 2018 to today. In fact, the report was published in January 2022, one month before the outbreak of the Russian-Ukrainian war. So perhaps they would list six phases. However, the period of the lowest level of relations, which started in 2018, still continues with a slight difference: Each day the lowest point records the new lowest one. Accordingly, the following political developments stand out when these five periods are examined.

At the beginning of the new millennium, the two countries' relations were mostly affected by the criticism of Putin for the invasion of Iraq by the US and the UK in 2003. Although Russia had supported the US in its war on terror after 9/11, the invasion of Iraq compelled Russia to reassess its desire for a growing relationship with the US and Russia's economic and security concerns (LaFraniere, 2024). Especially after the "invasion turned into occupation and violence" (Dixon, 2024, p. 85); Russia's concern increased as well. The fact that a significant number of the Muslim population in Russia, the majority of whom live in Chechnya, where the second Chechen War was ongoing; Iraq's invasion also created internal unrest in Russia (LaFraniere, 2024). Despite these disagreements with the United Kingdom, Putin had visited the United Kingdom. This trip was historic because Putin was the first Russian head of state since Tsar Nicholas I in 1843 to visit Russia (Waugh, 2003).

In the second phase of relations since 2000, from late 2003 to November 2006, there was a spectacular breakdown in relations due to a number of factors (Allan & Bond, 2022, p. 3). One of the issues was the United Kingdom's refusal to extradite Boris Berezovsky – who is a Russian business tycoon and rival of Vladimir Putin- due to being granted political asylum by UK (Hearst, 2003). This decision had strained two states relations. This tension intensified after the Orange Revolution in Ukraine in 2004. In the 2004, despite the thousands of accusations of fraud, it was declared that the Kremlin-backed candidate Viktor Yanukovych won the election. Against this decision, over the two weeks, millions of Ukrainians staged a nationwide non-violent protest that is known as the Orange Revolution (Dickinson, 2020; Karatnycky, 2005).

The protests led to a re-run of the election that was won by Viktor Yushchenko who supported by European and Western States (Traynor, 2004).

In addition to the 2004 presidential election in Ukraine, Rose Revolution in Georgia (The 2003 parliamentary election) and Tulip Revolution in Kyrgyzstan (the 2005 parliamentary election); Moscow perceived these "Color Revolutions" the US and its allies meddling in the region and support more confrontation with Russia (Mitchell, 2012, p.92). The Iraq war and these colour revolutions have led Russia to perceive the actions of the United Kingdom and the Euro-Atlantic community as unreliable states and to have a deep suspicion of them (Foxall, 2021, p. 13). In addition to these deep suspicions, Anglo-Russian relations significantly deteriorated after Aleksandr Litvinenko, a former officer in Russia's Federal Security Service (FSB) and prominent critic of Vladimir Putin, was murdered in London with radioactive polonium. Litvinenko had been granted asylum and citizenship in the UK where he exposed corruption and links to organized crime within Russian intelligence (Euronews, 2021). Although the United Kingdom considered this assassination as Russia's signal to its former agents who oppose the Putin regime and expose secrets; it is also a direct message to itself. In other words, Russia conveyed a direct signal to the UK to stop its activities to meddle in Russian internal affairs by granting asylum and citizenship to opponents of the Putin regime. Therefore, Britain reacted strongly against Russia, and the distrust of Russia began to mount more.

The third phase of bilateral relations -from 2007 until early 2014- indeed started with the diplomatic crisis. In May 2007, the UK requested the extradition of the main suspect of Litvinenko poisoning, Andrey Lugovoi, to stand trial for murder; however, the request was denied by Russia (Allan, 2018, p. 3). As a response to this denial, the UK condemns Russia's refusal as "unacceptable" and "extremely disappointing" (Reuters, 2007). Thereafter, former UK Foreign Secretary David Miliband announced the expulsion of four diplomats from the Russian embassy in London to send a clear and proportionate signal to Russia about the seriousness of the case for Britain (Tran, 2007). Indeed, it would be surprising if Russia extradited Lugovoi because in April 2007, almost one month ago, The Russian tycoon Boris Berezovsky stated to The Guardian about "*plotting the violent overthrow of President Putin from his base in Britain*". In the interview, he said that "*we need to use force to change this regime*

[because] it isn't possible to change this regime through democratic means. There can be no change without force, pressure" (Cobain et al., 2007). After this interview, Russia sent an extradition request to UK; however, it was rejected due to Berezovsky's asylum status. (Cobain et al., 2007).

Despite these crises and two countries' opposite position on the 2008 South Ossetia War between Russia and Georgia (Kite & McElroy, 2008); financial crisis of 2007-08 and the election of Barack Obama as president of US in 2008 who wanted to "reset" the diplomatic relations with Russia (Harding & Weaver, 2009), influenced the Russia-UK relations positively. In this regard, David Cameron, who became the Prime Minister of the UK in 2010, the rapprochement between UK and Russia had started. In 2011, with the hope of lifting the deep freeze relations, Cameron visited Russia (Wintour, 2011). One year later, as a paying a return visit, Putin visited the UK after seven years. During the London Olympics, Putin and Cameron discussed the Syrian Conflict, human rights issues and bilateral trade (Mulholland, 2012). Moreover, two countries' foreign and defense ministers held inaugural UK/Russia joint Foreign and Defence Ministerial talks on 13 March 2013 in London (United Kingdom Foreign & Commonwealth Office, 2013); three months later two countries' leaders met and held joint press conference in London (United Kingdom Prime Minister's Office, 2013). Nevertheless, as Duncan Allan and Ian Bond (2022, p. 4) underlined that with growing instability in the Middle East and the growing tension between Russia and EU over Ukraine in 2013–14; clouds were darkening between two countries' relations. Perhaps the first sign of future rifts between the two countries came in 2013 when before David Cameron travelled to St Petersburg for the G20 summit. Allegedly, President Putin's press secretary described the United Kingdom as: "*small island that no one listens*". Although President Putin's press secretary denied this allegation (N. Robinson, 2013) British officials seemed to think that this statement was true since David Cameron gave "a robust patriotic defence" against this description (Wintour, 2013). Indeed, even if this description was an allegation, it was still an important reflection of the Russian perception of the UK's position in the international system. Since then, the UK has adopted a more assertive approach to its relations with Russia, both in its words and its deeds (Foxall, 2021, p. 23).

The fourth phase of the bilateral relations began in February 2014 and ended in March 2018 (Allan & Bond, 2022, p. 4) Indeed, the event that led to the start of the new phase in bilateral relations - Russia's annexation of Crimea in 2014- has changed the upside-down relations into a continuing negative position. Ukraine also became the focal point of the two countries' relations. Therefore, it is possible to claim that the two countries' relations have almost been shaped by the two countries' positions towards Ukraine since Russia's annexation of Crimea in 2014. In this respect, to understand how trilateral relations of UK-Russia-Ukraine relations evolve, the prominent events between Russia and the UK through Ukraine between 2014-2023 will be discussed.

4.1.1. Strained Relations Between United Kingdom and Russia Over Ukraine Since 2014

After former Ukraine President Viktor Yanukovych's order for the suspension of trade and association agreements with the EU and opting for close ties with Russia (Traynor et al., 2014; N. Walker, 2023), crises that still today affect the relations between these countries had also begun. To protest Yanukovych's decision, thousands of people, which was the largest protest since the Orange Revolution in 2004, gathered in Kyiv's Independence Square (BBC News, 2013). With the increasing number of protesters, the government lost control, and the protests turned into clashes between the government and protesters. Hundreds of people were arrested, and dozens of protesters were killed (Weaver & McCarthy, 2014). As the demonstrations became more violent, the Ukrainian parliament impeached Yanukovych and called for new election. Yanukovych denounced this decision as a "coup" and fled to Russia (Urquhart & Neild, 2014). On the other hand, against this decision, Russia reacted strongly and recalled its ambassador to Ukraine for the deteriorating situation in Ukraine (BBC News, 2014a).

Initially, these developments were perceived as a resolution to the unrest in Ukraine. However, it became evident that they were merely the beginning of an endless conflict between Ukraine and Russia, which continues to this day (2024). On February 27, 2014, a group of pro-Russian gunmen took control of government buildings in Crimea (Siddique et al., 2014) and a day later, military troops in unmarked uniforms but looking like Russian uniforms (they were later called the Little Green

Man) seized two airports in Crimea. While the fingers were directed at Moscow, Russia persistently denied its involvement in the military offensive in Crimea (Salem & Walker, 2014). Later, to join Russia, Crimea's regional government decided to hold a referendum (Traynor et al., 2014) and more than 95 % of the voters in the referendum voted in favour of joining Russia (BBC News, 2014b). The referendum's result was not recognized by the majority of the international community and Russia was strongly criticized by them. Accordingly, the UK Foreign Secretary stated that:

> "*The UK condemns in the strongest terms Russia's flagrant disregard of Ukraine's sovereignty and territorial integrity. For the UK and her allies, the Crimea remains part of Ukraine. We are witnessing a clear attempt to pave the way for the annexation of part of the sovereign territory of an independent European state, through military force and an illegal and illegitimate referendum.*" (United Kingdom Foreign & Commonwealth Office, 2014).

Despite increasing criticism and sanctions against Russia by the EU and the US, Putin officially approved the annexation of Crimea on 21 March 2014 (BBC News, 2014c). Against this decision, On March 27, the General Assembly of the United Nations adopted a resolution declaring that the Crimean referendum was invalid (Felton & Gumuchian, 2014). Far from settling down, the situation became even more heated a week later. Pro-Russian protestors seized the regional government buildings in Donetsk, Luhansk and Kharkiv; and called for a referendum on secession from Ukraine. Against the control of the government building, the Ukrainian government sent security officials (BBC News, 2014d). Moreover, on 11 May, in Donetsk and Luhansk regions, despite Putin's advice to postpone, the referendum was held, and pro-Russia separatists set for victory with nearly %90% of the vote in favor of Donetsk and Luhansk People's Republic (Walker et al., 2014). On 5 September 2014, to end a five-month fight between pro-Russian rebels and Ukraine, they agreed on a 12-point ceasefire and signed the Minsk Agreement (BBC News, 2014e); however, with both sides' violations, the agreement failed. In February 2015, representatives from Russia, Ukraine, the "Organisation for Security and Cooperation in Europe" (OSCE) and separatist-held regions Donetsk and Luhansk signed a new 13-point agreement, which is called Minsk II (Al Jazeera, 2015; Reuters, 2022). This agreement was widely seen as a victory for Russia, as the freezing of the conflict would have prevented Ukraine from entering the European blocs and, at the same time, kept it permanently weak (Bond, 2015). Moreover, it would have kept the possibility of civil war in Ukraine alive, which allowed Russia to intervene and control Ukraine

(Brunson, 2019). Moreover, for Mark Galeotti, the Minsk agreement was born dead, and it actually did more harm than good for Ukraine. Far from bringing peace, it served as a tool to prevent a new agreement and a new arrangement about the crisis. Therefore, abolishing Minsk II would allow states to return to reality and avoid unrealistic expectations. That is why he emphasized that the UK should propose an agreement to replace Minsk II (Galeotti, 2021)

Following the annexation of Crimea and the conflict in Eastern Ukraine, Ukrainian armed forces faced several serious shortages of training and basic equipment (United Kingdom Parliament, 2015b). The UK Government opposed providing lethal arms to Ukraine at that time (Mills, 2022, p.3); however, with the direct request of Ukraine, the UK provided non-lethal equipment to Ukrainian armed forces (United Kingdom Foreign & Commonwealth Office, 2014). In this respect, in 2015, *"Operation Orbital"* was launched, which has been a significant assistance program to Ukraine's military forces by providing non-lethal assistance such as operational and intelligence capacity-building and sending advisory teams for training (United Kingdom Parliament, 2015a). The scope of the Operation Orbital has expanded over the years. Moreover, one year later, for closer defence cooperation between the two countries (in respect of sharing more information about threats, conducting joint exercises and training the Ukrainian armed forces), the two countries signed a 15-year Memorandum of Understanding (MoU) (Mills, 2022, p.4). Moreover, in 2018, to train the Ukrainian Navy, training teams from the Royal Navy and Royal Marines also deployed to Ukraine (Mills, 2022, p.3).

Apart from the Ukraine, Brexit also deeply tensed two countries relations. Accordingly, with Brexit, there were discussions about Russia's interference in Brexit. David Cameron stated that Russia "might be happy" with the results. The Remain campaign also stated that Russia secretly supported Brexit to weaken EU (Rosenberg, 2016). These allegations were further strengthened by the words of the leading names in the supporters of Brexit Campaign such as Nigel Farage and Boris Johnson. Moreover, despite Boris Johnson government's blocking and delaying efforts (Ruy, 2020), in the report on Russia that was prepared by the UK Intelligence and Security Committee of the Parliament in 2020, it was underlined that although it is difficult to measure the extent of the impact; state-owned Russian international broadcasters such

as Sputnik and Russian Today covered pro-Brexit or anti-EU content; and bots/trolls carried out disinformation campaigns on social media to influence the Brexit process (2020, p.9,12). The report also criticized the UK government for not inquiring about Russia's influence on the referendum process even though there were many open-source studies on Russia's influence on the referendum process.

> *"HMG [His/Her Majesty's Government] not seen or sought evidence of successful interference in UK democratic processes or any activity that has had a material impact on an election, for example influencing results. […] Despite the existence of open-source studies about influence, [they were] not fully taken into account"* (United Kingdom Intelligence and Security Committee of Parliament, 2020, p.13).

In this regard, the comment of the Scottish National Party Member of Parliament, Stewart Hosie indeed summarises the findings of the report:

> *"The report reveals that no one in government knew if Russia interfered in or sought to influence the referendum because they did not want to know" (Sabbagh et al., 2020).*

Furthermore, in the post-Brexit period, Russian politicians generally emphasize the positive sides of Brexit for Russia's interest. It was underscored that the United Kingdom was the most aggressive member towards Russia in the European Union. The UK was the country that consistently tried to implement various sanctions against Russia, and therefore, Brexit would make the European Union more friendly towards Russia (Rosenberg, 2016). As Allan and Bond (2022, p. 6,9) underlined, the UK was perceived as "*Russia's toughest opponent within the EU*", and Brexit significantly would weaken the ability of the UK to shape the EU's actions.

Indeed, after Brexit, the UK adopted a tougher stance against Russia. For instance, in 2017, UK Prime Minister Theresa May's tougher stance on sanctions than former US President Donald Trump during her visit to the United States (Smith, 2017) gave important clues that the United Kingdom would pursue a tougher foreign policy towards Russia in the coming years. The first examples of this attitude became more evident about two months later. On April 4, 2017, following a suspected chemical attack in Idlib that killed 58 people (BBC News, 2017), former UK Defense Secretary Michael Fallon blamed Russia for the attack and claimed that Russia was "*responsible for every civilian death*" in chemical weapons attack (Watts, 2017). After this fierce

statement, the Russian ambassador to the UK, Alexander Yakovenko, stated that the UK Defence Secretary's statements were "*hostile rhetoric not supported by evidence*"; and he also accused the UK of "*raising tensions in Europe*" by sending 800 troops to Estonia on the Russian border. In light of these developments, he also asserted that relations between the two countries have reached an "*all-time low*" (RT International, 2017). In the last months of the year, before the former UK Foreign Secretary Boris Johnson's Russia visit, Theresa May escalated her tough stance on Russia by explicitly accusing Russia of interfering in elections and carrying out cyber espionage across Europe (Mason, 2017). In a joint press conference by UK-Russia Foreign Ministers during Johnson's Russia visit, Russian Foreign Minister Sergey Lavrov blamed UK for low-level of bilateral relations and re-emphasized the Russian Ambassador Yakovenko's words: "*It's no secret that our relations are at a low point and that's not at our initiative*" (Walker, 2017). Indeed, the Russian ambassador was a bit early in calling the relationship between the two countries at the "lowest". In the period following 2018, it seems that each day brings a new lowest point for bilateral relations. As of today (2024), the record for the lowest point is continually being broken, and it appears that there is still further to go to reach the lowest "lowest point".

The case that clearly started the *fifth phase of bilateral relations - the lowest point in bilateral relations* - was the poisoning of a former Russian spy and his daughter by a nerve agent in the UK in March 2018. The UK blamed Russia for the attack because of the substance used (Novichok, a Soviet-era military-grade nerve agent) and the person who was attacked (BBC News, 2018). Although Russia has consistently denied any involvement in this attack, as well as in all previous incidents, as Smith & Robinson (2024) highlighted that by poisoning former spies in the UK, Russia aimed to demonstrate that it should be taken seriously, despite its relative lack of military, economic, and soft power. This was also meant to send a message to "potential future traitors that they would not get away with it".

As a response to the poisoning, the UK expelled 23 Russian diplomats, which was the biggest single expulsion in over 30 years (Pitas & Shirbon, 2018). As a response, Russia not only expelled 23 UK diplomats but went further by closing the British Consulate in St. Petersburg and the British Council, which is an organization that promotes the UK and the English language (Sabbagh & Pegg, 2018). Moreover,

in August 2020, Andrei Kelin, new Russian Ambassador to the UK, stated that "*I feel that Britain exaggerates, very much, its place in Russian thinking*" (Brown, 2020). While he denied all the involvement of Russia in the Brexit referendum, cyber-attacks and poisoning, he underestimated the position of the UK by saying "*The scope and place of Great Britain in Russian politics* [is] *not that big".* By accusing the UK of throwing "a lot of mud" into the relations, he also describes the two countries' relations as "close to being frozen" (Brown, 2020).

Shortly after this statement, on 18 August 2020, UK Defence Secretary Ben Wallace announced an initiative – "*UK-led Multinational Maritime Training Initiative for the Ukrainian Navy*" – to increase the ability of combat of Ukrainian Navy against to threats from the East in Black Sea. Wallace underlined that "*Ukraine lost much of its Navy capability during Russia's illegal annexation of Crimea in 2014 and Ukraine has since continued to face a rising number of threats in the Black Sea and Sea of Azov*". In response these threats, along with other countries, UK will send Royal Navy ships for the train (United Kingdom Ministry of Defence, 2020). Moreover, two months later, during Ukraine President Zelenskyy's visit to the UK, the two countries signed a "*Strategic Partnership Agreement*" that covers trade, defence, political cooperation, climate change and human rights. Most importantly, by this agreement, Britain's continued commitment to the sovereignty and territorial integrity of Ukraine was formalized (United Kingdom Prime Minister's Office Press Release, 2020). On February 2021, to mark the seventh anniversary of Russia's annexation of the Crimea, UK also announced the funding of new project that aims to improve the access of the essential services for the Ukrainians living in Crimea (United Kingdom Foreign, Commonwealth & Development Office, 2021).

In April 2021, world's attention shifted to developments on the border between Russia and Ukraine. On April 5, former UK Prime Minister Johnson and Ukrainian leader Zelensky, discussed the deep concerns about the Russian military activities on Ukraine's border and in Crimea (United Kingdom Prime Minister's Office Press Release, 2021). One day after this phone call, Russia announced the start of mass military drills with more than 4,000 training exercises across Russia (Meyer et al., 2021). As Mykola Bielieskov (2021, p.2) pointed out that although Russia acted as if it was just an ordinary military drill; what made it unusual was the scope and scale of

military activities close to Ukrainian border which recalls Russia's actions in 2014–15.

This tension, which started in April, became even more tense in November when Zelensky announced that there were nearly 100,000 Russian troops near the Ukrainian border (Reuters, 2021). As a result of Russia's increased troop build-up on the Ukraine-Russia border, former British Defense Minister Ben Wallace, at a joint press conference along with Ukraine Defence Minister Oleksii Yuriyovych Reznikov said that "*We are concerned about Russia's military build-up and activities around Ukraine's borders*". Also, it was announced that "*An Intergovernmental Framework Agreement*" was signed between the UK and Ukraine to develop the capabilities of the Navy of the Armed Forces of Ukraine (United Kingdom Ministry of Defence, 2021). With this agreement, the UK provided a loan package of £1.7 billion to Ukraine, which was to be used for the purchase of British vessels and weapons systems (Waitzman, 2021). Moreover, until December 2021, the United Kingdom only provided non-lethal aid to Ukraine. However, with the increasing Russian activities on the Ukrainian borders, the UK government indicated the sending of defensive lethal weaponry systems to Ukraine, and in January 2022, to increase Ukraine's defensive capabilities, the UK provided a new security assistance package that included anti-armour weapons (Mills, 2024a, p. 5). In fact, the US was the first country to provide major defensive lethal weapons by sending anti-tank missiles to Ukraine in 2018. Other than the US, Turkey was the only country that also provided lethal weapons (Bayraktar drones) to Ukraine before 2022 (Mills, 2024b, p. 8,50). Moreover, in October 2021, the Ukrainian armed forces had used Bayraktar drones for the first time to attack targets in Donbas (Mills, 2024b, p. 50).

While potential conflict was on the horizon, the international community undertook intensive diplomatic efforts to avoid a potential outbreak of conflict. In this regard, on 12 January 2022, NATO-Russia Council was held; however, as NATO Secretary General Jens Stoltenberg stated after the council's meeting, "*there are significant differences between NATO Allies and Russia [and] differences will not be easy to bridge*" (NATO, 2022b). This statement indeed shows that diplomatic initiatives did not seem to work and that difficult times lay ahead for Europe.

Two days after the NATO-Russia Council, a significant cyber-attack targeted Ukraine's government websites (Al Jazeera, 2022). On 22 January, the UK Foreign Secretary informed that Russia had planned to plot to install a pro-Moscow government in Ukraine and former UK Prime Minister Boris Johnson urged to *"ramp up pressure on Russia*" (Graham-Harrison et al., 2022). On February 1, 2024, the leaders of the UK-Ukraine held a joint press conference. At the conference, Boris Johnson stated that "*the UK and its allies are preparing a package of sanctions and other measures if Russian troops cross the Ukrainian border*" and announced new funding for Ukraine (United Kingdom Prime Minister's Office Press Release, 2022a). On 10 February, Russia launched its largest military exercise with Belarus since the Cold War, which lasted ten days. Indeed, the participation of Belarus in the exercise strengthened the possibility of war because analysts previously stated the possibility of Belarus as a possible route for Russian troops to invade Ukraine (Chappell, 2022). This caused considerable anxiety in Europe. On February 19, at the Munich security conference, former British Foreign Minister Liz Truss stated that:

> "*Ukraine could face the worst-case scenario of a Russian invasion as soon as next week […] I'm afraid that Russia has shown that they are not serious about diplomacy […] We need to be strong because that is the only thing that Russia understands*" (Lock et al., 2022).

Two days later, on 21 February 2022, Russia announced the formal recognition of regions under the control of pro-Russian separatists as the "Donetsk People's Republic" and "The Lugansk People's Republic" (Butchard, 2022). Moreover, on the same day, former UK Prime Minister Boris Johnson called Ukrainian President Volodymyr Zelenskyy and informed him that "*an invasion was a real possibility in the coming hours and days*" (United Kingdom Prime Minister's Office Press Release, 2022b). Two days after Boris Johnson's warning, on 24 February 2022, Russian President Vladimir Putin announced that *"[He] decided to carry out a special military operation*" (President of Russia, 2022) and Russian troops crossed Ukrainian borders from Belarus, East and South (Mills, 2024c).

Following Russia's invasion of Ukraine, the UK and EU imposed an unprecedented package of coordinated sanctions aimed at strategic economic sectors for Russia, such as energy, aviation and finance, as well as individuals with close ties with the Putin administration and those who helped Russia to invade Ukraine,

including actors in third countries (Mills, 2024c; Mills, 2024b, p.5; BBC News, 2022). In addition to these economic sanctions, many countries began supplying lethal weapons to Ukraine for the first time, such as Germany and Sweden, and as the war continued, new types and numbers of lethal weapons continued to be supplied (Mills, 2024b, p. 5). In the aftermath of these sanctions, Russia published a list of unfriendly countries that includes all EU and NATO member countries (except Turkey) (Teslova, 2022). The war is continuing today (2024) and many countries, notably the US, UK, and EU member states, continue to impose major new sanctions. But two years after the start of the war, as Noah Berman (2024) underlined "*those sanctions have not caused widespread economic collapse or halted Russia's aggression against Ukraine*. Nevertheless, while sanctions may have seemed ineffective, the fact that Russia has not reached its political and military goals in Ukraine so far, and the conflict is once again restricted in eastern Ukraine, indicates that at least military assistance to Ukraine has been effective.

However, it is difficult to say that the war will end soon and without end (even after the end of the war), there is no sign that Anglo-Russian bilateral relations, which have been at a very low level since 2018, will improve in the near future. Russia's blaming British naval personnel for the explosions in the Nord Stream gas pipelines which carries Russian gas to Germany/Europe (Faulconbridge & Ravikumar, 2022) and accusing the British troops of involvement in a Ukrainian drone attack on the Black Sea Fleet in Sevastopol (Bachega & Gregory, 2022) summarize the ongoing rivalry between the two states after the Russian invasion of Ukraine in 2022.

Indeed, as Andrew Foxall (2021, p. 3) pointed out, Russia regards itself as a great power and one of the most important countries in the world, while it considers the UK not as its equal but as a "*second-tier power*". In addition, the UK is seen as an "*unreliable international actor*" and a "*Russophobic country*". In this context, even though the UK is not a power that could pose a direct threat to Russia, due to the UK's close ties with the US and "[being] seen as central to the Western anti-Russian lobby" (United Kingdom Intelligence and Security Committee of Parliament, 2020, p.2), UK posed a significant direct threat to Russia's interests, especially in Ukraine.

With the many factors such as “UK's numerous support to Ukraine against Russia in many areas since 2014, the UK's position in the eyes of Ukrainians as the country that “does best” to provide help them against Russia's invasion (Munich Security Conference, 2023, p.24), becoming the first country that signed a long-term (ten years) security cooperation agreement with Ukraine on January 12, 2024 (Mills, 2024b, p.25) it would not be surprising that relations between Russia and the United Kingdom will continue to be based primarily on their relations with Ukraine. In this respect, considering Russia's view of the UK and the UK's strong alliance with Ukraine, which poses a significant threat to Russian interests, it is unlikely that bilateral relations will improve in the foreseeable future, especially if the UK continues to enhance its collaboration with Ukraine.

4.2. Trilateral Relations of the United Kingdom, China, and Hong Kong

The Anglo-Sino relations go back centuries, and more than any other European state, Britain has been playing a more active role in China in terms of politically, economically and militarily (Eisel, 2007, p. 4). The UK confronted China in the Opium Wars, colonized some Chinese territories (e.g. Hong Kong) and became involved in the Chinese Civil War that took place between 1945 and 1949 between Nationalists and the Communists (Encyclopaedia Britannica, 2024a). Although it was the early years of the Cold War and there was a threat from the Soviets to Europe, Britain had ended diplomatic relations with the Nationalist Government in Taiwan in 1950 and recognized the new communist Chinese government under the leadership of Mao Zedong (Eisel, 2007, pp. 4-5). In this respect, the United Kingdom and the People's Republic of China’s (PRC) official relations had started in 1950 when the United Kingdom recognized the PRC as the first major Western state (British Embassy Beijing, 2017).

To officially recognize communist China at such an early time, there were various reasons for the UK. First of all, Britain considered Chinese communism and Soviet communism different from each other, and China would not become a Soviet’s satellite state. In this regard, the close relations with China did not mean to help the Soviet Union. Also, by establishing close ties with China, the UK could pursue a balancing strategy against the Soviets. The second and most important reason was that

China had always meant economic interests for Britain. Accordingly, the UK, which has historically had close relations with China, was keen to restore its economic interests in China after the Civil War (Feng, 1994, p. 167). However, in the Korean War, China supported North Korea and Western states supported South Korea. Therefore, the war prevented the two countries' diplomatic relations from evolving further. Especially with the imposition of mutual sanctions, bilateral relations were frozen.

Since mutual sanctions were imposed; diplomatic relations between the two countries could not be fully established until 1972. Also, during the Cultural Revolution, a socio-political movement carried out by Mao Zedong in China between 1966 and 1976, Britain became one of the main targets of the anti-Western movement, and China-UK relations were negatively affected. While relations between the two countries were deteriorating, on the other hand, relations between China and other European states, especially with France, were improving. This situation was economically damaging for the UK, which prioritized economic interests in its relations with China. Therefore, the United Kingdom decided to change its policy toward China. In this respect, the UK decided to support China to regain its permanent seat at the United Nations Security Council (Eisel, 2007, pp. 5–10). The UK had supported the resolution of the US in 1961, which set conditions for a two-thirds majority vote in the UN General Assembly for China to regain its seat in the United Nations Security Council (UNSC). However, at the UN General Assembly in 1971, the UK voted against the US resolution, which indirectly supported China's legitimate representation at the UNSC on behalf of the whole of China (Lin & Tao, 2019). With this decision, as the UK had hoped, rapprochement between the two countries was started.

After this rapprochement, full diplomatic relations were established with the exchange of ambassadors in 1972 (Embassy of the People’s Republic of China in UK, 2010). Since then, the two countries have had two main agendas: Economic relations and Hong Kong. Indeed, As Peter Ferdinand (2000, p.29) pointed out, until the handover of Hong Kong to China on July 1, 1997, Anglo-Sino relations “were always coloured by Hong Kong". The Hong Kong issue plays a fundamental role in the

relations between the two countries. To understand why Hong Kong has such a role, it is necessary to review the history of Hong Kong.

As parties of the First Opium War, China and Britain fought between 1839-42 and the China (Qing dynasty) was defeated. As a loss of the war, China ceded Hong Kong Island to Britain. After the Second Opium War, which took place between China and Britain, as well as France from 1856 to 1860, China ceded the southern part of the Kowloon Peninsula bordering Hong Kong (Encyclopaedia Britannica, 2024b). In addition, China "granted a 99-year lease of the new territories on the mainland of China" to Britain in 1898 (United Kingdom Parliament, 2014). Accordingly, all of the territories were combined to form what we today call Hong Kong, which was a British colony until 1997. After the establishment of diplomatic relations in 1972, there were 25 years remaining until the lease expired. Therefore, during these 25 years, the handover of Hong Kong to China occupied almost all the meetings of the two countries' officials.

In this respect, On 19 December 1984, the two countries signed the "Sino-British Joint Declaration" that established the principles of handing over Hong Kong to China. Based on this Joint Declaration, Hong Kong would be governed as a Special Administrative Region (SAR) of China. According to this system, called "One Country, Two Systems", Hong-Kong would become part of China and Beijing would be responsible for its defence and foreign affairs while Hong Kong would have its autonomy by retaining its control over currency, taxation, customs, cultural and economic relations with third states, legislative and independent judicial power. Moreover, according to the agreement, the social and economic systems of Hong Kong would remain unchanged for 50 years following the handover (United Kingdom House of Commons Foreign Affairs Committee, 2019, p. 34; Kaiman, 2014).

With the handover of Hong Kong to China, as Shaun Breslin (2004, p. 409) emphasized, *"almost overnight, the single biggest issue that had influenced UK–China relations for over a decade [was resolved]."* From 1997 to the mid-2010s, it can be said that bilateral relations were totally shaped by economic relations. During this period, the economy was given high priority in bilateral relations and crises/tensions between the two countries were not allowed to undermine the economic relations.

Therefore, issues between the two countries were mostly ignored and underplayed in favour of economic interests. For instance, in response to violence and clashes between demonstrators and police during anti-government protests in Tibet in 2008 (Watts, 2008) the United Kingdom stated its concern about the human rights and criticized the handling the protests. However, to prevent tension between the two countries, the UK Foreign Secretary stated that the United Kingdom considered Tibet as part of the People's Republic of China and did not support Tibetan independence (United Kingdom Parliament, 2008). As the Tibet crisis demonstrates that, in the coming years, the human rights issue would be a hot topic between the two countries over the human rights violations and abuses against Uighur Muslims in Xinjiang (Waitzman, 2023); however, it was carefully addressed so as not to undermine bilateral economic relations.

In parallel to the UK Government's strategy paper on China, which was launched in 2009 and which identified China as a "*major priority*" for the UK in the years ahead (United Kingdom Parliament, 2009), the UK sought closer ties with China in order to boost economic development between the two countries in the early 2010s. With this aim, David Cameron visited China in 2010 with more than 50 British business leaders and several ministers. The delegation to China was the largest British trade delegation ever to visit China, and numerous trade agreements were signed between the two countries (United Kingdom Prime Minister's Office, 2010a). During this visit, former Prime Minister David Cameron also delivered a speech at Beida University in Beijing, underlining the importance of strong relations with China for the UK:

> *"We want a strong relationship with China […] In the argument about how to react to the rise of China I say it's an opportunity […] China's success - and continued success - is good for Britain and good for the World (United Kingdom Prime Minister's Office, 2010b)*.

This visit was the first step in a "golden era" in bilateral relations that was to last for almost a decade. However, there were two major developments that took the bilateral relationship to the next level: "UK's support for the establishment of the China led Asian Infrastructure Investment Bank (AIIB)" and "Chinese leader Xi Jinping's visit to UK in October 2015". To promote closer political and economic relations with the world's fastest-growing markets – *Asia Pacific region* – as a first major Western country, the UK announced its intention to become the prospective

founding member of AIIB (United Kingdom HM Treasury, 2015b). Although this statement was welcomed by China; the US, which criticizes the UK publicly very rarely, voiced its unease about the UK's intention. In response to the UK's decision, a US official stated "*We are wary about a trend toward constant accommodation of China, which is not the best way to engage a rising power*" (Watt et al., 2015). Despite US criticism, three months later, on 29 June 2015, the UK signed the "founding agreement of the AIIB in Beijing (United Kingdom HM Treasury, 2015a). The UK's signing of the founding agreement of the AIIB took bilateral relations to the next level; however, it was the Chinese leader Xi Jinping's visit in 2015 brought the bilateral relationship to its highest point. During Xi Jinping's visit, the two countries committed to "building a global comprehensive strategic partnership for the 21st century" that ushered in a golden era of bilateral relations (United Kingdom Foreign & Commonwealth Office, 2015).

In 2015, UK-Chinese bilateral relations were in their golden era; however, since then, bilateral relations have started to transform into more bitter and strained relations. In a report on "UK-China relations" prepared by the International Relations and Defence Committee of the UK House of Lords (2021, pp.12-16) the reasons for the transformation in bilateral relations were explored, and different domestic and external factors were underlined. The main domestic factor was identified as Brexit and the change of the prime minister in the aftermath. During the David Cameron era, the UK focused more on economic relations, whereas Theresa May's government was "*much more conscious of the security dimensions of the relations*". On the other hand, the main external factors were China's more assertive and nationalistic stance on national sovereignty and territorial integrity under Jinping's rule. In this regard, China's policy of consolidating its control over Hong Kong and its increasing assertion of military power over the China Sea and Taiwan have been the main factors that have strained relations. Moreover, another important external factor was the shift in US policy towards China after Donald Trump, who was sceptical towards China, became US president in 2016. During the Trump era and his successor Biden, the US adopted a more competitive approach towards China. Therefore, the pressure of the US on the UK and due to the importance of the special relations with the US, the UK had to recalibrate its policies towards China. Since having good and strong relations with the US is the most important security interest for the UK, the US' pressure on the UK to

change its policy towards China was an important external factor for the UK, as will be discussed below in the case of Huawei. Therefore, while there was a period under David Cameron when a mercantilist approach was adopted and economic relations with China were prioritized; incidents in the post-2016 period have led the UK to prioritize security concerns over economic interests.

In parallel, according to Eren Waitzman (2023) who is researcher at the UK House of Lords, the tension in bilateral relations after 2016, were experienced on five issues: Hong Kong, geopolitical differences, human rights concerns, cybersecurity, and sanctions. In this context, the next section will examine the UK-China relationship through these five issues, especially Hong Kong, in order to understand how the bilateral relations has deteriorated from the golden era to tense and strained level.

4.2.1. Straitened Relations Between United Kingdom and China Over Hong Kong

In the early post-Brexit period, the two countries' relations continued without significant change. In fact, it should be underlined that the UK sought to preserve good relations with China in order to avoid economic damage, particularly in the wake of Brexit. Any tension would have been much more economically devastating for the UK than China. Accordingly, in the post-Brexit period, both countries took steps to maintain good relations and statements of officials by both countries highlighted the continuation of the golden era. In this respect, on 20 December 2016, former UK Foreign Secretary Boris Johnson hosted Chinese State Councillor Yang Jiechi. After the meeting, both parties “reaffirmed their commitment to working together under the Global Strategic Partnership” (United Kingdom Foreign & Commonwealth Office, 2016). Also, in the following months, the commitments to strategic partnership and preserving the golden era” were reaffirmed after the meeting between UK Prime Minister Theresa May and Chinese President Xi Jinping’s foreign policy adviser (United Kingdom Prime Minister’s Office Press Release, 2016).

The emphasis on “preserving the golden era in bilateral relations” was reaffirmed by the two countries' officials at almost every opportunity in the following period. For instance, even during the phone call between the two countries' leaders after North Korea's nuclear tests in September 2017, the two countries’ intention to continue the

"Golden Era" of bilateral relations was highlighted "(United Kingdom Prime Minister's Office, 2017a). Moreover, after six months of this phone call, two leaders spoke over suspected chemical attacks in Douma in Syria. Unsurprisingly, they also again reaffirmed their "commitment to a "Golden Era" of UK-China relations and a deeper strategic partnership"(United Kingdom Prime Minister's Office, 2018). The following statement of the UK's PM May, in fact, reveals why the two countries need to emphasize constantly that the golden era in relations should continue: "*The PM also noted the need to recognise and respect the international law of the sea, in the context of adherence to the wider rules-based international systems*" (United Kingdom Prime Minister's Office, 2018). This phone call was perhaps the first signal that the golden era was coming to an end. Although there were reassurances that the good relations between the two countries would continue, Theresa May's point that "the need to recognize and respect the international law of the sea" was in fact the first official signal of Britain's displeasure with China's actions in the China Sea and the early sign that there is a risk that bilateral relations could deteriorate over geopolitical events.

Not long after this signal, about two months later, another, but this time more explicit, signal was given by the United Kingdom, which had the potential to deteriorate relations. It was announced that "*British and French warships will sail to the disputed South China Sea*" (Jennings, 2018). Due to this decision, there was minor tension between the two states, but both sides also refrained from damaging the economic relations. Among these concerns, ahead of former UK Foreign Secretary Jeremy Hunt's visit to China, he stated that "*[since] UK leaves EU, [UK will become] ever more outward-looking and [deepen] this vital partnership for the 21st century*" (United Kingdom Foreign & Commonwealth Office, 2018a). During his visit, significant new trade agreements worth more than £9 billion were signed (United Kingdom Foreign & Commonwealth Office, 2018a). By this visit, it was evident that UK tried to balance economic and security concerns. While it was trying to maintain good economic relations with China to minimize the economic loss it would suffer after leaving the EU, on the other hand, it could not ignore security concerns. In a choice between the two, even if the economy had the upper hand, it was not as strong as it used to be, and there was a significant possibility that the choice between the economy and security would change.

Nevertheless, two weeks after the British Foreign Secretary's visit to China, former UK Defence Secretary Gavin Williamson's speech in Washington, indicated explicitly that Britain would prioritize security. In his speech, Williamson stated Britain's desire to pursue its position as a global power by investing in sea power. Furthermore, in response to the underestimation of the UK's power, he stated that the UK would modernize and counter threats from states such as China and Russia so that the UK would never be underestimated (Grady, 2018). Thereafter, one month later, a British warship sailed close to the Paracel Islands in the South China Sea where China claims sovereignty. In the aftermath of this incident, China's Foreign Ministry condemned the UK by stating that British ships entered China's territorial waters without permission, so that they violated Chinese law and relevant international law and infringed on China's sovereignty. Moreover, China also urged the UK to end its provocative actions which harm the "*broader picture of bilateral relations and regional peace and stability*" (The Guardian, 2018). In response to Chinese criticism, the UK insisted that its warship was conducting a "freedom of navigation exercise" in accordance with international law (BBC News, 2018).

The tensions in the South China Sea also spilt over into cyberspace. On December 20, 2018, the UK announced that the Chinese advanced persistent threat group – APT 10 – conducted cyber-campaigns on behalf of the Chinese Ministry of State Security to obtain sensitive trade secrets data and the UK's and its allies' intellectual property. In his statement, UK Foreign Secretary Jeremy Hunt stressed that the cyber campaign by the Chinese hacking group was one of the most serious and large-scale cyber intrusions against the UK and its allies. In response to this cyber campaign, he stated that "*Our message to [states that enable these] activities is clear […] We will expose your actions and take other necessary steps […] Chinese government are not upholding the commitments China made directly to the UK in a 2015 bilateral agreement"*(United Kingdom Foreign & Commonwealth Office, 2018b).

Indeed, this statement was a breakthrough because after implicit criticism of China's actions in the China Sea, China was directly held responsible for an action in an official press statement by the UK. Moreover, the phrases used by Jeremy Hunt in his statement, "together with allies", and "China's failure to commit to the 2015

bilateral agreement", were explicit indicators of the shift in relations. Geopolitical differences and cybersecurity, which are two of the five elements highlighted by Eren Waitzman (2023) as major challenges between the two countries, have been apparent. In addition to these two problems, Hong Kong's pro-democracy protests and follow-up events, as well as human rights concerns, played catalytic roles in the deterioration of the bilateral relationship.

In their analysis for the Council on Foreign Relations, Lindsay Maizland and Clara Fong (2024) argue that freedom in Hong Kong has declined since 1997 because when China increased its control over Hong Kong, protests erupted against the decision, and in response to these protests, China increased its control even more. In fact, this dilemma summarized what happened in Hong Kong between 2019 and 2020. As mentioned above, according to the principle of "one country, two systems", Hong Kong has a separate jurisdiction from Beijing. However, on April 3, a draft was submitted to the Hong Kong legislature that would allow the extradition of criminal suspects from Hong Kong to mainland China (The Economist, 2019). The bill was considered as evidence that China pursued to increase its control over Hong Kong (BBC News, 2019b). Hence, the proposed bill led to the start of months of protests against this bill. In June 2019, Hong Kong witnessed the largest protests and the clashes between protesters and police became increasingly violent (Cheung & Hughes, 2020). As a result of these growing protests and rising violence, Chief Executive Carrie Lam decided to withdraw the bill by stating that her decision was also supported by China. Nevertheless, her decision did not help to stop the protests. The protesters continued to demonstrate by demanding full democracy and an independent investigation into police actions, until the outbreak of Covid-19 in 2020 (Cheung & Hughes, 2020).

The reported police brutality and excessive usage of nonlethal weapons (e.g. rubber bullets and tear gas) during the protest that erupted due to unifying fear with China Alan (Mahtani & McLaughlin, 2019) drew international attention to the region (Maizland & Fong, 2024). Unsurprisingly, the strongest criticism of the proposed bill and the violence against protesters came from the United Kingdom. In opposition to this draft law and the brutal crackdown on demonstrators, the UK stated that the 1984 Joint Declaration must be respected. In response to the UK's reaction, the Chinese Ambassador to the UK, Liu Xiaoming, said that "[Joint Declaration] is a historical

document [and] completed its mission" (Embassy of the People's Republic of China in the UK, 2019). Chinese Ambassador's statement prompted further reaction from the UK. In a speech to Parliament, The Minister for Europe and the Americas, Alan Duncan stated that:

> "*The UK is fully committed […] One Country - Two Systems Principle […] We reject the Chinese Government's assertion that the joint declaration is an "historic document by which they mean that it is no longer valid*" (United Kingdom Parliament, 2019a).

In parallel to Duncan's statement, former UK PM Theresa May also stated the importance of the preservation of Hong Kong's high degree of autonomy and urged China to respect to the legally binding Joint Declaration of 1984 (United Kingdom Parliament, 2019b).

With the outbreak of the Covid-19 pandemic, the Hong Kong crisis was frozen for a short time. However, it was anticipated that tensions between the two countries would increase after UK Foreign Secretary Dominic Raab said that "*we cannot have business as usual [with China] after the crisis, and we will ask hard questions*"(Donaldson & Mayes, 2020). Shortly after this announcement, China introduced the "National Security Law" in Hong Kong by taking advantage of the lockdowns and assuming that there would be no protests against it. In order to prevent a repeat of the protest in Hong Kong similar to the 2019 pro-democracy protests, China made illegal a wider range of dissenting by criminating anything that was considered "secession", "subversion", "terrorism" and "collusion with foreign or external forces". Anyone who commits any of these four crimes can be imprisoned for life (BBC News, 2020a).

Chinese officials defended the law by emphasizing that it was highly necessary for the protection of national security in Hong Kong (Cheung & Hughes, 2020). On the other hand, against this law, there were many criticisms that the "new law brings the end of Hong Kong" by severely undermining the One Country-Two System framework and causing Hong Kong to lose a significant degree of autonomy (Kuo, 2020; Kuo & Davidson, 2020). In response to this law, the UK protested China and stated that the new law was a "clear and serious breach" of the Joint Declaration and International Law and undermined the autonomy of Hong Kong. Moreover, the UK

announced a "*new visa type*" which was a route to British citizenship for people in Hong Kong (United Kingdom Parliament, 2020). Under this new type of visa, which the UK is offering only to people in Hong Kong, people with British Nationals (Overseas) status - BN(O) – (a status is a form of British nationality created for people from Hong Kong so they could retain a form of British nationality after Hong-Kong handed over China in 1997 (United Kingdom Home Office, 2024)) and their dependent family members (estimated at 5.4 million out of 7.5 million eligible Hong Kong residents) would be able to live in the UK for up to five years, after which they could apply for permanent residence and British citizenship (Gower & Kirk-Wade, 2021, p. 3). In 2021, around 90,000 people in Hong Kong applied for the Hong Kong British National (Overseas) visa, which was officially launched on January 31, 2021 (Kwan, 2021). Following the UK's visa strategy, China's Foreign Minister called on the UK to "correct its mistakes immediately" and warned the UK not to interfere in China's "domestic affairs" (BBC News, 2020c). Moreover, in response, China announced that the passports of BN(O) would no longer be recognized by China (Hale, 2021).

While the Hong Kong issue was occupying the agenda of the two countries, there was also the Huawei banning crisis between the two countries. Under the Trump administration, by blaming Huawei for posing a dual threat to national and economic security, the US banned national companies from selling products and services to Huawei without US government approval (US Mission China, 2019). Huawei was the target of the US due to various reasons such as being founded by a former Chinese army officer (Bowler, 2020); allegation for close ties with Chinese intelligence (Westbrook & Kaye, 2018); increasing findings of severe vulnerabilities of the company's products which increased the suspicions that the company was helping the Chinese government (Bowler, 2020); the role of the Huawei as "world's biggest supplier of telecoms gear" (The Economist, 2018) and forefront company to dominate the market for the next generation of wireless communications, called 5G (Araya, 2019). In this regard, the US has restricted technology exports to Huawei (Silva, 2024) and has encouraged its allies not to use Huawei products.

One of the countries where this pressure was felt the most was the United Kingdom due to its special relations with the US. The US increased its pressure on the UK not to use the 5G technology of Huawei (Stubbs & Alper, 2020). Accordingly, the

US stressed that transatlantic intelligence sharing would be at risk if Huawei infrastructure were used in the UK, and special relationships could deteriorate. Also, it was stated that it would be "*nothing short of madness*" for the UK to give this authorization to a Chinese company (Sabbagh, 2020). In response to this pressure from the US, former UK PM Boris Johnson stated that they would not use infrastructure that would damage national security or the ability to work with Five Eyes intelligence partners, while on the other hand, in order for the British people to have a much better Internet, those who say not to work "with a company" should also say the alternatives (Proctor, 2020). With this statement, Johnson was indeed admitting that there was no viable alternative to Huawei for the UK despite there was security concerns.

On the other hand, China exerted severe pressure on the UK, sending threatening messages to the UK to refrain from banning Huawei. For example, the Chinese ambassador to the UK stated that if the UK banned Huawei, it would "*send a very bad message not only to Huawei but also to Chinese businesses*" (Embassy of the People's Republic of China in UK, 2019). In addition, Chinese Ambassador (Xiaoming, 2020) also warned that banning Huawei would take the UK backwards technologically and undermine Chinese and investor confidence in the cooperation between the two countries. Indeed, the warnings coming from China signalled that if the UK could not resist the pressure from the US and decide to ban Huawei products in 5G infrastructure, the China would take serious economic decisions and economic relations -perhaps the last thing that could be described as positive between the two states- would be seriously jeopardized.

Accordingly, in order to find middle ground between the two states, the UK decided to let Huawei be used in the UK's 5G networks, but the company was banned from supplying kits to sensitive parts of the network (Kelion, 2020). In other words, although it could not satisfy both sides, the UK tried to take a step that would not completely break relations with both sides. Nevertheless, the Huawei decision triggered a fierce backlash from US officials. By implying that the special relationship between the two countries was at risk because of just a Chinese phone company, the US expressed its disappointment that an unreliable vendor was allowed to be present in the British market and that this decision would seriously damage the special relationship between the two countries (Stewart & Sabbagh, 2020).

Nevertheless, six months later, the UK reversed its earlier decision, made in January 2020, and imposed a ban on operators in the country from purchasing any Huawei equipment after 2020. Furthermore, the UK decided to completely remove Huawei's 5G equipment, which had already been installed within seven years. (Sandle & Faulconbridge, 2020). To explain the reason for this U-Turn decision, former UK Digital Minister Oliver Dowden said that "*it was not an easy decision to make [however] it is the right one for the UK telecoms networks, for our national security and our economy, both now and indeed in the long run*" (Sandle & Faulconbridge, 2020). As Dowden underscored, it was a very difficult decision for the UK because after taking this decision, the UK knew that the golden era between the UK and China was completely over (Woodcock, 2020). As expected, China's reaction to this U-turn decision was aggressive. Chinese Ambassador to the UK, Liu Xiaoming, stated that the relations between the two countries were "*seriously poisoned*" and that "*it was a dark day*" in relations, but it was a "*much darker day for the UK*" because it missed an important technological development opportunity (BBC News, 2020b). Moreover, recognizing that the US played an active role in the background of this decision, the Chinese Ambassador stated that the UK was *"at a critical historical juncture*"; the UK should have had "*enough wisdom*" and should not have allowed *"anti-China forces and Cold War warriors to kidnap China-UK relations*" (BBC News, 2020b).

Indeed, in 2021, the British government would clearly indicate which side it would choose over the "critical juncture" and give significant clues about its foreign policy for years to come. Accordingly, in March 2021, the British Government published a policy paper titled "*Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy*," which outlined the government's vision for the UK's role in the world over the next decade. In the report, the foreign policy strategy towards China was defined as pursuing a "*positive trade and investment relationship" while "improving [its] ability to respond to the systemic challenge that [China] poses to [its] security, prosperity and values - and those of [the UK's] allies and partners*" (United Kingdom Government, 2021, p.22). In this regard, it was observed that the UK Government considered China as a threat to the international system. In 2023, the policy paper was revised under the Rishi Sunak

administration, and at this time, China's threat to the international system was clearly articulated as follow:

> "*China poses an epoch-defining challenge to the type of international order we want to see, both in terms of security and values – and so our approach must evolve […] And we are taking new action to protect ourselves, our democracy and our economy at home* (United Kingdom Government, 2023, p.3)

Another important issue concerning China in this report was the UK's "*tilt towards the Indo-Pacific*" policy towards the region. According to the report, it was highlighted that the "*UK will pursue deeper engagement in the Indo-Pacific*" region which was vital to the UK's "economic and security" interests and [its] global ambitions" (United Kingdom Government, 2021, p.22,66). To pursue its goal towards the region by 2030, the UK would try to have its broadest and most integrated presence in the region with European partners and would commit to closer and deeper partnerships for the long term (United Kingdom Government, 2021, p.66).

The first reflection of the UK's new foreign policy towards the region was seen in 2021 when the UK, the US and Australia announced a joint security pact. On 16 September 2021, the UK, the US and Australia announced a trilateral security pact (AUKUS) that brought these three states together to work closely on key defence capabilities, including submarine technologies (helping Australia build nuclear-powered submarines) and advanced technologies such as quantum technologies and artificial intelligence (Tobin, 2024). In response to the historic AUKUS pact, which was considered as a security pact for encountering China in the region; China condemned the three countries for being "*extremely irresponsible*" and acting with a "*Cold War mentality*". China also stated that this agreement would increase the arms race and damage regional security and stability (BBC News, 2021). While it was clear with the AUKUS agreement that the UK would adopt a more aggressive and confrontational attitude towards China in the region, ten days after the announcement of the agreement, the British Warship passed through the Taiwan Strait, which China considers as its internal territorial water. During this passage, the Chinese navy "followed and warned the British warship" and condemned the UK as "engaging in behaviour that "harboured evil intentions" (Cheshire, 2021).

While the tension in the region had been significantly escalating, Russia's invasion of Ukraine in February 2022 heightened concerns about potential military actions by China against Taiwan. There are substantial indicators and reasons for this concern such as China’s significant military build-up in the region; entirely arming at least three islands in the South China Sea with a wide range of different equipment (POLITICO, 2022); claiming the arming of islands as necessary for its national defence by asserting the sovereignty over the islands (AP News, 2022); engaging in numerous grey zone actions such as sending numerous fighter jets into Taiwanese airspace (Davidson, 2022); and declaring "to take over this self-governing territory" by force if necessary (Gardner, 2023).

This concern was heightened by China's decision to allow its military to conduct "armed operations" outside the country. This decision raised concerns because Putin had announced before the start of the invasion of Ukraine that Russia would launch a "special military operation". In this context, legalizing the deployment of armed forces abroad was seen as an attempt to "define a future military intervention in Taiwan as a non-war operation" (Birtles, 2022). Taiwan's Defence Minister Chiu Kuo-cheng also stated that the Russian-Ukrainian war would be an example for China. According to the minister, China would take notes from Russia's failure to make progress, and therefore, China would "definitely seek speed" (Reuters, 2023b).

As the Chinese threat to Taiwan intensified, the United Kingdom enhanced its relations with Taiwan. Accordingly, the Foreign Affairs Committee of the House of Commons reports described Taiwan as an already independent country under the name of the Republic of China (Lau, 2023). Although this report did not reflect the official foreign policy of the UK, it was very important for bilateral relations that Taiwan was recognised as an independent state in an official document. In addition to this incident, another development that could further strain the two countries was the visit of Lizz Truss as a former UK PM to Taiwan at the invitation of a think tank. In her speech, she underlined that the biggest state-based threat to the UK's economy was China and that there was no greater threat than Chinese global dominance. Also, she urged the UK government to take a tougher stance against China (Boyle, 2023). In response to this visit, China urged British policymakers to stop political shows on the Taiwan issue; however, the visit did not cause a crisis between China and Britain as expected

because China considered this visit a "dangerous political show" and stated that "it would not harm bilateral relations (Badshah, 2023).

What really deteriorated bilateral relations over Taiwan was the "*Enhanced Trade Partnership Agreement*" between the UK and Taiwan, which aims to expand economic and trade ties between the UK and Taiwan (Taiwan Today, 2023). Since it was a diplomatic agreement and the UK did not officially recognize Taiwan, the UK was criticized by China. In this regard, the Chinese ambassador to the UK stated that states with diplomatic relations with China should not have any official contact with Taiwan and that the UK should stop strengthening its relations with Taiwan under the excuse of trade cooperation and exchange of officials (Reuters, 2023b).

In parallel with its "tilt to the Indo-Pacific" foreign policy, the UK has been trying to establish close relations with the states in the region to balance China. However, China considers the UK's strategies to be a part of the US's Asia strategy. Also, since the UK ruled out any military aid to Taiwan and stated that the UK has no plans to recognize Taiwan (Curtis, 2024, p.5); China did not feel a direct threat to the UK. Moreover, it is hard to tell that China also considers the United Kingdom as a great power. In other words, although the UK describe China as a systemic threat, the UK does not pose a similar threat to China. This perception of China was indeed echoed by the words of China's media spokesman in his interview in response to the question "How would you regard your relationship with Britain":

> "*First of all, between China and Britain, from the Chinese perspective, Britain is not a rival, it is not a competitor […] What do China and Britain compete with? […] So I think the British government should not overestimate its impact on the global scene and view China as a rival. China is a fact; China is a mega-trend for Britain to live with and get along with*" (Nicholson, 2023).

Hence, the main factors that have spoiled the relations between the two countries were not the security issue but political and economic factors in the eyes of China. In this regard, the main issues for China were Hong Kong, which China considers the UK directly interfering in its internal affairs and undermining its sovereignty, and the banning of the usage of Huawei kits in the 5G infrastructure, which harmed Huawei's and China's interests and prestige. That is why China reacted strongly to the United

Kingdom when its national sovereignty and economic interest were undermined and threatened by the United Kingdom rather than the UK's security threats.

On the other hand, the UK mostly tried to balance its economic and security interests in relations with China. Especially after Brexit, which significantly dampened its economy, the UK had to overlook the security issues in favour of its economic interest. Nevertheless, the UK changed its approach towards China due to internal and external factors, as discussed above. In this regard, China's increasingly assertive policies and activities in the South China Sea, exploitation of its economic power for its political interests, violation of the "one state, two systems" framework by undermining the autonomy of its former colony Hong Kong, human rights violations and abuses -especially against the Uyghurs in Xinjiang- and numerous cyber-attacks have persuaded the UK to reconsider its bilateral relations with China. In particular, with the recent (May 2024) Chinese cyber-attack that hacked the UK Ministry of Defence – which exposed the personal details of thousands of current and former members of the armed forces (amounting to around 270,000 people) (Coates, 2024; Keate & Boscia, 2024) – it would not be a prophecy to say that bilateral relations will take a more negative course in the near future. Thus, as this recent cyber incident indicates, as bilateral relations between the two countries continue to deteriorate (especially due to increasing cooperation between the UK and Hong Kong), cyber-attacks will continue to be employed to a greater extent as a foreign policy tool by China.

4.3. The Trilateral Relations the United Kingdom, Iran and Israel

> "*There are hungry wolves ambushing us and removing the diplomatic cover from their faces. They are showing their real faces. And the most evil of them all is the British Government*"
>
> "*Ayatollah Ali Khamenei*"
> (McElroy, 2009)

The United Kingdom and Iran's relations have a long and complex history, which consists of almost all kinds of historical events: from an invasion to organizing a coup, an embassy siege and numerous diplomatic crises (Lyons, 2015). Because of all these historical encounters, Iran's perception of the United Kingdom, especially in the post-1979 period, was clearly expressed in the quote above from former Iranian Supreme Leader Ayatollah Khamenei's speech. From Iran's perspective, rather than

being a direct threat to Iran, the UK has been a country that provoked domestic turmoil in Iran by supporting anti-regime elements. Hence, the fox, is known for its sly and cunning behaviour and due to its former imperial power, the “old fox” has been used to describe UK in Iranian media (Pourparsa, 2015). On the other hand, in the eyes of the UK, Iran is a country that has posed a direct threat to its interests in the Middle East by supporting proxy powers across the Middle East, targeting its allies in the region and, most importantly, through the possibility of obtaining nuclear weapons. Therefore, UK-Iran relations are not just a relation between two countries, but a type of relation in which many bilateral relations are intertwined, and many different elements affect each other even if they seem different from each other. Therefore, it is not possible to isolate UK-Iran relations from many different regional factors, UK-Israel relations in particular. In order to understand the multi-dimensional nature of the relations between the two countries, it would be appropriate to begin historical section with the joint British and Soviet invasion of Iran in 1941.

One of the fundamental causes why Iran distrusts the United Kingdom and regards it as a constant threat stemmed from Iran’s invasion by the United Kingdom and the Soviet Union in 1941. At the beginning of WW2, Iran decided to remain neutral. This policy was welcomed by Britain. However, German soldiers were present in Iran even after the start of the war, and Iran had refused to expel Germans. It was because of the fear of displeasing Germany after Germany started to offence towards Russia and there was the possibility of the Germans to come until Baku. In addition to the presence of German soldiers, Iran was in a strategic geo-political position, which was an important route for supplying aid to the Soviets. Accordingly, Britain and the Soviets decided to invade Iran in 1941 (Eshraghi, 1984, pp. 27-30).

After World War II, the British and Soviet troops withdrew from Iran in 1946. After Mohammad Mosaddegh - the leader of the National Front Party, which sought to reduce the power of the clerics and the monarchy - became prime minister in 1951; he subsequently decided to nationalize a British-owned Anglo-Iranian Oil Company (Abrahamian, 2013, p. 2). However, as a main beneficiary of Iranian oil, the United Kingdom reacted strongly to this decision. In response, the UK imposed an economic embargo on Iran and urged the International Court of Justice (ICJ) to review the case. However, the ICJ decided not to intervene and implicitly supported Iran's decision

(Afary et al., 2024). The crisis did not end until 1953 when the Central Intelligence Agency (CIA) and the British Secret Intelligence Service, also known as MI6, organized a coup to overthrow Mosaddegh. With these two major events, the occupation of Iran in 1941 and the intervention in Iran for the coup, the roots of hostile sentiment towards Britain had been planted (Abrahamian, 2013, p. 2).

In 1953, an agreement was reached on Iranian oil. Accordingly, an international consortium was established for the exploitation of Iranian oil, replacing the Anglo-Iranian Oil Company. The name of the consortium was changed to The British Petroleum Company (BP) in 1955. The company's activities in Iran continued until the 1979 Islamic Revolution. Therefore, between 1954 and 1979, Iranian oil was controlled by an international consortium in which the UK and the US were major partners (Bolat, 2013, pp. 72–73). However, with the Iranian Revolution of 1979, the new regime nationalized the company without any compensation. As Gökhan Bolat emphasizes, the fact that Western states had such control over Iranian oil until the 1979 Iranian Revolution exacerbated the American-British-Israeli-cantered enmity against the West that its impact today is felt deeply (Bolat, 2013, pp. 72–73).

In the aftermath of the oil crisis, there was a rapprochement in relations between the two countries, which remained relatively stable until the 1979 revolution. In 1955, the United Kingdom and Iran joined (along with Pakistan and the US later) the Baghdad Pact, which was a cooperation pact established in 1955 by Turkey and Iraq so as to balance the influence of the Soviet Union in the Middle East. With the withdrawal of Iraq in 1959 after the Coup in Iraq in 1958, the centre was moved to Ankara, and its name also changed to Central Treaty Organization (CENTO) (Yeşilbursa, 2020, pp. 854–856). Moreover, Shah Mohammad Reza Shah Pahlavi visited the United Kingdom in 1959 and two years later, Queen Elizabeth II visited Iran in return (Davar, 2022). In the following years, bilateral relations seemed stabilized however, it was severely shaken by the Iranian Revolution in 1979.

After the Iranian Revolution in 1979, Iran's stance toward Western states, especially the United States and Israel, significantly strained the bilateral relations between the United Kingdom and Iran. Initially, the United Kingdom closed its embassy in Tehran. Additionally, in 1980, a crisis occurred in the United Kingdom,

although it did not directly impact the relations between the two countries. In April 1980, six Iranian-Arab Gunmen stormed the Iranian Embassy in London and took 26 hostages to demand the release of Arab prisoners held in Iran and the independence of Khuzestan where a region in southern Iran. On the sixth day of the siege, gunmen killed the Iranian cultural attaché and threw his body off the embassy. Following this incident, British Special Air Service carried out a rescue operation called Operation Nimrod that rescued 19 hostages while 5 out of 6 gunmen were killed and one was detained (National Army Museum, n.d.; SOF News, 2023). This historic event was followed by the Iraq-Iran war, which would shape bilateral relations for almost a decade. In the early phase of the war, the UK proclaimed its neutrality, but later, the UK changed its position to “impartiality”. Due to its impartiality, the UK also refused to supply lethal weapons to both sides, whereas there was criticism toward the UK’s narrow definition of the lethal weapon (Gray, 1988, pp. 421-422). The war ended with a ceasefire in 1988, amidst a growing number of commercial ships being hit in the Gulf and the idea of arms embargoes against Iran for it repeatedly refusing the UN Security Council’s calls for a ceasefire (Gray, 1988, pp. 427-428).

With the end of the war, the embassy was re-opened in 1988. However, relations were strained again a year later by the publication of the book "The Satanic Verses" by British-Indian author Salman Rushdie. Since the book fictionalized the life of the Prophet Muhammad, Iran's supreme leader, Ayatollah Khomeini, issued a fatwa ordering Muslims to kill the author (Erlanger, 2022). Since Iranian leader’s fatwa urged Muslims to kill its citizens, the UK condemned the Iranian leader; and tried to hide and protect his citizens for years. In 1998, Iranian President Mohammad Khatami declared that he no longer supported the killing of Salman Rushdie. Since then, the author began to participate in some public events. Almost three decades later, in 2022, he was stabbed in New York, and Britain discussed imposing sanctions on Iran for its possible involvement in the stabbing (Blackall, 2022). It is unknown whether Iran had any role in this incident; however, the blame of the UK for Iran, even after three decades, demonstrates how deeply rooted this case is in bilateral relations.

Bilateral relations in the 2000s were marked by the September 11 attacks and the invasion of Iraq. Indeed, former US President George W. Bush's famous phrase "axis of evil" - Iraq, Iran, and North Korea - in his 2002 speech was a clear indication

that UK-Iran relations would also be shaped by this vision. In 2003, the US invasion of Iraq, along with the UK, over Iraq's alleged possession of weapons of mass destruction, raised the alleged prospect of a pre-emptive strike against Iran as well. However, the lack of evidence of the existence of these weapons in Iraq reduced the likelihood of an invasion of Iran and led to the implementation of policies aimed at preventing Iran from acquiring nuclear weapons. In fact, this led to the development of relations between Western countries and Iran in the post-2003 period in line with the framework for limiting Iran's nuclear capability, which continues even today (2024) as well.

Accordingly, after the invasion of Iraq, the US-led allies also increased pressure on Iran, especially after the International Atomic Energy Agency (IAEA) raised concerns about Iran's alleged nuclear weapons program due to Iran's failure to comply with its obligation to declare its nuclear material (Arms Control Association, n.d.). Although Iran claimed that its nuclear program was for civilian purposes only, Germany, France, and the United Kingdom drafted a resolution in 2004 condemning Tehran's reluctance to work with the IAEA inspectors. In this regard, the United Kingdom condemned Iran for "undermining confidence" in its nuclear program (BBC News, 2004).

Iran considers nuclear power as one of the pillars of its national power (France 24, 2022). One of Iran's primary goals in seeking nuclear capability is to enhance its security against its archenemy – Israel. Iran sees the US as the "Great Satan" and Israel as the "Little Satan," representing the US in the region (Motamedi, 2023). Additionally, Iran considers the UK's relations with Israel significant due to the UK's role in establishing Israel, its special ties with the US, joint operations and policies in the Middle East, and its support for Israel in the region. The United Kingdom has strategic and historical relations with Israel. The Balfour Declaration (1917) - British Foreign Secretary Arthur James Balfour's statement of British support for "the establishment in Palestine of a national home for the Jewish people"- is regarded as the founding document of the state of Israel that was established in 1948 after the UK withdrew from Palestine in 1948. Since then, although the relations between the two states have been volatile, the UK has been one of the most important supporters of Israel. In recent years, with the strengthening economic, military and diplomatic

relations between the UK and Israel, the two countries' relations "had never been better, and all past tiffs felt long forgotten," as Stephen Oryszczuk stated (2020). On the other hand, this increasing cooperation between the two states has negatively affected the UK relations with Iran. Therefore, the UK's government's unequivocal support for Israel in many cases has made the trilateral relations between Israel, Iran and the UK more evident. For instance, after Iranian President Mahmoud Ahmadinejad said in 2005, "Israel should be wiped off the map"; Ahmadinejad's "speech was immediately condemned by the US and Britain" (MacAskill & McGreal, 2005). In 2008, during his speech at the Israel Parliament, former United Kingdom Prime Minister Gordon Brown stated his support for Israel against Iran:

> *"For the whole of my life, I have counted myself as a friend of Israel […]To those who question Israel's very right to exist, and threaten the lives of its citizens through terror, we say: the people of Israel have a right to live here, to live freely and to live in security. [UK] will continue to lead […] to prevent an Iranian nuclear weapons programme [and stand] ready to lead in taking firmer sanctions [on Iran]. Iran has a clear choice to make: Suspend its nuclear weapons programme [or face] growing isolation and the collective response." (Blair, 2008; Voice of America, 2009)*

Moreover, a year after Brown's visit to the Israeli parliament, it was revealed that Iran had begun construction of another nuclear facility, despite the UN's call to suspend enrichment activities. Although Iran insisted that its activities did not violate UN regulations; the UK, US and France warned Iran to comply with the requirements and in case of failure to do so, to impose more severe sanctions (BBC News, 2009). Iran's repeated vows to destroy Israel, as in Ahmadinejad's statement, and the continuation of its nuclear program have raised concerns that Iran could develop nuclear weapons and use them against Israel. In this respect, 2010, as detailed in the previous chapter, a so-called US-Israeli cyber-attack, named Stuxnet, was launched against Iran's Natanz nuclear facility, severely damaging Iran's nuclear enrichment efforts by disrupting a significant number of the facility's centrifuges (BBC News, 2012).

Although Stuxnet damaged Iran's nuclear development, the IAEA reported in 2011 that there were some indications that Iran was developing nuclear weapons (Reynolds, 2011). Following this report, UK Chancellor George Osborne announced that the UK would impose new sanctions that cut off all financial ties with Iranian banks, as Iranian banks were funding Iran's nuclear program (BBC News, 2011b). In

response to this decision, Iran expelled British Ambassador and downgraded diplomatic ties (Dehghan, 2011). Moreover, after the UK's sanction decision, hundreds of protesters attacked to UK Embassy in Tehran. Following this attack, UK closed its embassy in Iran and expelled all Iranian diplomats and ordered to close Iranian Embassy in London (BBC News, 2011c).

As bilateral relations continue to be strained over the nuclear program, after years of negotiations, the P5+1 countries (Five UNSC permanent members; China, France, Russia, the United Kingdom, United States plus Germany) and Iran reached an agreement in 2015, known as "*Joint Comprehensive Plan of Action (JCPOA)*". According to this agreement, while Iran agreed to suspend certain activities and allow IAEA's intensified inspections; in return, UNSC's sanctions, multilateral and bilateral sanctions against Iran were lifted (Tobin, 2022). Following the signing of the deal, relations between Western states and Iran had softened and were relatively stable. However, Donald Trump, who was one of the critics of the JCPOA due to its benefits to Iran, became US president in 2018 and withdrew the US from the deal (Bozorgmehr, 2022). In his statement, Trump harshly criticized the deal for failing to stop Iran's proxy wars and missile program:

> *"The Iranian regime is the leading state sponsor of terror. [Iran] exports dangerous missiles, support fuels conflicts across Middle East [and] terrorist proxies and militias […] So-called "Iran deal was supposed to protect the US and our allies [however the deal] allowed Iran to continue enriching uranium [that enable Iran to acquire a nuclear weapon in the future]* (The New York Times, 2018).

In addition to withdrawing from the deal, the US also imposed significant sanctions (on critical Iranian sectors such as banking and the oil industry) that nearly led the JCPOA to collapse (K. Robinson, 2023). Despite the US's withdrawal from the agreement, Iran and the other signatory states declared that they would remain committed to the deal (Landler, 2018). However, the deal could not be expected to survive in the long term without the main pillar of the deal which was the US. At least, it was obvious that the functionality and effectiveness of this agreement would be very limited without the US even if no additional state withdrew from the agreement.

In 2019, Iran announced the partial break of its commitments to nuclear deal as a result of the growing US military presence in the Middle East and increasing pressure on Iran. Following Iran's decision, the United States decided to impose new sanctions against Iran (El-Ghobashy et al., 2019). While everyone was waiting for the tension in the region after the US withdrawal from the deal and Iran's partial withdrawal from it; on January 3, 2020, General Qassem Suleimani, one of Iran's most important figures, was killed by a US drone attack in Baghdad. Following the drone strike, the US took responsibility by announcing that the drone attack was a decisive act of defence and was carried out by President Trump's order (Borger & Chulov, 2020). In the aftermath of this attack, Iran made a very strong statement and declared that it would no longer abide by any restrictions related to the 2015 nuclear deal. Therefore, after Iran's statement, as BBC Defence Correspondent Jonathan Marcus emphasized that the nuclear deal "*on life support ever since the Trump administration abandoned it in May 2018, may now be in its final death throes*" (BBC News, 2020).

After Iran's decision, the E3 group (UK, France and Germany) that have tried to maintain the nuclear deal, also criticized Iran by stating that "*instead of reversing course, Iran has chosen to further reduce compliance with the JCPOA"* (United Kingdom Foreign & Commonwealth Office, 2020). While hopes for the deal were significantly diminished, following the election of Joe Biden as the new US president, there was a renewed optimism regarding the prospects of the deal. In this respect, in 2021, Joe Biden underlined that he would be ready to talk with Iran and return to the 2015 nuclear deal if Iran complies with its commitments. Moreover, he also eased several sanctions that were imposed to Iran under the Trump administration (Lee, 2021). After the relatively optimistic approach of the US towards Iran, the two countries met in Vienna on April 6, 2021, and agreed to return to the nuclear deal (Erlanger, 2021). Since then, there have been many discussions between the P5+1 countries and Iran; however, due to various incidents such as the Western states' constant criticism of Iran's human rights violations, the Russia-Ukraine war, the Hamas-Israel war, and the recent Iranian drone attack on Israel, the finalization of a new deal has failed. In this respect, unless there is a major change, it is unlikely that a new agreement will be signed in the near future it is unlikely that a new agreement will be signed in the near future (Loft, 2023, p. 5; K. Robinson, 2023).

Apart from the nuclear weapon issue between the two countries, as indicated in a report prepared by Philip Loft (2023, p.4) for the UK Parliament (House of Commons) titled “Iran's Influence in the Middle East”, UK's main concern about Iran was not limited to Iran's nuclear activities, but also Iran’s continuous support to its proxy network and armed groups across the Middle East. Since the Iranian revolution, Iran has supported an increasing number of fighting forces in the region and established a network called the *'axis of resistance'* in the Middle East (Vakil, 2023). This network, with Hezbollah at its heart, operates mostly in Iraq, Lebanon, Palestine, Syria, Yemen, where it wages a hybrid warfare in line with Iran's interests (Robinson & Merrow, 2024). In this regard, the UK criticizes Iran for destabilizing the region by supporting proxy powers and harming its allies in the region (United Kingdom Government, 2021, p. 85). In this respect, following the death of three US soldiers in an attack on a US base in Jordan in 2024, UK Foreign Secretary David Cameron stated that Iran would be "held accountable" for its "proxies". Also, ahead of the joint UK-US offensive in response to the attack on the US base in Jordan against the Iranian-backed Houthis in Yemen, Cameron put forward that "*We need to send the clearest possible signal to Iran that what it is doing through its proxies is unacceptable*" (Gillett, 2024).

Figure 4. 1: Countries Where Notable Iran-Backed Militas Are Active (As of February 2024)

Source: (Robinson & Merrow, 2024)

One of the most prominent conflicts against the UK's allies in the region actively supported by Iran through proxies, has been the Israeli-Hamas War that started after Hamas's breach of the Gazan border and attacks on Israeli cities on October 7, 2023 (Operation Al-Aqsa Flood). Although the allegations that Iran helped Hamas to plan its attack on Israel, have been denied by all parties to the war (Tani, 2023); Iran has expressed its unequivocal support for the Hamas attack. For instance, Iran's Supreme Leader Ali Hosseini Khamenei offered his congratulations to the Palestinian fighters and stated that Iran would support them until the liberation of Palestine and Jerusalem (Cafiero, 2023). On the other hand, after the Hamas's attack, the United Kingdom offered its "unequivocal support" for Israel (Helm, 2023). Indeed, it was not surprising that the UK stated its unconditional support of Israel because, in 2021, the two countries had signed a "Memorandum of Understanding" that extended bilateral relations to a strategic partnership by deepening and broadening cooperation. As a continuation of this agreement, two years later, the United Kingdom and Israel signed a long-term agreement called the "*2030 Roadmap for UK-Israel Bilateral Relations*", which strengthens the two countries' relationship in many areas, from security to technology, climate change to health (United Kingdom Foreign & Commonwealth Office, 2023; Wintour, 2023b).

In the vision section of the agreement, there was also an important reference to what this agreement aims to achieve: *"Israel and the United Kingdom will be at the forefront of efforts to tackle [...] efforts to delegitimize or demonize Israel."* While Iran was implicitly targeted in this statement, there was even a section in the defence and security section of the agreement that gave special attention to Iran:

> *"We work closely to counter the current threat from Iran […] We will work to ensure Iran never has nuclear weapon capabilities; we will seek to counter Iran's destabilising regional activity […] we will confront the threat posed to us both domestically"(United Kingdom Foreign & Commonwealth Office, 2023).*

Moreover, former UK Foreign Secretary James Cleverly, put forward that: "*The Roadmap is a testament to the strength of our close and historic relationship [and the two countries] stand [together] against Iran's malign influence in the region*" (Wintour, 2023b). As it is evident from these statements, there has been strong cooperation between the two countries against Iran, and this cooperation will continue

to be strong in the coming years. In this respect, after Hamas's attacks to Israel, the UK also dispatched military to the Eastern Mediterranean by the Prime Minister in support of Israel and regional stability (United Kingdom Prime Minister's Office Press Release, 2023). Despite this close relations with Israel, the UK also expressed its position by criticizing new settlements as "*illegal under international law*" and that settlement expansion should be halted (UK House of Commons Library Specialists, 2024, p.14). Moreover, UK Foreign Secretary David Cameron's suggestion of the two-state solution for peace in Palestine was criticized by Israel (Forrest & Mitchell, 2024).

Despite growing criticisms against Israel in the international community due to the humanitarian crisis in the Israel-Hamas War, the UK has continued to support Israel. In particular, in case of any threat to Israel's security, UK provides support to Israel. For instance, as a result of Iran's intense military campaign towards Israel by its proxies, Israel conducted an airstrike on the Iranian Embassy in the Syrian capital, Damascus. As a response to this attack, Iran had vowed to retaliate against Israel (Regan et al., 2024). In this respect, Iran launched more than 300 drones and missiles towards Israel. Almost all of the drones and missiles were intercepted, not only by Israel but with the assistance of the UK, France and the US (Berg et al., 2024). Although Iran informed about the drone and missile strikes before they were launched to minimize the impact and prevent a regional war" (Vakil & Saab, 2024); the UK assisted Israel in shooting down these drones and missiles. This help indeed demonstrates that the UK has been actively engaged in defence of Israel. Although there have been many Western states that support Israel, Iran imposed sanctions only on the United Kingdom and the United States for helping Israel (Farhat, 2024). Hence, imposing sanctions against the UK by Iran indeed shows how the perception of Iran towards the United Kingdom and Israel.

On the other hand, the United Kingdom, as mentioned above in the Russia-Ukraine and China-Hong Kong relations, has been considered as a country that intervenes in internal affairs or creates a threat to itself through alliances rather than posing a direct security threat. For this reason, the United Kingdom is often the prime suspect, especially when there is internal turmoil. This perception especially applies to Iran's perception towards the UK, which is called Old Fox. For instance, in 2009, the opposition's allegations that the elections were frauded led to the spark of biggest

upheaval since the Iranian Revolution of 1979 (BBC News, 2011a). The United Kingdom was blamed for organizing these attacks due to the role of BBC Persia (banned in Iran) which allegedly supported protesters. Accordingly, Iranian Supreme Leader Khamenei refers to the United Kingdom as "*the most evil of foreign powers*" for its involvement in the demonstrations to appeal to traditional resentment of British interference in Iranian affairs (McElroy, 2009; Tait, 2009). In response to Iranian criticisms of UK's involvement in its internal affairs, the United Kingdom has been condemning Iranian regime for the human rights violations.

One of the most recent controversies involving the UK's alleged role in the protests in Iran and the UK's criticism of Iran for human rights violations arose during the unprecedented protest in 2022 following the death of 22-year-old Mahsa Amini, as a result of beatings by morality police (BBC News, 2022b). To suppress the protesters, security forces used "disproportionate use of lethal force" according to the UN mission, and at least 500 people were killed during the protests (Pelham, 2024). While Iran was trying to suppress these protests, on the other hand, criticized London-based Persian-language media outlets for instigating riots and causing a hostile environment in Iran (Mehdi, 2022). In fact, Iran's disturbance about the news of these media outlets became more evident when British-Iranian journalists working for London-based Farsi-language media outlets received serious death threats (Weaver, 2022). After the threats reached serious levels, The Foreign Secretary summoned Iran's most senior diplomat in the UK and stated that the UK does not "*tolerate threats to life and intimidation of any kind towards journalists, or any individual, living in the UK*" (United Kingdom Foreign & Commonwealth Office, 2022). Moreover, as Patrick Wintour (2022) emphasized, Iran's obsession with the "*conspiracy*" against the London-based media outlets that they are working with foreign agents against Iran led to the arrest of a British-Iranian dual national who had been in contact with the BBC.

Also, Iran executed British-Iranian national Alireza Akbari -former defence deputy minister of Iran- due to charges of spying for Britain (for MI6) (Reuters, 2023a). In reaction, the UK Prime Minister stated that it was a "*cowardly act [that] carried out by a barbaric regime with no respect for the human rights of their own people*" (Wintour, 2023a). On the other hand, Iran summoned the British ambassador to Tehran. Another example took place after the UK ambassador to Tehran, Simon

Shercliff, called on the Iranian government to release the imprisoned journalist in his tweet on August 8, Journalists' Day (Iran International, 2023). To protest this tweet, Iran summoned Ambassador Shercliff and criticized his acts as a "*clear example of interference in internal affairs*" (The Islamic Republic of Iran Ministry of Foreign Affairs, 2023). Moreover, over the anniversary of the death of Mahsa Amini, the UK, the US, and the EU imposed multiple sanctions against Iran (The Guardian, 2023).

Lastly, the deterioration of UK-Iran bilateral relations has been exacerbated by Iran's supply of weapons to Russia following the outbreak of the Russia-Ukraine war in February 2022. Indeed, Iran and Russia were rivals for most of the last two centuries and after the Islamic Revolution in 1979, Iran's Supreme Leader, Ruhollah Khomeini, hated the Soviet Union almost as much as he hated the United States (Byman & Pollack, 2023). However, after the US intervention in the Middle East and the possibility of an attack on Iran, there has been a need for "*great power*" support for Iran. The required support has come from Russia through providing sophisticated weapons and diplomatic support by its permanent seat on the UN Security Council (Byman & Pollack, 2023). Moreover, due to both states' opposition to the US-led international order and the US's intervention in the Middle East, cooperation has been strategic and beneficial for both states (Tazmini, 2021). Russia, on the other hand, has been keen on maintaining the status quo in the Middle East and has been willing to cooperate with Iran on regional issues (Güneylioğlu, 2023, p. 59). In particular, after launching a military intervention in Syria in 2015, it was very important to have a country that can act in collaboration. While the United States' interest and role in the region have been on the decline, Russia's growing influence has also facilitated Iran's increased engagement, with both military and diplomatic support from Russia. Accordingly, as Murat Güneylioğlu underlines, Iran and Russia's alliances have been based on a "*sort of tactical and transitory alignment on specific mutual goals and interests*" rather than a "*full-fledged alliance*" (Güneylioğlu, 2023, p. 58).

After the outbreak of the Russia-Ukraine War, Iran started providing Russia with powerful weapons and even offered to send Shiite militias from the Middle East to fight in Ukraine (Byman & Pollack, 2023). By "*deepening the military cooperation*" (Hafezi et al., 2024), the two countries' relations became closer than ever before in history (Gramer & Mackinnon, 2023). The increasing cooperation raised concerns in

the United Kingdom due to the direct impact of Iranian military support in the Russia-Ukraine War. Consequently, this escalating cooperation also provoked a strong reaction from the United Kingdom and further strained UK-Iran bilateral relations. Accordingly, former UK Foreign Secretary James Cleverly stated that "*Iran had become one of Russia's main military supporters and that the relationship between them was threatening global security*" (Maishman & Hancock, 2022). The main reason why this alliance is so problematic for the UK and the US in particular is that the conflicts in the Middle East and the war in Ukraine are increasingly intertwined that threaten global security (Smagin, 2024). Therefore, the involvement of the two countries in both regions through their alliances threatens the UK's allies in these regions and harms the UK's interests.

In conclusion, the United Kingdom and Iran have had a long, complex, and difficult relationship. Over the past decade, the bilateral relations between the United Kingdom and Iran have been shaped by several important factors. From Iran’s perspective, the United Kingdom is a threat because of its interference in Iranian domestic politics, its commitment to the US-led system of international order, its imposing sanctions against Iran, its consistent support for Israel and its active presence in the region. On the other hand, the main factors that increase tensions for the United Kingdom are Iran's nuclear enrichment policy, its growing activities and expanding proxy networks that destabilize the Middle East, and the UK's concerns about Iran's human rights abuses and threats against British journalists. Indeed, when these factors are taken together, Britain's relation with Israel is at the heart of the tensions between the two countries. For example, the most prominent issues in the eyes of the UK, are Iran's nuclear enrichment policy and proxy networks, which cannot be seen as independent of Israel. Therefore, it is not possible to examine the UK's relations with Iran independently from its relations with Israel. In this respect, quantitative analyses will be conducted in the next section to test the impact of the UK, Iran, and Israel, along with other trilateral relations mentioned above, on cyber disruption operations targeting the UK.

4.4. Quantitative Analysis of Cyber Disruption Operations Targeting the United Kingdom and Its Trilateral Relations

In the United Kingdom's Integrated Review report (2021), which outlines the British government's long-term foreign policy, it was revealed that the UK was the target of state threats. These threats were carried out in the form of a hybrid combination of traditional tools and coercion tools, such as cyber threats, disinformation, propaganda, and sabotage (United Kingdom Government, 2021, p. 70). With the increasing hybrid threats, the sharp boundaries between war and peace have been becoming ever more blurred. The "grey zone", which represents this uncertainty, is constantly expanding with the efforts of states to gain superiority over their rivals by using a combination of traditional and non-traditional methods. The increase in the number and effectiveness of non-traditional methods, especially with the technological developments in recent years, offers states wide room for manoeuvre in their foreign policies.

Cyber-attacks are one of the main tools that allow states to operate in grey zones, primarily due to their advantages of creating uncertainty and plausible deniability. According to the UK's National Cyber Security Centre (2023, p. 11), there have been emerging cyber threats from state-sponsored actors, and the greatest threats to the UK come from China, Russia, and Iran. The United Kingdom, which has identified itself as a target of these state-sponsored actors, has been the primary target of cyber disruption operations in Europe. In this respect, the following Figure 4.2 created by the dataset extracted from NETSCOUT, demonstrates the frequency and volume of DDoS attacks targeted at the United Kingdom between 2014 - 2023.

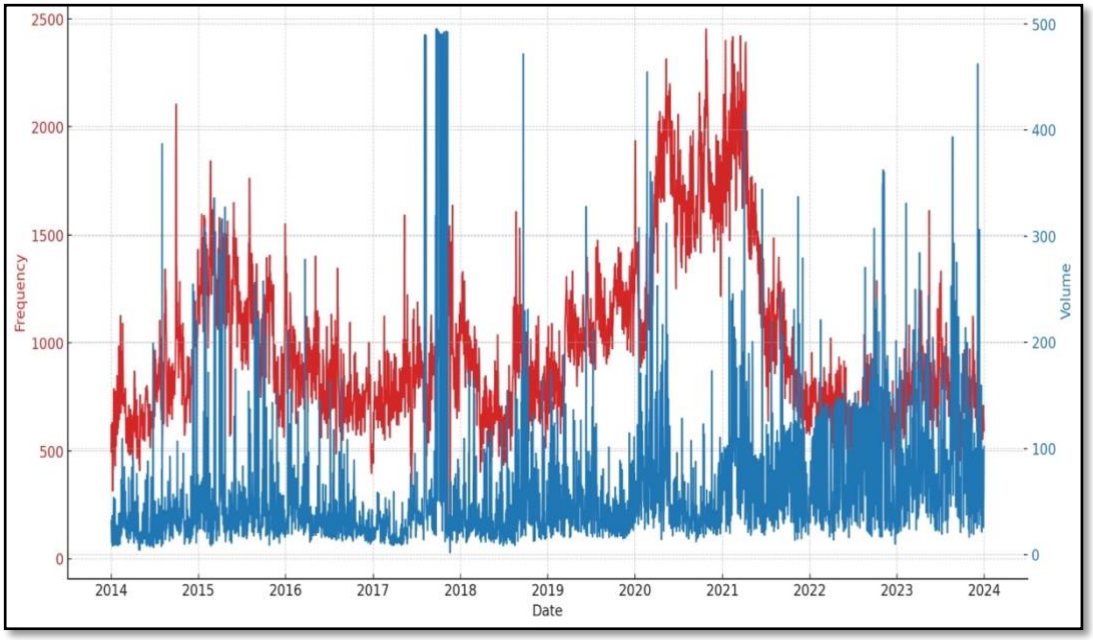

Figure 4. 2: Annual Trends in Distributed Denial-of-Service (DDoS) Attacks Targeting the United Kingdom from 2014 to 2023

The Figure 4.2 depicts the frequency and volume of cyber disruption operations targeting the UK between 2014 and 2023, with red bars representing the frequency and blue bars the volume. Frequency indicates the frequency of DDoS attacks that occurred on a specific date, while volume indicates the intensity of the DDoS attacks. Although there is a correlation between the two indicators, it is important to note that there are no direct relations between frequency and volume. There may be a high frequency of DDoS attacks, but if the intensity of these attacks is very low, they may remain ineffective. On the other hand, if the volume of these attacks is high, they can have significant consequences. For example, an attack with 1000 soldiers can have a significant impact on the target, but two missiles might cause more devastating results. In short, two variables are important indicators of DDoS attacks and should be evaluated together for more comprehensive analysis.

In addition, the majority of these cyber-attacks are of a relatively low level, as they are conducted by various non-state actors for a variety of reasons. For this reason, while the frequency of cyber-attacks is high, they might be low-level and ineffective. On the contrary, when the state or state-sponsor actor conducts a series of cyber operations, both the volume and frequency of the DDoS attacks increase significantly. It is because, as Akgül (2021, pp. 429-430) emphasized for the grey zone warfare,

using a lot of tools combined, coordinated and simultaneously in the long term necessitates great capacity, and the state has such capacity - even only big and revisionist states. Thus, the non-state actors cannot have such the capacity to conduct grey zone strategies. In this respect, conducting severe DDoS attacks with high volume and high frequency over a long period of time requires state support. Nevertheless, each country encounters hundreds/thousands of cyber-attacks every day, depending on their population, the prevalence of information and communication technologies and internet usage. So, the figures in question may be perceived as exceedingly high in one country yet may be regarded as relatively ordinary or low for another country. Therefore, cyber-attacks on each country should be investigated individually, and a threat level specific to that country should be determined. In this regard, to detect significant cyber-attacks in the systems and networks, researchers try to find the anomalies in the flow of the data (Al-amri et al., 2021; Dutta et al., 2020; Karimipour et al., 2019). To find the anomalies/outliers, they adjust a level (threshold) that identifies what can be accepted as normal and different from the majority of the data (Bajaj, 2020). In other words, a threshold is used to find out the outliers/anomalies in the data.

With this approach, the frequency of DDoS attacks in the UK from 2014 to 2023 was grouped into two clusters using K-Means Clustering to represent normal and anomaly data in the dataset. On the other hand, for the volume of DDoS attacks, dividing dataset into two clusters did not entirely capture the data's complexity. This was because the threshold was set at approximately “200” by KNN, and the anomaly cluster contains limited number of cyber-attacks. This might have caused the exclusion of many significant cyber-attacks because 200 was a high number when the overall data was analysed in the dataset. However, by dividing the dataset into three clusters, as shown in Figure 4.3 below, a more accurate representation of the data's distribution was obtained. Consequently, the threshold was determined based on cluster 0. Thus, the sum of cluster 1 and cluster 2 represents the values exceeding the threshold in terms of cyber-attack volume.

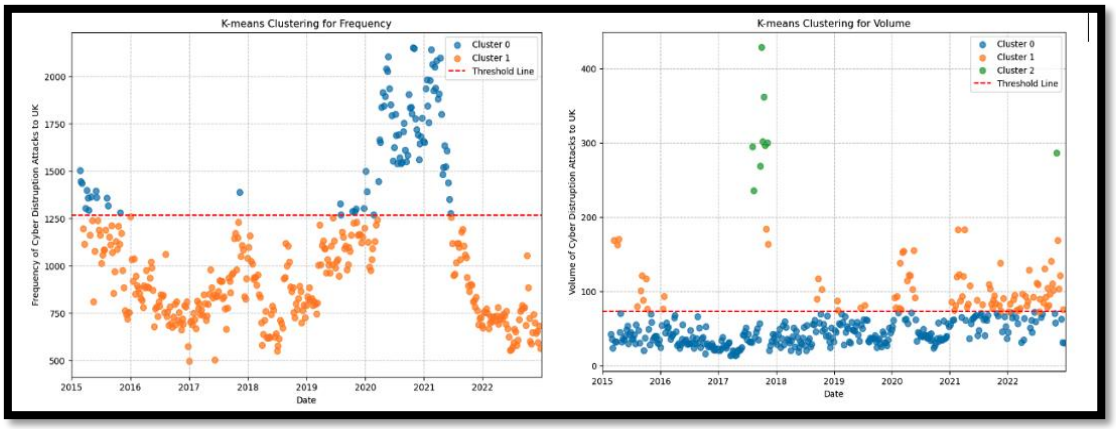

Figure 4. 3: Threshold Levels of Frequency and Volume of DDoS Attacks Targeting United Kingdom

Lastly, two additional conditions were set for the threshold. Although high frequency and high volume alone might not be enough to tell there is a significant cyber-attack; still high frequency and volume might indicate the possibility of serious cyber-attacks. Especially, for the early warning system, missing these kinds of cyber-attacks might cause problems. Therefore, based on the cyber-attack data directed at the UK, two conditions, "frequency of cyber-attacks >1500" and "volume of the cyber-attacks > 130", were also included. The values of 130 and 1500 have been designated as another threshold since they are observed as an upper threshold in line with the distribution of cyber-attacks in the KNN cluster analysis, as shown in Figure 4.3 above. Thereafter, based on the KNN cluster model and the two additional conditions, a new binary category that indicates whether the volume and frequency of DDoS attacks simultaneously exceed the threshold or not was obtained, as shown in Table 4.2 below and Figure 4.4 below.

Table 4. 2: New Dataset Format After Setting Threshold

Date (Weekly Date)	DDoS Attacks to United Kingdom		Serious Cyber Disruption Operations
	Frequency	Volume	
2015-02-22	1503,71429	42,37181	True
2015-03-01	1446	35,16723	False
2015-03-08	1436,57143	23,74328	False
2015-03-15	1195,57143	168,7838	True

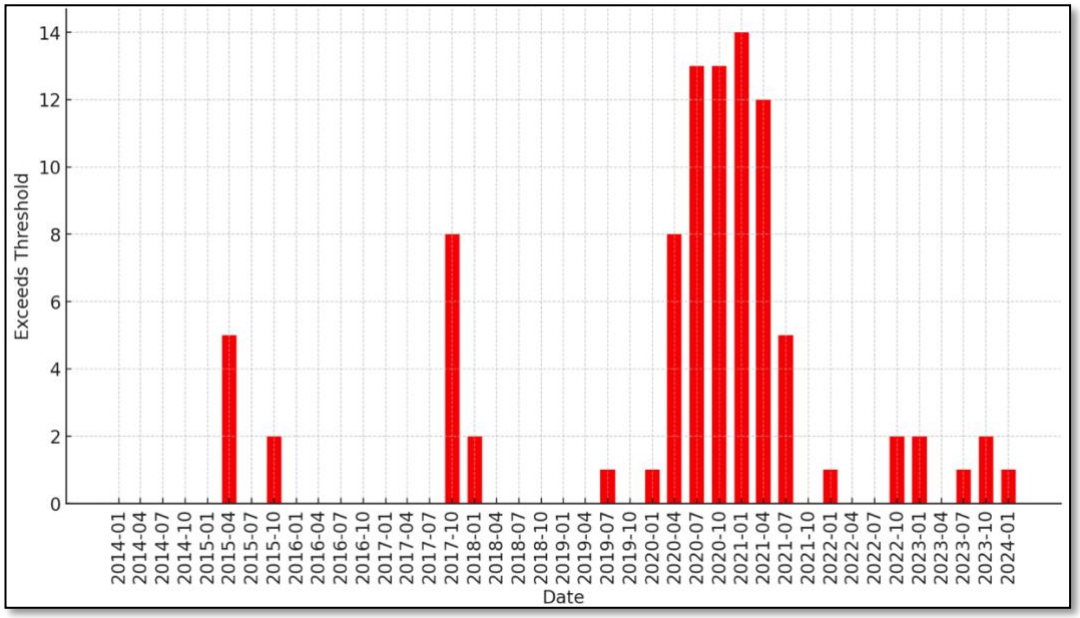

Figure 4. 4: Frequency of Significant DDoS Attacks Against the UK in Quarterly Intervals (2014-2023)

As previously discussed in the methodology section, the dataset includes data regarding whether cyber-attacks exceeded the threshold or not in that particular week, as demonstrated in Table 4.2 above. In this respect, Figure 4.4 above illustrates the number of weeks in a quarter period of each year between 2014 and 2023 in which the UK became the target of cyber-attacks that exceeded the threshold. In other words, Figure 4.4 illustrates the possible state-sponsored serious cyber-attacks directed at the United Kingdom between 2014-2023.

According to Figure 4.4, it is observed that serious cyber disruption operations were carried out against the UK, especially in 2015, 2017, 2020 and 2021. Specifically, between 2020 and mid-2021, the UK was subjected to constant serious cyber disruption operations in this 10-year period. Indeed, this period overlaps with the shift of the United Kingdom's foreign policy in line with the Global Britain Doctrine which advocates for the UK to engage in active foreign policy at both the systemic and regional levels. In this regard, the UK's active role at both systemic and regional levels strained its relations with China, Russia, and Iran. In other words, the transformation of the UK's foreign policy overlaps with the increase in the number of cyber-disruption operations targeting the UK. In this context, it is possible to make an interpretation of the UK's foreign policy just by looking at this graph. However, to test this study's

hypotheses and evaluate three trilateral relations – "*United Kingdom-China-Hong*", "*United Kingdom-Russia-Ukraine*", and "*United Kingdom-Iran-Israel*" and disruptive cyber operations targeting the United Kingdom between 2014-2023 – three separate Binary Logistic Regression analysis are conducted. The results of these analyses yielded the following findings.

Table 4. 3: Three Binary Logistic Regression Analyses Results

	Coefficient	**P Value**	**Pseudo- R^2**
Constant	-2.63	0.001	0.08
United Kingdom & Ukraine	0.80	0.002	
United Kingdom & Russia	-0.48	0.017	
Constant	0.33	0.55	0.17
United Kingdom & Hong Kong	0.49	0.001	
United Kingdom & China	-1.55	0.001	
Constant	-2.11	0,001	0.05
United Kingdom & Israel	0.97	0.001	
United Kingdom & Iran	-0.03	0.834	

Prior to any interpretation of the findings, it is essential to define the basic terms of the logistic regression analysis. In the regression analysis, the constant term (or intercept) represents the value for the dependent variable when all independent variables are "0" (Siegel & Wagner, 2022, p. 372). In this respect, the value of the constant indicates that there may be other variables that also explain the effect on the dependent variable. On the other hand, the regression coefficient basically represents the effect of each independent (predictor) variable(s) on the dependent variable while holding the other independent variables fixed (Siegel & Wagner, 2022, p. 372). In other words, the regression coefficient indicates the impacts of the independent variable on the dependent variable. Therefore, the higher it is, the more influence it has on the dependent variable. Thirdly, the P-value represents the probability, for a given statistical model, that the null hypothesis is true (Nahm, 2017, 241). In other words, in statistical analysis, the p-value indicates the statistical significance. In general, a p-value of 0.05 (golden standard) is considered a threshold value, with $p > 0.05$ indicating "no significance". Therefore, the smaller the p-value, the greater the statistical significance (Nahm, 2017, 241).

Last but not least, pseudo-R-squared (R^2) represents the strength of prediction of the logistic regression model (Hu et al., 2006, p.847). However, it is important to note that there are differences between linear regression and logistic regression in terms of the interpretation of the R-squared value. In linear regression models, (R^2) and the adjusted (R^2), which range from 0 to 1, measure the goodness of the model's fit. When (R^2) is close to 1, it indicates how well independent variables explain the dependent variable. On the other hand, in logistic regression, pseudo-(R^2) are a "versatile goodness-of-fit indicator for logistic regression models. While (R^2) of linear regression represents the proportion of explained variance, pseudo-(R^2) of logistic regression measure the "improvement in model likelihood over a null model". In this regard, it is hard to tell that there is a consensus on what the best benchmark values for pseudo-(R^2) should be. Furthermore, factors such as sample size, number of independent variables, and categories of the dependent variable influence all pseudo-(R^2) values in logit regression *(Hemmert et al., 2018, pp. 507-509)*. This means that including many predictor variables and reducing the number of categories of dependent variables is likely to result in higher pseudo-(R^2) values, and vice versa.

This study conducted three binary logistic regression analyses that individually tested all trilateral relations' impact on the cyber-disruption operations targeting the UK, as shown in Table 4.3. Based on pseudo-(R^2) values, these analyses initially indicate that the UK's trilateral relations with China and Hong Kong explained 17% of the cyber-attacks targeting the UK, while the relations with Russia and Ukraine explained 8%, and the relations with Iran and Israel explained 5%. These results show that the UK's trilateral relations with China and Hong Kong have better explanatory power regarding cyber-attacks on the UK. However, the primary focus of these analyses is to test whether there is individual impacts of each trilateral relation of the UK on significant cyber-attacks, rather than evaluating how well the model explains the dependent variable. Therefore, pseudo-(R^2) has limited explanatory powers in this study but the parameters of "p-values" and "coefficients "of these logistic regression analyses. In this regard, in order to make the binary logistic regression results more explicit, Figure 4.5 below was designed.

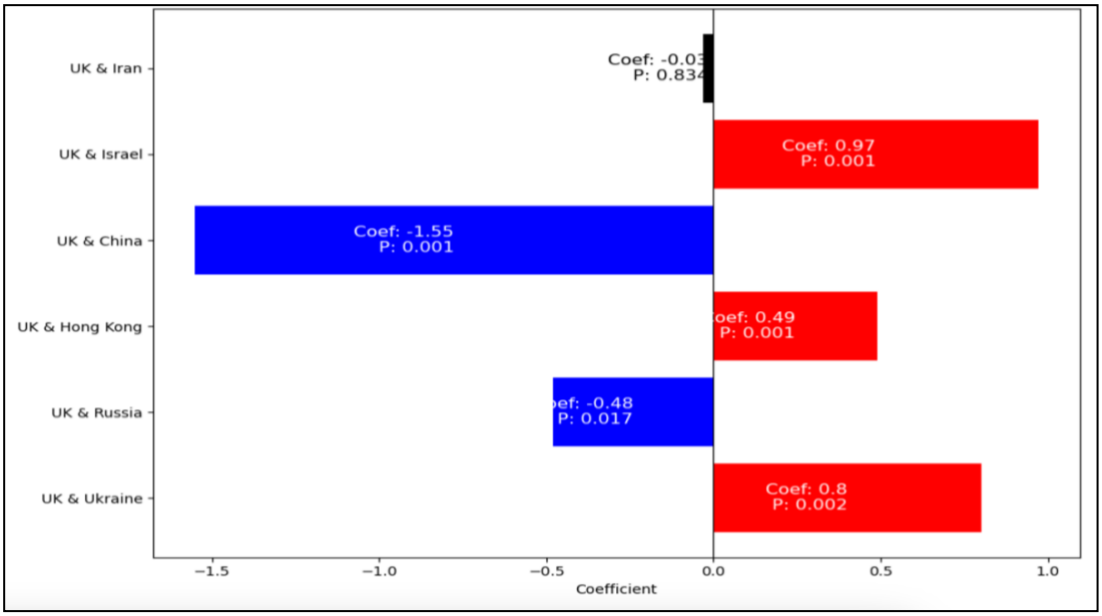

Figure 4. 5: Three Binary Logistic Regression Analyses Results

According to this figure, the blue bars show the countries where an increase in the conflict score (or in other words, a decrease in the cooperation score) in bilateral relations with the United Kingdom leads to an increase in cyber-attacks directed at the United Kingdom. The red bars on the right side show the bilateral relationships in which an increase in the cooperation score to the UK is the driver of an increase in cyber-attacks against the UK. The black bar shows that there is no statistically significant relationship between the increase and decrease in cyber-attacks against the UK.

In this regard, these results demonstrate that there is an increased likelihood of serious cyber-disruption operations towards the UK when:

- The UK's cooperation level increased with Israel (0.97), Ukraine (0.80) and Hong Kong (0.49) (as H2a suggests)
- UK's conflict level increased (cooperation level decreased) with China (-1.55) and Russia (-0.48) (as H1a suggests, but there is no statistically significant relationship with Iran in either a positive or negative direction).

According to this result, when the UK's dyadic relations deteriorated with China and Russia, the United Kingdom received major cyber-attacks. On the other hand, the UK's close relations with Ukraine, Hong Kong and Israel also increase the possibility of being the target of the major cyber-attacks for the UK. In addition, with a "-1.55"

co-efficient, the UK-China bilateral relations have the most impact on the increase in cyber-attacks directed at the UK, followed by UK-Israel (0.97) and UK-Ukraine (0.80) relations. In this regard, for the cyber-security of the United Kingdom, the UK's bilateral relations with China, Israel, and Ukraine should be given great attention. However, it should be noted that these findings do not directly imply that China, Russia, and Iran are the perpetrators of cyber operations against the UK. This study does not aim to test it. This analysis only tests whether these countries' dyadic relations have an impact on the increase/decrease of cyber-operations toward the UK.

Indeed, due to attribution problems, which is one of the most important problems of cyber security due to the design of the internet, which prioritises secrecy over security, states have difficulty identifying the perpetrators of the attacks. Even if they detect the sources, it is rather challenging to penalize or sanction if the attackers live in another country. In this respect, states that want to remain in the grey zone while exploring the other actors without overpassing the thresholds utilise the cyber-tools. Especially in case of a crisis, a third actor that conceives the relations between the two countries has started to deteriorate, may try to exploit the crisis and confuse the target by launching an attack at this very moment, which is called a false flag operation. Since the two rivals most probably blame each other for the cyber-attacks, other third parties are involved in the conflict to exploit the crisis. In this respect, in the case of a crisis, not just the rivals conduct cyber-attacks but also the third actors who perceive the crisis as an opportunity. Consequently, when bilateral relations deteriorate, it would be incorrect to suggest that only the actors directly involved in the crisis utilize cyber tools. Therefore, when the United Kingdom's bilateral relations with China and Russia deteriorate, it is hard to directly blame China and Russia as the perpetrators of the cyber-attacks.

However, since this study analyses the impact of a period of 10 years of bilateral relations on whether cyber-disruption operations exceed the threshold, the statistically significant results indeed make these countries the usual suspects of cyber-attacks on the UK. The fact that there is a statistically significant relationship in a 10-year period indicates that this is not a coincidence; it is being used as a complementary instrument in foreign policy. In addition, the findings of the increasing possibility of significant cyber-disruption when the cooperation level increases with Hong Kong, Ukraine and

Israel also provide a serious clue that the three usual suspects may play a significant role in conducting cyber-attacks.

Also, it is necessary to open a parenthesis about Iran. According to the results, there is no statistical relationship between the UK – Iran dyadic relations and cyber disruption operations targeting the UK. There could be various reasons for this finding: First of all, compared to China and Russia, Iran may not be able to use cyber tools simultaneously along with other tools because it does not have enough technological capacity as Russia and China. For example, according to the National Cyber Power Index, Iran ranked 10th in the overall 2022 ranking, while China and Russia ranked second and third respectively (Voo et al., 2022, p. 9). As Table 4.4. below indicates, while Iran was not among the top ten cyber powers in the 2020 ranking – it was ranked 23rd (Voo et al., 2020, p. 11) – it ranked 10th in the 2022 ranking. As James Andrew Lewis (2019) points out, Iran is not yet in the top ranks of cyber powers, although it is rapidly improving its cyber capabilities and is ahead of most states in its strategy and organization for cyber warfare. Hence, Iran's inability to simultaneously use cyber tools at the same level as China and Russia when their relations deteriorate with the UK may underscore the need for technological capability to use cyber tools as a complement to other foreign policy tools.

Table 4. 4: Comparison of the Top 10 Cyber Powers in 2020 and 2022 Based on the National Cyber Power Index

Rank	2020	2022
1	US	US
2	China	China
3	UK	Russia
4	Russia	UK
5	Netherlands	Australia
6	France	Netherlands
7	Germany	ROK
8	Canada	Vietnam
9	Japan	France
10	Australia	Iran

Source: (Voo et al., 2022, p. 10)

However, DDoS attacks are one of the least complex types of cyber-attacks due to the requirement of less technical knowledge and resources compared to other cyber-attacks (Brantly, 2018, p. 42). Therefore, DDoS attacks can be conducted regardless of the capacity of the state actors. This situation brings us to the second reason, which is relations between the United Kingdom and Iran are influenced by the United Kingdom's relations with countries in the region rather than their bilateral relations. As discussed in the previous chapter, the UK is perceived by Iran as a threat to the regime's security, particularly in the case of the protests in Iran, by exacerbating domestic unrest through media networks and spying activities. Indeed, this behaviour is also parallel with the balance of threat. According to Stephen Walt (1985), states seek to balance perceived threats, with geographic proximity as a key factor in shaping those perceptions. Similarly, Barry Buzan and Ole Weaver (2003, p.11) argue that political and military threats travel more easily over short distances, thereby linking insecurity to proximity and the tendency for states to fear their neighbours more than distant powers. Therefore, the role that the UK plays in the region may be more important to Iran than the UK itself. In this regard, the UK's relations with Israel - the main rival and the archenemy of Iran in the region - could be more urging to the use of cyber disruption operations against the UK.

This situation brings to the fore the importance of another aspect. When dyadic relations deteriorate, states indeed have the bulk of tools (e.g., economic, diplomatic, and military tools, as well as cyber tools). However, when a rival state improves its relations with a strategically significant country, states have relatively fewer foreign policy tools. At least, states refrain from applying overt tactics and tools against rival states. At that point, cyber-attacks which are one of the tools that enable states to operate in grey areas primarily due to the advantages of creating ambiguity and offering plausible deniability, have become useful tools.

For example, when the UK and Israel signed an agreement which could threaten Iran's interests, how could Iran react to this development in the best way? If Iran wants the UK to withdraw from this agreement, how can it convince the UK, or if it cannot convince the UK, how can it show its displeasure in the strongest possible way? As a response, Iran seems to have many tools, such as imposing economic sanctions, summoning the ambassador, or using the military option as a last resort against

Britain's allies in the region; however, it has indeed a very limited number of tools. One of the most important reasons for this is the power gap between Iran and the UK. Since the two states are not equal in terms of both hard and soft power indexes, what Iran does bilaterally against the UK will actually cause more damage to Iran than the UK. Then, the question is how Iran can convey its signal directly to the UK without escalating the crisis in such a situation.

This situation also applies to Russia and China. Even if China and Russia perceive the UK as a second-tier power in the international system, it would be misleading to assess the UK by its national power alone. Due to both its special relations with the United States, NATO membership and its being a major actor in the US-led international system, any attack or sanction against the UK would also target the US and other Western states. Hence, as discussed in the theory of hybrid warfare, the actor at a conventional disadvantage applies hybrid tools to eliminate that advantage without triggering a significant backlash. In this context, the usual suspects - Russia, China and Iran- could employ cyber disruption operations as instruments for tacit bargaining and conflict resolution against the UK when the UK increases its cooperation with Ukraine, Hong Kong and Israel. In other words, for states who are reluctant to use (or unable to use) other tools and want to do “something without triggering significant response” rather than “doing nothing”, cyber-attacks offer strategic utility for the states.

When conducting a cyber disruption operation, the main goal is to influence society, not to cause severe harm to an adversary. If the aim is to cause significant damage, states have a variety of traditional methods at their disposal which are more likely to be effective than cyberattacks. Nevertheless, in case of a very serious attack, whether it's through kinetic or non-kinetic tools, states respond strongly. In simple terms, if the impact of the operation goes beyond a certain point, regardless of the method used, states will react. Thus, cyber disruption operations are used to conduct "influence operations" with the aim of influencing society and creating disruption for political purposes.

As an influence instrument, DDoS attacks are particularly deployed to degrade the morale of countries embroiled in socio-political upheaval (Hummel & Dobbins,

2022, p. 11). Disruption operations generally target the business sector and public institutions that are widely used by the population, rather than military or governmental targets. While a state may be able to hide an attack on military or government sources, it becomes much harder to conceal a DDoS attack on public targets. It is because people can experience the impacts of DDoS attacks (Maness & Valeriano, 2016, p. 317). In this regard, the main purpose of this is to create a psychological impact by affecting as many people as possible with cyber-attacks. In other words, by conducting constant and frequent cyber disruption operations to targets that more people can experience the impact of the attacks, threat actors aim to create a perception of insecurity and incompetence towards the government and related institutions. In this way, threat actors aim to exert pressure on governments. Since these attacks also cause a limited impact on the target but a greater impact on society, giving proper responses is also challenging for states. Hence, states that want to express their disturbance about an incident without provoking a significant response may resort to cyber disruption operations to directly influence society and indirectly impact the government. In this respect, the psychological effect of DDoS attacks on societies, rather than their physical effects, led states to react to DDoS attacks.

For instance, according to Boaz Dolev and David Siman-Tov (2022), Iran has been conducting cyber-operations against Israel to produce a psychological effect. Iranian-affiliated cyber actors carry out numerous low-level cyber-attacks and publicise them via social media accounts. Through these attacks, Iran intends to induce fear in the Israeli public that the government cannot provide adequate security and that Iran may launch more serious cyber-attacks in the future. Thus, Iran's strategic objective is to pressure the public and thereby influence Israeli decision-makers and the ongoing conflict between Israel and Iran (Dolev & Siman-Tov, 2022)

In addition to the statistical test of ten-year bilateral relations on cyber-attacks, this study further strengthens the H2 hypothesis by examining the cases in which the UK have been the target of significant cyber-disruption operations when its cooperation level increases with Ukraine-Hong-Kong and Israel. In this direction, when trilateral relations between the UK, Russia and Ukraine were examined initially, the first example is the "*Multinational Maritime Training Initiative for the Ukrainian Navy*", which was signed between the UK and Ukraine on 18 August 2020. With this agreement, the United Kingdom aided Ukraine to increase the ability of combat of the

Ukrainian Navy against threats from the East in the Black Sea. Within the scope of this agreement, the UK agreed to send Royal Navy ships for the train (United Kingdom Ministry of Defence, 2020). Considering the naval power of the United Kingdom, collaboration with Ukraine and enhancing Ukraine's naval power in the Black Sea was indeed a direct threat to Russia, even if Russia considers the UK as a secondary power. During the week of August 18, 2020 (16-23 August 2020), the dataset showed that the United Kingdom was the target of cyber disruption operations that exceeded the threshold. In this regard, it can be assumed that this agreement might increase the usage of cyber-disruption operations against the UK.

In addition, two months after the launch of the "UK-led Multinational Maritime Training Initiative for The Ukrainian Navy", Ukrainian President Zelenskyy visited the UK. During his visit, on 8 October 2020, the two countries signed a historic *'Strategic Partnership Agreement'* that covered various areas, such as trade, defence, political cooperation, climate change and human rights. Most importantly, the agreement formalized the UK's commitment to Ukraine's sovereignty and territorial integrity (United Kingdom Prime Minister's Office Press Release, 2020). As Maryna Vorotnyu (2021) - Associate Fellow at Royal United Services Institute- highlighted, with this agreement, UK had strengthened its support to Ukraine against Russia's hybrid threats. In this regard, the UK sought to strengthen the resilience of the Ukrainian economic, trade, security and political ecosystem through increasing cooperation with Ukraine. Therefore, it was not surprising to expect a strong reaction from Russia against this agreement. In this respect, when the period – 4 October & 11 October 2020 – was examined, it was observed that UK once again became the subject of significant cyber-attack.

On the other hand, for the United Kingdom-China and Hong Kong trilateral relations, two prominent incidents stand out. On 21 May 2020, China had introduced new "National Security Law" in Hong Kong to prevent a repeat of the protests in Hong Kong similar to the 2019 pro-democracy protests. The proposed legislation was criticized for bringing "*the end of Hong Kong*" through severely undermining the One Country-Two System framework that guarantee autonomy of Hong Kong (Kuo, 2020; Kuo & Davidson, 2020). Despite criticisms, Chinese parliament passed a this controversial national security law and it had gone into effect on 30 June 2020 (Kuo, 2020). In

response, UK criticize new law as "*clear and serious breach*" of the "Joint Decleration and International Law" and undermines the autonomy of the Hong Kong. Moreover, on 1 July 2020, UK announced a new type of visa that offers a route to British citizenship for people in Hong Kong (United Kingdom Parliament, 2020), which significantly escalated the tension between UK and China. Following the UK's decision, China's Foreign Minister called on the UK to "correct its mistakes immediately" and warned the UK against interfering in China's "domestic affairs" (BBC News, 2020c). In this regard, when the cyber-attacks on the United Kingdom between 28 June-5 July 2020 were reviewed, it was observed that the cyber-attacks that took place between these dates exceeded the threshold of significant cyber-attacks.

Six months after the UK announced this new visa type, on 31 January 2021, it was officially launched and began to take applications from Hong Kong residents who have British Nationals (Overseas) status and their dependent family members. After this official launch, China announced that the passports of BN(O) would no longer be recognized by China and criticized the UK for violating international law and interfering with its internal affairs (Hale, 2021). In this direction, when the period between 31 January- 7 February 2021 was examined, once again, it was observed that the UK became the target of a significant level of cyber disruption operations after it increased its level of cooperation with Hong Kong.

In addition to the UK's two trilateral relations, lastly, when the relations between the UK, Iran and Israel are reviewed, although there is no statistically significant impact of 10 years of UK-Iran bilateral relations on cyber-attacks targeting the UK, for a short period of time, there are serious indications that cyber-attacks might have increased over the incidents with Iran. For instance, on January 3, 2020, General Qassem Suleimani, one of Iran's most important figures, was killed by a US drone attack in Baghdad. Even though the United States was responsible for the attacks, as a forefront ally of the US, the United Kingdom also faced significant degree cyber-attacks during the crisis period. It is also possible to argue that during the unprecedented protest in 2022 following the death of 22-year-old Mahsa Amini, Iran was significantly disturbed by London-based Farsi-language media outlets, and there were even serious death threats to journalists in these media outlets. After the threats reached serious levels, on 11 November 2022, The Foreign Secretary summoned Iran's

most senior diplomat in the UK and stated that the UK does not "*tolerate threats to life and intimidation of any kind towards journalists, or any individual, living in the UK*" (United Kingdom Foreign & Commonwealth Office, 2022). When the cyber disruption operations targeting the UK in this period are analyzed, it is observed that significant levels of cyber-attacks were carried out against the United Kingdom between 6-13 November 2022. Despite these two cases, the fact that there are no statistical causal relations between the level of bilateral relations and the cyber-attacks. These findings show that cyber disruption operations are not prior foreign policy tools by Iran against the UK for its bilateral relations. At least, it can be argued that cyber tools are not a long-term foreign policy tool directly used by Iran in its bilateral relations with the UK, but rather a short-term tool, or one that varies depending on the importance and type of incident.

On the other hand, as discussed above, cyber tools have become a long-term strategic tool for Iran when UK increased its level of cooperation with Israel. In this respect, the following two cases stand out when examining UK-Israel relations. Firstly, to celebrate the 100th anniversary of the Balfour Declaration, Israeli Prime Minister Benjamin Netanyahu visited the UK. During his visit, UK Former Prime Minister Theresa May stated the UK's support for Israel. Accordingly, May stated that "*we are proud of our pioneering role in the creation of the State of Israel", "we [...] declare our support for Israel [and we] also remain absolutely committed to Israel's security* (United Kingdom Prime Minister's Office, 2017c) Moreover, during Netanyahu's visit, the two states also agreed to deepen their cooperation in various areas. In this area of cooperation, "defence and security cooperation, particularly in the fields of counter-terrorism and cyber security," came to the forefront. Moreover, the two leaders also underlined the necessity of the international community to work together to counter Iran's destabilizing activity in the region (United Kingdom Prime Minister's Office, 2017b). Accordingly, when the level of cyber-attacks targeting the UK during the period of Netanyahu's visit (between 2-5 November 2017), it was observed that these attacks exceeded the level of threshold.

In addition, during the two weeks of the Israeli-Hamas conflict in May 2021, the United Kingdom announced its support for Israel. In the former UK's Middle East and North Africa Minister James Cleverly's speech in the parliament on 19 May 2021, Cleverly stated:

> *"We strongly condemn these acts of terrorism by Hamas […] who must permanently end their incitement and rocket fire against Israel. There is no justification for the targeting of civilians. Israel has a legitimate right to self-defence and to defend its citizens from attack"* (United Kingdom Parliament, 2021).

In the parliamentary debates, the role of Iran in these attacks was also frequently emphasized by other members of parliament (MPs). In discussions, MPs generally pointed out the role of Iran in the Israel-Hamas conflict by backing Hamas and its proxy networks in the Middle East that threaten the stability and peace of the region. Regarding the MPs' questions of what should be done to Iran in response to Iran's actions, Cleverly stated that "*Israel is responding to rockets fired at it from an organisation closely associated with Iran [...] Our desire to prevent Iran acquiring a nuclear weapon we cannot be blind to its broader regional destabilising activity*" (United Kingdom Parliament, 2021). With these statements, the UK explicitly states that it considers Hamas as part of Iran's proxy network and, therefore, Hamas's attacks on Israel were indeed supported by Iran. In this regard, when the cyber-attacks targeting the UK between 6-21 May 2021 were examined, it was seen that the UK was once again subjected to significant cyber-disruption operations.

It is possible to increase the number of these examples. With these examples and statistical analysis, this study provides important insight into the role of Russia, China, and Iran in cyber-attacks on the UK. Also, the intense period of cyber-attacks directed at the United Kingdom in 2020 and 2021, as seen in Figure 4.4 above, also matches with the report of the UK National Cyber Security Centre (NCSC). Accordingly, NCSC (2024) revealed that during 2021 and 2022, a China state-affiliated actor, APT31, systematically targeted institutions and parliamentarians of the UK through malicious cyber companies. Although this study does not directly identify countries as in the NCSC report, it still provides important analyses of the long-term role of the usual suspects. In this regard, this study also provides an insight into which bilateral relations have a greater impact on the increase in cyber-attacks. By identifying which bilateral relations exert greater influence, this analysis enables states to take pre-emptive measures based on the states that are involved in the relations. With these findings, this study offers a practical method for developing an early warning system for politically motivated cyber disruption operations, which is one of the main goals of this study.

In addition, the increase in cyber-attacks when the UK has increased cooperation with Israel, Ukraine, and Hong Kong also suggests that cyber threat actors might also target the allies of the targeted state as well. As a member of various international organizations and alliances, the security of the UK is not independent, especially from regional actors. Even if cyberspace is a dimension with no geographical limitations or physical limits, regional aspects still play a major role. In this regard, this study also tests whether there is a correlation between the frequency of cyber-attacks targeting the UK and the countries that are in Western and Northern Europe. For this aim, Pearson Correlation analysis is conducted.

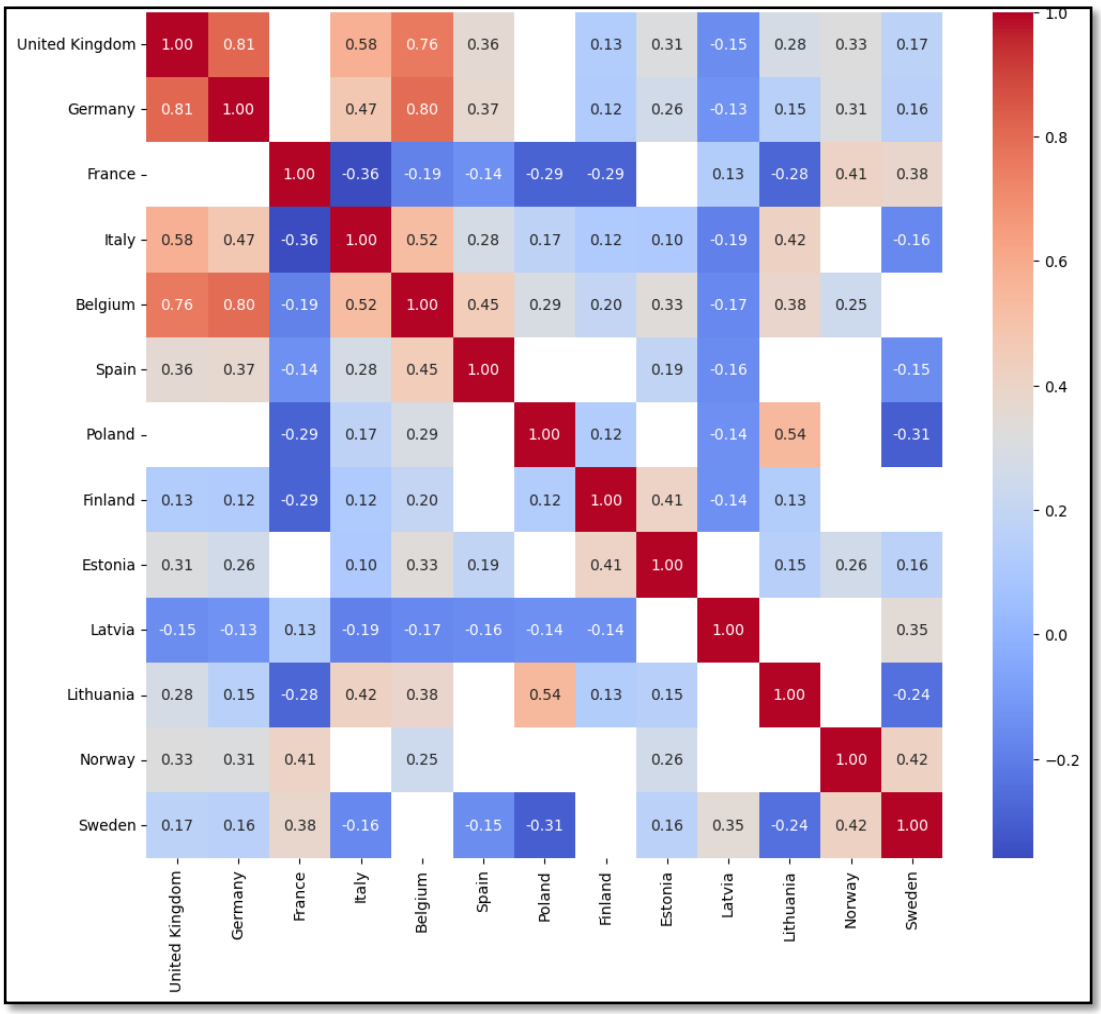

Figure 4. 6: Correlation Matrix of DDoS Attacks (Weekly Average) Targeting European (Western and Northern) Countries (2015-2022)

Figure 4.6 above illustrates the significant correlation between the frequency of DDoS attacks targeting labelled countries between 2015 and 2022. Positive correlations are represented in red, while negative ones are shown in blue. The

darkness of the colour indicates the strength of the correlation, approaching 1 or -1 as it becomes darker. When analysing the significant correlations of cyber-attacks targeting the UK and other countries between 2015 and 2022, the most notable correlation was found with the countries listed in Table 4.5 below.

Table 4. 5: Top Four States with the Highest Correlation with DDoS Attacks on the United Kingdom

	Country	Coefficient	P-Value
1	Germany	0,81	0.001
2	Belgium	0,76	0.001
3	Italy	0,58	0.001
4	Spain	0,36	0.001

In this regard, the Pearson Correlation analysis revealed that there was significant positive correlation between the UK and Germany, Belgium, Italy, and Spain regarding the frequency of cyber-attacks between 2015 and 2022. Such a high correlation over almost a decade, especially with Germany and Belgium, suggests that, although the levels of cyber-attacks targeting these three states differ, they experienced similar increases and decreases in cyber-attack trends at similar times during the 10-year period. This result provides important clues about the possible perpetrator of these cyber-attackers.

Moreover, this finding also provides important clues about European security. Despite the United Kingdom's decision to leave the European Union (EU) with Brexit in 2016 and its subsequent official departure from the EU in 2020, it is important to note that the UK's security should not be considered independent from the EU. Although the UK has adopted a more global foreign policy with the Global Britain doctrine in the post-2020 period, the strong positive correlation with Germany and Belgium provides important evidence that the UK has still been considered as a European actor, rather than systemic actor by perpetrators. In this respect, this finding also suggests that while examining cyber-attacks, it should also be taken into consideration that states are also exposed to cyber-attacks due to their alliances, especially in the same region. In other words, even if a country is not directly involved in the crisis, it can still be the target of cyber-attacks because of its close relations with the target state.

In the next section, based on these analysis and findings, this study will move beyond to create a model that simultaneously evaluates the UK's complex bilateral relations. It will evaluate different combinations and determine which positive relationships between countries have a negative impact on certain bilateral relations and *vice versa*. By this analysis, it will assess the influence of all these complex relations on cyber-attacks. This analysis is important because it will pave the way for an early warning system for state-sponsored cyber disruption operations. Accordingly, in the next section, developing such an early warning system with a machine learning model will be addressed in detail.

4.5. Artificial Intelligence-Based Early Warning Model for Detecting Politically Motivated Cyber Disruption Operations

In the recent United Kingdom's Integrated Review (2023), which outlines the British government's long-term foreign policy, it was underlined there was constant and dynamic systemic competition above and below the threshold of armed conflict across overlapping strategic arenas. This competition has been causing social and economic changes, especially with the development of new technologies, and these technological advances are leading to an increased ability to threaten, harm and damage countries, societies and individuals (United Kingdom Government, 2023, p. 9). Technological advances, such as artificial intelligence, have continued to develop and become more widely available, further increasing the threat landscape. As indicated in the European Union's Artificial Intelligence Act, the first regulation on artificial intelligence, there are multiple risks that AI poses (European Parliament, 2023). Therefore, as NATO (n.d.) emphasized with these developments, "The speed, scale and intensity" of hybrid threats, *which* NATO give high priority to counter, have intensified in recent years. Hence, as underlined in the Integrated Review report, the rise of hybrid threats necessitates a more robust and integrated approach (United Kingdom Government, 2023a, p. 33).

However, as Dimitrios Triantaphyllou (2023) emphasized AI is a double-edged sword. While AI multiplies the "*potential of AI-driven cyber threats with the proliferation of sophisticated malware and automated attacks*", on the other hand, it can also offer "*ground-breaking solutions in redefining cybersecurity strategies by*

contributing to enhanced threat detection and predictive analytics". In other words, as with every technology, AI also offers dual usage that could be used by both aggressors and defenders to enhance either defence or offence. In this regard, AI could make a significant contribution to one of the main difficulties of countering hybrid threats which is "detecting". Accordingly, NATO (n.d.) emphasizes a three-step strategy for countering hybrid threats: "Prepare", "deter", and "defend". Similarly, The UK's Strategic Report (2021, p. 70) underscores the importance of "detecting", "understanding", "attributing", and "acting" in response to state threats in physical or cyberspace domains. Both NATO and the UK stress the significance of similar initial steps in their strategies against hybrid threats. In this respect, AI has the potential to significantly contribute to both detecting and preparing against state-sponsored hybrid threats, such as cyber-attacks. In this respect, AI could help to develop an early warning system to detect hybrid threats, which is a crucial initial step to countering hybrid threats.

As Sebastiaan Rietjens (2020, p. 3) underscores that developing such a model would be crucial to provide early information to decision-makers as well as populations that enable them to adopt the appropriate measures. However, developing such an early warning system against hybrid threats is not an easy task because, in their nature, hybrid threats are designed to be undetected and unattributed. The aim of a hybrid threat is to confuse the target by sending weak and frequent signals. Since "*hybrid threats are designed to blur the distinction between peace and war*" (2020, p. 2), developing an early warning system requires new solutions. In other words, threat actors apply hybrid tools for their ability to provide plausible deniability and cause confusion and disruption for the target. Hence, developing an early warning model could be challenging for such a threat. In this respect, Treverton et al. (2018, p.91) underlined that attribution and early warning are possible but tricky tasks for cyber-attacks. In particular, when considering DDoS attacks, they are mostly low-level attacks and are carried out by many actors for different reasons. In addition, since these attacks contain a lot of noise data, it is quite difficult to distinguish which are state sponsored as a foreign policy tool.

However, being able to develop a model that can predict politically motivated state-sponsored cyber-attacks, could be crucial for resilient systems against state-

sponsored threats. In order to develop such a model, it is necessary to take into account various variables relating to states and their bilateral relations. In other words, to develop an early warning model, the complex relations between states should be included in the analysis. In this direction, the event data method – which includes almost all incidents between states – offers to include a significant number of variables related to states and their dyadic relations. For example, instead of including variables such as war, treaty, military alliance, criticism, condemnation, and diplomatic visit, event data consists of all these events and assigns a score to each event based on the Goldstein scale. Therefore, event data, which includes almost all variables related to dyadic relations and allows the transformation of bilateral relations at the quantitative level by assigning a score between -10 and +10 to each event, offers a great opportunity to develop such a model. In this case, a model that can simultaneously evaluate a significant number of bilateral relations between countries, identify patterns within these relations, and determine how these patterns affect the increase or decrease of cyber-attacks, would be able to make predictions using this model. Nevertheless, evaluating all these different variables simultaneously and finding patterns between these different variables is a very challenging task.

Nevertheless, with the development of artificial intelligence, an AI-supported early warning system can be developed for such complex relations. Artificial intelligence is the ability of computers to perform tasks that would typically require human intelligence, such as recognizing patterns, learning from experience, and making predictions. Furthermore, as a subdomain of AI, machine learning (ML) models use "*statistical algorithms to find patterns in data*" (Christie, 2020). For the analysis of big data, it is very difficult for a human to perform statistical analyses and find the correct links between too many variables without missing important ones. On the other hand, machine learning can comprehend the complex structure of data and, based on the training of given data, it can recognize patterns between variables and make predictions. For instance, by using machine learning models, models are trained by correct labelled data and the trained models are used to determine to new classification when a new unlabelled dataset is introduced (Christie, 2020).

Based on all findings in the previous section, it was decided that by simultaneously evaluating dyadic relationships of various states and cyber-attacks, it may be possible to develop an early warning model for politically motivated cyber-attacks. However, this model cannot be designed to directly identify cyber-attacks and warn countries of the potential damage from these cyber-attacks. Instead, this model could analyse the various dyadic relations a state and the frequency/volume of cyberattacks targeting that state. Based on this analysis, this model can provide warnings regarding the likelihood of a state becoming the target of an increased frequency/volume of cyber operations, particularly disruptive ones. In this regard, this study developed an AI-based early warning model that detect politically motivated cyber disruption operations based on the dyadic relations of UK.

To develop this model, the supervised machine learning (SML) algorithms are used. In SML techniques, researchers train models using labelled datasets. Based on this training, artificial intelligence models can classify the new test datasets. Therefore, this technique is called as SML model. This technique is generally preferred to make more accurate classification, especially in areas where many factors need to be considered simultaneously, and therefore, it is challenging to make the classification. In this regard, SML models are used in different sectors, from detecting anomalies in networks (Elmrabit et al., 2020; Nawir et al., 2018) to disease diagnosis (Sokoliuk et al., 2020). For a similar task, in this study, to predict/classify whether there will be significant cyber operations that exceed the threshold when new conflict-cooperation scores between countries are obtained, supervised machine learning models are used.

There are several supervised machine learning algorithms such as Random Forest (RF), Support Vector Machines (SVM), Gradient Boosting and K-Nearest Neighbors (KNN). First of all, the Random Forest model is designed to predict a value or class by combining the results of multiple decision trees to solve classification and regression problems. This model is used for various applications, including cybersecurity for its suitability for nonlinear problems, high accuracy, and efficient computation (A. K. Singh et al., 2023). Secondly, the SVM is an important model for solving complex classification, regression, and outlier detection problems. This model works by constructing a hyperplane that separates data points into different classes (such as anomalies and normal instances). In this regard, the model tries to find the

hyperplane that has the maximum margin between the classes (Ioannou & Vassiliou, 2021). Thirdly, Gradient Boosting is an ensemble learning approach that improves prediction accuracy by combining multiple weak models to create a stronger prediction model. In this machine learning model, each successive model corrects the errors of the previous models by focusing on the residual errors, gradually increasing the accuracy of the ensemble prediction (Natekin & Knoll, 2013). Last but not least, KNN is a non-parametric algorithm which classifies data points based on their proximity and association with other available data. The KNN model calculates the distance between data points, and based on the proximity of data points, it assigns a class using the most frequent class or average (Martinasek et al., 2016).

Given that the four models employ distinctive classification techniques, it is decided that rather than opting for a single approach, all four supervised machine learning models are trained. To train these models, the UK's conflict-cooperation scores with 14 countries between 2014-2023 and cyber disruption operations targeting the UK between 2014 and 2023 were used as the training data. Before presenting the findings, it is important to explain why these 14 countries' dyadic relations with the UK were selected. There are five major reasons:

First of all, as mentioned above, the UK's six dyadic relations with Iran, Israel, China, Hong Kong, Ukraine, and Russia were included. Secondly, due to special relations, the increasing partnership in recent years and the increasing rivalry with China, the United States-UK dyadic relation was also included. Especially as indicated in the Integrated Review report, systemic competition, the main driver of the deteriorating security environment, has been intensifying for UK (United Kingdom Government, 2023a, p. 8). In this respect, as a part of the US-led international system, the relations between the two countries should be included in the analysis. Thirdly, with the outbreak of the Russia-Ukraine War in 2022, two Nordic states -Finland and Sweden- have faced serious pressure from Russia, especially after they expressed their desire to become a member of NATO. Against this pressure, The United Kingdom have assured unconditional military assistance and support against Russia (Walker, 2022). Hence, the UK's dyadic relations with Sweden and Finland were also included.

Fourthly, this study also included the UK's dyadic relations with Germany, Belgium, Spain, and Italy due to the significant positive correlation between the frequency of cyber disruption operations targeting the UK and these states. In the previous chapter, as discussed that these countries, especially Germany and Belgium, have a significant positive correlation in terms of being target of cyber disruption operations. By including the UK's dyadic relations with these countries, more detailed analysis could be conducted by taking into consideration the common threat actors to these states. Finally, the bilateral relations between the UK and France, which play an important role in Europe, are also included. In terms of the cyber disruption operations, there is no correlation between the UK and France. However, given France's role in the EU and the fact that it is one of the most important actors in Europe and various parts of the world, the UK's relations with France can have both regional and systemic implications. Therefore, the bilateral relations between France and the UK are also included in the model. In this respect, based on data on frequency and volumes of DDoS attacks targeting the UK and UK's 14 dyadic relations between 2014-2023, the four machine learning models were trained, and the following results were obtained.

Table 4. 6: Trained Machine Learning Models and Their Validation Performance Results

Performance Metrics / Models	Trained Machine Learning Models' Validation Performance			
	Random Forest	Gradient Boosting	SVM	KNN
Validation Accuracy	0.8689	0.8689	0.8852	0.9180
Validation Precision	0.8333	0.8333	0.8000	0.8667
Validation Recall	0.625	0.625	0.7500	0.8125
Validation F1-Score	0.7143	0.7143	0.7742	0.8387

Table 4. 7: Trained Machine Learning Models and Their Test Performance Results

Performance Metrics / Models	Machine Learning Model's Test Performance			
	Random Forest	Gradient Boosting	SVM	KNN
Test Accuracy	0.9194	0.9194	0.9194	0.9516
Test Precision	0.8571	0.8571	0.7778	0.8889
Test Recall	0.6	0.6	0.7	0.8
Test F1-Score	0.7059	0.7059	0.7368	0.8421
ROC AUC	0.9346	0.9135	0.9231	0.9337

In the assessment of these machine learning models, it is crucial to understand the key performance metrics that reflect the effectiveness of a model in making predictions. The following metrics can be measured as indicated in below:

- *Accuracy* is the proportion of total number of correct predictions.
- *Precision* is the proportion of correct predictions of the positive values.
- *Sensitivity (Recall)* is the proportion of correct positive observations out of total positive instances. Therefore, it is also called as *True Positive Rate (TPR)*.
- *The F1 score*, or *F-score*, indicates the accuracy of the test. The value of the F1 score ranges from 0 to 1. Therefore, as the score is closer to 1, the accuracy of the test increases.
- *The Area Under Curve (AUC)* measures the classification performance of the model across all potential classification thresholds (Elmrabit et al., 2020, pp. 5-6).

When evaluating both the validation and test performance of different trained machine learning models to predict whether there will be significant cyber-attacks against the UK based on dyadic relations of the UK, it was observed that among four models, KNN had the highest accuracy, precision, recall and F1-score on both validation and test. While performance metrics of validation indicate the success of the model's training data's prediction, performance metrics of test indicate how the model is good at predicting by test data. While the other models' performances are also considerably decent, KNN's especially better precision and recall in test performance, indicate that it is the most reliable machine learning models for predicting cyber disruptive operations towards the UK based on UK's dyadic relations in future.

In this context, the KNN model has learnt best the relations between the bilateral relations of the United Kingdom trained during this 10-year period and the attacks on the UK and gives the best prediction results on whether the United Kingdom would become the target based on the newly introduced dataset. In this direction, if an early warning system is developed with the KNN model over the bilateral relations of the United Kingdom, an early warning system that predicts politically motivated cyber-operations can be developed.

Moreover, in analysing the significance and impact of dyadic relations on cyber-disruption operations to the UK, the KNN Model shows that the dyadic relations of the UK with China, Iran and Ukraine are the most influential three dyadic relations in terms of the likelihood of the UK being targeted by a significant cyber-attack, as Figure 4.7 below demonstrates. Indeed, in the previous section, Binary Logistic Regression analysis also revealed that the UK's dyadic relations with China and Ukraine had a significant impact on the likelihood of disruptive cyber operations against the United Kingdom. However, the Iran-UK dyadic relation was not statistically significant, but Israel-UK was. This finding shows how artificial intelligence models can simultaneously analyse better complex variables, identify the links between these variables, and make valid predictions. In addition, not only KNN models but also other machine-learning models demonstrate that the UK-China relations consistently appear to have the most impact, with the UK-Ukraine and UK-Iran (their orders change) and the UK-Israel relations also emerge as significant in some machine learning models. Therefore, it can be put forward that the UK's political events related to China, Ukraine and Iran are the most influential dyadic relations for ML models when assessing the potential for significant cyber disruption operations against the United Kingdom.

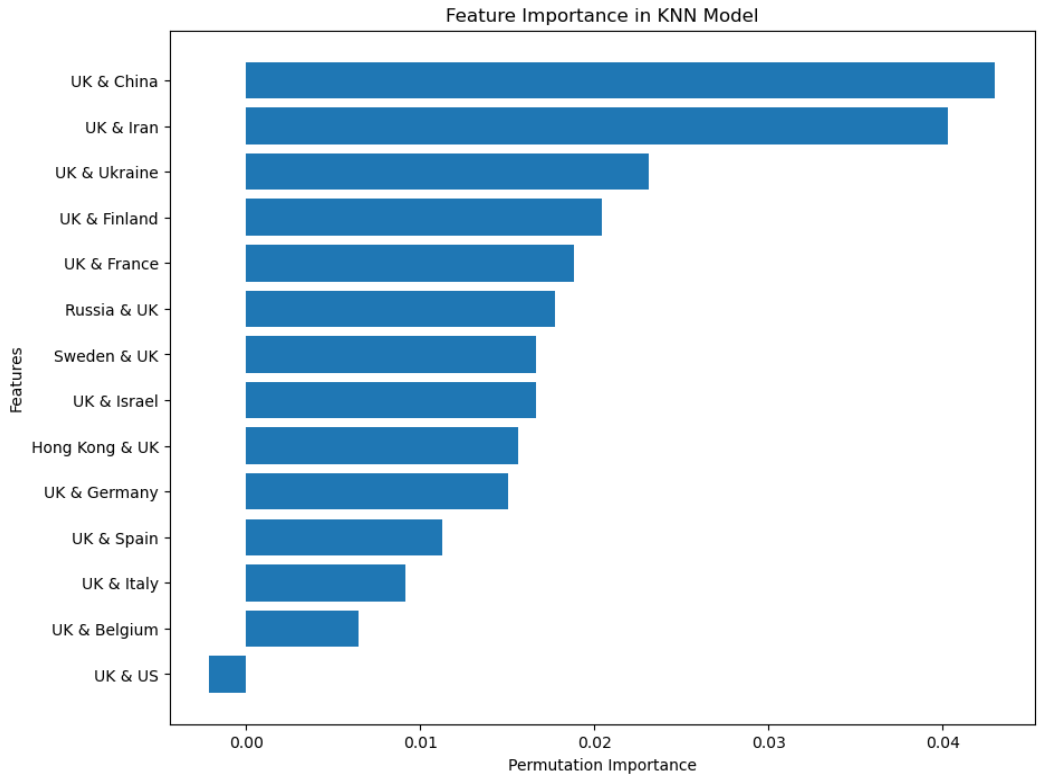

Figure 4. 7: The Impact of Dyadic Relations on Cyber Disruption Operations Targeting the UK According to the KNN Model

On the other hand, the bilateral relations between the United Kingdom and the United States appear to have a negative impact on the model's prediction performance. This indicates that including the UK-US model in the training process diminishes the model's capability of prediction. This sheds light on how threat actors view the relations between the two countries. Due to their special bilateral relations, it seems that the relations between the two countries are generally perceived as positive, and changes in their cooperation-conflict level do not significantly affect their relations. Therefore, it could be assumed that cyber-attacks are often used as a complementary tool when the UK's bilateral relations impact regional/domestic issues, as discussed earlier. In other words, UK may not be seen as a systemic rivalry but rather as a threat when involved in regional/domestic activities, as in the cases of Ukraine, Hong Kong, and Israel. Therefore, its relations with the United States do not change the target actors' perceptions but bilateral relations that affect its regional activities.

In short, this study concludes that given the consistent performance of the K-Nearest Neighbours (KNN) model across different metrics, machine learning algorithms can be effectively used to detect potential politically motivated cyber disruption attacks targeting the United Kingdom, which is focus of this research. This model could serve as a pioneering model for similar predictive systems for other states. Also, this model would pioneer the development of a real-time automated predictive model that collects the news and cyber-attacks in real time and assesses the conflict-cooperation level between states and cyber-attacks towards that country. The development of such a real-time early warning model for possible significant cyber-attacks could be a useful tool for countries to enable the necessary mechanisms to react/respond to possible significant cyber-attacks. Therefore, by improving the readiness of public institutions, citizens and private companies against cyber-attacks, this model could contribute to states and societies becoming more resilient.

CONCLUSION

This study examined the role of cyber-attacks as a foreign policy instrument in trilateral relations, focusing on the United Kingdom's trilateral relations and cyber disruption operations directed at the UK. In this context, the aim of this study was to examine how cyber disruption operations are being used by the so-called "usual suspects" as a tacit bargaining instrument against the UK in response to the UK's increased cooperation with Ukraine, Hong Kong and Israel, which are strategically important actors for Russia, China and Iran respectively. In line with this purpose, throughout this study, two main research questions were addressed: "*Under what circumstances do states resort to cyber-attacks as instruments of foreign policy?*" and "*How can states enhance their detection and identifying capabilities of politically motivated cyber disruption operations as a major hybrid threat?*"

To comprehend the role of cyber tools, this study initially conducted a literature review on hybrid warfare, in which cyber-attacks are a key component. Hybrid warfare involves a "*low-level conflict across the spectrum of capabilities*" that combines kinetic and non-kinetic means to "*enable an actor to achieve its political objectives without having to resort to large-scale conventional war*" (Najžer, 2020, p. 29). Hybrid warfare has been engaged by the actors who seek to exploit the target's vulnerabilities by utilising all available means for political objectives, integrating tactics that align with one's strategic culture, geographical conditions, and available economic and military tools without engaging power politics by overt tools. Therefore, hybrid warfare does not conform to a one-size-fits-all pattern, which makes it rather complex (Lasconjarias & Larsen, 2015, p.3). Indeed, hybrid warfare, in terms of merging conventional and unconventional means for a political purpose, is not novel. This study argues that what makes hybrid warfare novel in the new millennium is we have never before witnessed the synchronised use of different instruments of power tailored to specific vulnerabilities to produce synergistic effects on such a scale (Cullen & Reichborn-Kjennerud, 2017, p.8). In other words, its "*scale is bigger; the speed and intensity are higher*" (NATO, 2015). Hence, with these three features -*speed, scale*

and intensity- that result from increased interconnectivity and rapid technological change, hybrid usage of kinetic and non-kinetic tools creates an ambiguity which complicates the decision-making process.

In recent years, with increasing virtual connectivity through the wider use of information and communication technologies and growing economic dependency, the use of multiple tools in a synchronized way has become more effective. Hence, new tools of hybrid warfare, such as cyber-attacks and disinformation campaigns, have become prevalent tools. This development has led researchers to include more non-kinetic means in the concept of hybrid warfare, which has led to a significant expansion of the concept in the last decade. Also, after the so-called "Gerasimov Doctrine", which emphasized the growing importance of non-military means to achieve political and strategic goals, non-kinetic tools became popular in the context of hybrid warfare. Thus, instead of a combination of regular and irregular warfare, hybrid warfare came to refer to the synchronized use of non-kinetic tools such as lawfare, economic coercion, cyber-attacks, disinformation campaigns and sabotage.

On the other hand, this study also addressed the criticism of hybrid warfare stemming from its conceptual stretching, which argues that the concept has deviated from its original form and has become a buzzword (Solmaz, 2022a, 2022b; Bilal, 2021). Additionally, there are criticisms that the changing nature of modern warfare should be described using other concepts, such as hybrid threat and grey zone warfare, rather than hybrid warfare (e.g. Sean Monaghan, 2019; Azad et al., 2023; Mazarr, 2015; Caliskan & Liégeois, 2021;). To address these criticisms, the study compared hybrid warfare and grey zone warfare via Theodore Jensen's classification, which examines grey zone warfare through three camps, namely the "New Era Camp", the "Hybrid Warfare Camp" and the "Nothing New Camp" (2019). According to Jensen, "*New Era Camp"* asserts that although the tools are not new, gray zone warfare is a distinct concept because it is the natural extension of "geopolitical shifts [in] international environments" (2019, p. 18). As Hal Brands argues (2016, p. 4), the changing international realms are the driving force of these new challenges. Hence, the New Era Camp argues that previous concepts are indeed the product of the Cold War, which is the extension of the two-power competition. On the contrary, grey zone warfare is the product of the post-Cold War period. Secondly, the "*Hybrid Warfare*

Camp" considers the grey zone warfare either as a part of the hybrid warfare or used two concepts interchangeably by just using a "slash (/)" between two concepts (e.g. Cantwell, 2017; Freier et al., 2016). Among this group, some scholars (e.g., Insisa, 2023) also underscored the difficulty of distinguishing grey zone warfare and hybrid warfare through the activities of states. Lastly, the third camp- "*Nothing New Camp*", as described by Jensen (2019, p. 23), consists of those who see no utility in using the term grey zone and believe that it is simply a rebranding of existing forms of warfare concepts and nothing new about it.

Based on a literature review of hybrid warfare, hybrid threat and grey zone warfare, it was concluded that the primary distinction lies in the degree of emphasis on the use of non-kinetic tools. However, the study argues that classifying tools such as cyber-attacks is challenging and will become more difficult in the future. It is because while cyber-attacks are considered as non-kinetic tools, as the Stuxnet case demonstrated, cyber-attacks can also cause significant physical damage as kinetic tools, even if they are rare. As Nathan Freier (2009, pp. 84-85) put forward, although hybrid challenges may not be military in nature, they can still pose severe threats to national interests and necessitate a strategic response. Furthermore, with further technological developments, especially in AI, the offensive capabilities of cyber-attacks will significantly increase. Accordingly, as United Kingdom National Cyber Security Centre (2024) asserts that "*all types of cyber threat actors are already using AI to varying degrees*", and "*AI will almost certainly increase the volume and heighten the impact of cyber-attacks*".

Given the growing challenge of classifying these instruments, this study proposes a shift in focus towards a deeper understanding of the role of the tools themselves, rather than further theoretical and conceptual debates. Although different techniques can be employed simultaneously, distinct approaches are required when considering these tools, given that they differ significantly from the others in terms of both their methods of employment and their effects. It is, therefore, more effective to analyse each tool separately to minimize the impact of these tools and make societies/states more resilient against their harmful usage. In parallel to this argument, after the literature review of hybrid warfare, the focus of

this research shifted entirely to examining how cyber-attacks have been used as a tool by states.

In line with this purpose, the different roles of cyber tools in interstate relations were discussed based on the assumptions of "*three groups of scholars*". Although these three distinct perspectives were based on Lennart Maschmeyer and Nadiya Kostyuk's (2022) inaugural categorization of the strategic role and value of cyber operations, this study further developed this categorization through a systematic examination of the different roles of cyber tools in interstate relations. Thus, this study contributed to the existing literature by creating a more comprehensive theoretical framework for systematically analysing the role of cyber tools. In this classification, the first group's common viewpoint is that "cyber-attacks have been changing the nature of war" and "have led to a revolution in military affairs." They argue that cyber war would substitute for conventional war, and cyber tools could change the balance of power in the international system. On the other hand, the *second group* opposes the concept of cyber war, stressing that cyber tools are rather limited in terms of escalation and coercion, and cyber tools become effective when combined with other traditional tools. From this perspective, they argue that "cyber tools are not revolutionary but evolutionary; not substitutive but complementary". Moreover, some of the scholars in the second group assert that cyber tools are being used as conflict management tools. They argue that the main motivation for states to choose a limited-effect cyber-attack instead of a conventional weapon is to primarily prevent the escalation of conflict while at the same time eliminating critics of "nothing is being done" from the domestic audience. Lastly, the proponents in the *third group* assume that cyber tools are new standalone tools that can change the balance of power between states without using force through the cumulative impact of short-of-war cyber-attacks. Cyber-attacks are short of war, and states intentionally limit themselves to increase the reward. Also, they disagree with the notion that cyber tools are limited because they do not lead to war or conflict. Their viewpoint is that such a perspective is misguided because evaluating cyber-attacks based on their physical effects can misinterpret the behaviour of states. Instead, they propose evaluating the long-term cumulative effects of cyber-attacks instead of analysing their individual effectiveness. This is because the cumulative impacts of cyber-attacks can alter the balance of power in the international system rather than individual ones.

Based on these three different perspectives about the role of cyber tools, this study adopted a hybrid approach that combines the second and third groups' assumptions. From the second group's main assumptions, it was underscored that *cyber-attacks are considered contemporary tools of statecraft, used alongside other tools to achieve countries' particular objectives.* However, in contrast to the analysis of individual cyber-attacks, in parallel with the third school, this study also adopted the perspective that cyber tools should also be examined based on their long-term use in the context of rivalry between states. This is because, as Valeriano et al. (2018, p.11) stated, cyber strategy does not necessarily aim to obtain direct concessions. In contrast to the direct use of cyber tools for the purpose of obtaining immediate concessions, rival states employ these tools to shape long-term rivalry in a more indirect manner. By analysing long-term impacts, the way states use cyber instruments as foreign policy instruments can be evaluated from a more holistic perspective. It is also possible to better determine when and in what situation state cyber-tools become more applicable tools for states. In this way, the use of various cyber tools by different states for different motivations at different times can be more explicitly shown. Accordingly, this study put forward that *"cyber tools are utilised as foreign policy instruments by states to coerce and leverage concessions, with the eventual goal of gaining a strategic advantage over rivals".*

Furthermore, this study also aimed to expand the understanding of cyber-attacks' role by underlining the strategic role of third-party actors for rival states, which has mostly been overlooked in the literature. In other words, this study stressed why the role of cyber-attacks should also be studied through a trilateral relations lens. In general, it is expected that when there is a crisis between two countries, they engage in cyber-attacks against each other. Therefore, the role of cyber-attacks has been addressed by analysing the reciprocal cyber-attacks against each other, and their dyadic relations are examined. While this approach provides essential insights into the use of cyber-tools in bilateral relations, this study claimed that it is overlooked to recognise that states maintain both conflicting and cooperative relationships with multiple actors simultaneously. The relations of the states are not two-dimensional. These relations take place in complex networks. Hence, a single positive or negative change in bilateral relations can result in a multitude of different combinations in

different bilateral relations. The oversight of this aspect in the literature limits our understanding of the effects and causes of cyber-attacks.

Another crucial aspect that is often neglected in the literature but which this study emphasises is the fact that states can be subjected to serious cyber-attacks in the event of a rapprochement of their relations. The majority of studies in the literature focus on the examination of the cyber-attacks used during a crisis between states. They generally consider cyber-tools as a foreign policy tool in conflicts. However, this study argues that while states have various foreign policy instruments to use when their relations worsen, they are less equipped to respond when a state, particularly one of strategic importance, establishes good relations with a rival state. Nevertheless, cyber-tools are useful tools for those kinds of situations because cyber-attacks enable states to operate in grey areas due to the advantages of creating ambiguity and deniability. When states are unwilling to use other tools but want to do "something" "rather than doing nothing"; cyber-attacks offer strategic utility. Hence, cyber-attacks are viable options for states to convey signals without triggering a significant response. Accordingly, this study contends that in contrast to explicit bargaining, which relies on informal or formal diplomatic exchanges, states use cyber disruption operations as instruments of tacit bargaining against rivals when the rival increases its cooperation with a strategically important state in order to influence the rivals' policy choices through behaviour.

Based on this hybrid approach that includes the second and third group of scholar's perspectives as well as the role of third actor relations and diplomatic good relations, to examine the complex relations between the changing dyadic relations of countries and the use of cyber disruption operations as a complementary foreign policy tool, the United Kingdom and its trilateral relations with "Russia-Ukraine", "China-Hong Kong", and "Iran-Israel", between 2014-2023 were chosen as a case study. In this context, this study conducted three logistic regression analyses and tested whether increasing/decreasing conflict-cooperation scores of each trilateral relation had an impact on the increase/decrease of cyber disruption operations toward the UK between 2014-2023. Based on these analyses, this study observed that there was an increased likelihood of serious cyber-disruption operations towards the UK when the UK's cooperation level increased with Israel (0.97), Ukraine (0.80) and Hong Kong (0.49)

(as H2a suggests) whereas UK's conflict level increased with China (-1.55) and Russia (-0.48) (as H1 suggests). Among these relations, with a "-1.55" coefficient, the UK-China bilateral relations had the most impact on the increase in cyber-attacks directed at the UK. At this point, a small parenthesis should be opened: It is important to note that these findings did not directly imply that China and Russia were the perpetrators of cyber operations against the United Kingdom. The study did not conclude that the UK was the target of significant cyber disruption operations solely as a result of its conflict with Russia and China. Rather, it indicated that such operations were more likely to occur as the level of conflict increased.

However, since this study analysed the impact of a period of ten years of bilateral relations on whether cyber-disruption operations exceed the threshold, the statistically significant results indeed make these countries the usual suspects of cyber-attacks on the UK. The fact that there is a statistically significant relationship in a 10-year period indicates that this is not a coincidence; it is being used as a complementary instrument in foreign policy. In addition, the findings of the increasing possibility of significant cyber-disruption when the cooperation level increases with Ukraine, Hong Kong and Israel also provide a serious clue that the three usual suspects (Russia, China and Iran) may play a significant role in conducting cyber-attacks.

Moreover, this study also found that compared to China and Russia, there was no statistical relationship between the UK-Iran relations and cyber-attacks targeting the UK. Although this could stem from Iran's limited technical capacity in comparison with China and Russia, this study posited that the UK's relations with Israel – the main rival and the archenemy of Iran in the region – could be more urging to the use of cyber disruption operations against the UK. The role that the UK plays in the region may be more important to Iran than its direct bilateral relations with itself. Also, the deterioration of relations with the UK might not be a significant concern, given that the relations were already characterised by a certain degree of tension. Therefore, it is unsurprising that there is no statistical relationship with UK-Iran, but there is UK-Israel on the increasing likelihood of the cyber-attacks. In this respect, the fact that increasing likelihood of cyber-attacks directing the UK when its cooperation level increases with Israel, Ukraine and Hong Kong demonstrated that three usual suspects might see the United Kingdom as a potential threat. This threat arises when the UK is

directly involved in regional/internal affairs by engaging in relations with Ukraine, Hong Kong, and Israel, where Russia, China, and Iran attach great strategic importance.

In addition, this study found that significant cyber disruption operations specifically targeted the United Kingdom in 2020-2021, when the UK began to pursue active policies both systemically and regionally in line with the Global Britain doctrine. In this period, the United Kingdom increased its engagement in regions where the main state threats to the UK, which are Russia, China and Iran, played a significant role, and tried to balance these state-based threats through increasing partnerships in these regions. In response to playing an active role at both the systemic and regional levels by actively implementing the active Global Britain doctrine in this period, the UK was exposed to the most intense cyber disruption operations. Russia, China and Iran, who were reluctant to use other tools but wanted to do "something" "rather than doing nothing", when the UK increased its cooperation with Ukraine, Hong Kong and Israel, cyber disruption operations offered strategic utility for these states. In other words, in contrast to explicit bargaining, which relies on informal or formal diplomat exchanges, by using cyber disruption operations as an instrument of tacit bargaining, these states try to influence the policy choices of the UK through behaviour". In this context, the fact that United Kingdom experienced more cyber-attacks in these years is also important in terms of validate the hypotheses and assumptions of this study regarding cyber-disruption operations.

While the primary focus of this study is the trilateral relations of the United Kingdom, researchers may examine a range of trilateral relations and test the relationships between them and cyber-attacks. For example, they can examine the relationships between foreign policy and cyber-attacks in trilateral relations such as "US-Turkey-Greece", "US-China-Australia", and "Iran-Israel-United Arab Emirates/Saudi Arabia". These examples can be easily expanded by including numerous states across different regions. The applicability of this method and trilateral perspective to analyse the role of the cyber-tools as a foreign policy tool, indicates the high external validity of this selected methodology and hybrid perspective.

On the other hand, to increase the internal validity of this study, this study also conducted additional analyses. In this context, the increase in cyber-attacks when the UK has increased cooperation with Israel, Ukraine, and Hong Kong also suggests that cyber threat actors are also targeting the allies of the targeted state. As a member of various international organizations and alliances, the security of the UK is not independent, especially from regional actors. Even if cyberspace is a dimension with no geographical limitations or physical limits, regional aspects still play a major role. Therefore, this study also tested whether there was a correlation between the frequency of cyber-attacks targeting the UK and the countries that are in Western and Northern Europe. For this aim, Pearson Correlation Analysis was conducted, and analysis revealed that there was significant positive correlation between the UK and Germany, Belgium, Italy, and Spain regarding the frequency of cyber-attacks between 2015 and 2022. Such a high correlation over almost a decade, especially with Germany and Belgium, suggests that, although the levels of cyber-attacks targeting these three states differ, they experienced similar increases and decreases in cyber-attack trends at similar times during the 10-year period. This result provided important clues about the possible perpetrator of these cyber-attacks.

Moreover, this finding also provides important clues about European security. Despite the United Kingdom's decision to leave the European Union (EU) with Brexit in 2016 and its subsequent official departure from the EU in 2020, it is important to note that the UK's security should not be considered independent from the EU. Although the UK has adopted a more global foreign policy with the Global Britain doctrine in the post-2020 period, the strong positive correlation with Germany and Belgium provides important evidence that the UK has still been considered a European actor rather than a systemic actor by perpetrators. In this respect, this finding also suggests that while examining cyber-attacks, it should also be taken into consideration that states are also exposed to cyber-attacks due to their alliances, especially in the same region. In other words, even if a country is not directly involved in the crisis, it can still be the target of cyber-attacks because of its close relations with the target state. Therefore, this finding demonstrates why it's not enough to only analyse the relationship between two countries when studying cyber-attacks. Moreover, even though this study provides a trilateral analysis, this may also be inadequate for understanding the role of cyber-attacks. The high correlation between Germany and

the United Kingdom indicates that studying the United Kingdom in disregarding Germany would limit the study. Therefore, future studies should also take regional elements into account in order to obtain a more comprehensive analysis.

In light of the findings of the analyses, this study also evaluated the use of cyber disruption operations in fluctuating relations and discussed why DDoS attacks have been preferred as a complementary foreign policy tool, particularly within the framework of modern coercive diplomacy. Cyber disruption operations generally target the business sector and public institutions that are widely used by the people rather than military or governmental targets. While a state may be able to hide an attack on military or government sources, it becomes much harder to conceal a DDoS attack that targets publicly accessible sources. It is because people can experience the impacts of DDoS attacks (Maness & Valeriano, 2016, p. 317). In this regard, the main purpose of this is to create a psychological impact by affecting as many people as possible with cyber-attacks. By conducting constant and frequent cyber disruption operations to targets that more people can experience the impact of the attacks, threat actors aim to create a perception of insecurity and incompetence towards the government and related institutions. Hence, states that want to express their disturbance about an incident without provoking a significant response may resort to cyber disruption operations to directly influence society and indirectly impact the government. Thus, cyber disruption operations are used to conduct "influence operations" with the aim of influencing society and creating disruption for political purposes.

Since these attacks also cause a limited impact on the target but a greater impact on society, giving proper responses is also challenging for states. Targeted countries encounter significant difficulties in detecting these hybrid threats and attributing them, particularly when the threat is low-level and sponsored actors persistently deny involvement. Therefore, while hybrid threats are already difficult to detect and attribute, deterring and responding to hybrid threats properly is even more challenging. Especially in the future, with new technologies, there will be more attack options, and the number and scope of the hybrid threats will increase significantly. Hence, it will not be possible to prevent or deter the usage of all these tools.

In this context, this study contented the necessity of enhancing states' and societies' resilience capabilities against hybrid tools rather than completely trying to prevent them. To increase resilience to combat hybrid threats, one of the primary steps is to detect the attacks. Due to the design of the internet, cyber-attacks are inherently difficult to detect and identify. Although it is relatively straightforward to realize the effects of a DDoS attack when compared with other forms of cyber-attack, such as espionage and sabotage; it is crucial to determine if the DDoS attack is sponsored by a state and which state is responsible for it. Hence, detection the anomaly is one of the priority steps in combating hybrid threats, especially for cyber-attacks. In accordance, to enhance the detection capacities of the states regarding the second main research question, this study also developed an early warning system to detect politically motivated cyber disruption operations based on the analysis of the complex dynamic relations of states.

In order to develop a system, it was necessary to create a model capable of simultaneously evaluating different bilateral relationships, identifying patterns within these relationships, and determining how these patterns influence the increase or decrease of cyber-attacks. However, evaluating all these variables simultaneously and finding patterns between them is a very challenging task. In this context, the ability to identify and recognize patterns within complex big data, and the capacity to make high accuracy/precise predictions based on learning from the training data when a new dataset is introduced; this study applied Artificial Intelligence (AI) models in developing an early warning system to predict possible politically motivated significant cyber disruption operations.

Indeed, as with all technological tools, AI is also a dual-use technology. As Jenny Jun (2024) underlines, "*many AI-enhanced techniques are a "double-edged sword" that can aid both the offence and the defence*". It is inevitable that the frequency and intensity of cyber-attacks will increase with the development and broad dissemination of AI. However, it is also evident that artificial intelligence will provide significant assistance for defence. In order to reinforce cyber defence, states have already been trying to integrate AI into their systems to ensure the security of their digital infrastructure. For example, Rob Joyce, the director of the United States National Security Agency Cybersecurity Directorate, revealed that

AI helped the US in detecting Chinese operations targeting critical US infrastructure (Vicens, 2024). In parallel, in this study, artificial intelligence models were also used for the early warning system to be developed to predict possible politically motivated significant cyber disruption operations.

To predict/classify whether there will be cyber operations that exceed the threshold when new conflict-cooperation scores between countries are obtained, this study applied supervised machine learning algorithms. Accordingly, this study used the four supervised Machine Learning models, which are *Random Forest, Support Vector Machines, Gradient Boosting* and *K-Nearest Neighbors.* These models were trained with the dataset of the United Kingdom's bilateral relations (conflict-cooperation score) with 14 states and the dataset on whether DDoS attacks' frequency and volume directed at the United Kingdom between 2014-2023, exceed the threshold (in other words, whether there is significant cyber disruption operation or not). After training these four models, based on AI performance metrics, this study compared these four ML models' performance to determine which model was superior in which aspects and which model was the most promising for developing an early warning system for politically motivated cyber disruption operations. In this regard, this study found that among four models, *K-Nearest Neighbors (KNN)* had the highest accuracy, precision, recall and F1-score on both validation and test.

While the other models' performances were also considerably decent, KNN's especially better precision and recall in test performance indicated that it was the most reliable ML model for predicting cyber disruptive operations towards the UK based on the UK's dyadic relations in future. In this context, the KNN model performed best in identifying the relationships between the UK's bilateral relations and cyber-attacks against the UK, based on training with the 10-year period dataset. It also provided the most accurate predictions of whether the UK would become a target based on the newly introduced dataset. In this direction, this study offered a prototype AI-based early warning system that predicts politically motivated cyber-operations against the United Kingdom based on its dyadic relations.

Moreover, the KNN model also offers a feature which shows the significance of each dyadic relations on the model's prediction performance. In other words, it can

be identified which of the bilateral relations is more important in the predictive capacity of the model. In this respect, dyadic relations of the UK with China, Iran and Ukraine are the most influential three dyadic relations in terms of the likelihood of the UK being targeted by a significant cyber-attack, as discussed in the last chapter. Indeed, according to Binary Logistic Regression analysis, the Iran-UK dyadic relation was not statistically significant, but the Israel-UK was. In contrast to Logistic Regression Analysis' results, KNN model found out that Iran-UK relations were also important to make prediction about the cyber-attacks targeting the UK. This finding indicates that how AI models can analyse better complex variables, better identify the links between these variables, and make valid predictions. In addition, not only KNN model but also other machine-learning models demonstrate that the UK-China relations consistently appear to have the most impact, along with UK-Ukraine and UK-Iran and the UK-Israel relations (their ranks change). Therefore, this study provided importance clues that UK's political events related to China, Ukraine and Iran are the most influential dyadic relations for ML models when assessing the potential for significant cyber disruption operations against the United Kingdom.

Last but not least, bilateral relations between the United Kingdom and the United States appear to have a negative impact on the model's prediction performance. This finding indicated that including the UK-US model in the training process undermines the model's prediction performance. Although this fact may be viewed as a negative aspect of the model, it does, in fact, reinforce the findings of the logistic regression analysis. Given the special nature of the US-UK relations, it was assumed that the general perception of their relations was positive. Therefore, changes in the level of cooperation and conflict between the two countries did not significantly affect other countries' perceptions. In this regard, it could be asserted that cyber-attacks are often used as a complementary foreign policy tool of the usual suspects when the UK is directly involved in regional/domestic affairs. In other words, the UK was not seen as a systemic rivalry but rather as a threat when involved in regional/domestic affairs, as in the cases of Ukraine, Hong Kong, and Israel. Therefore, its relations with the United States do not change the usual suspects' perceptions of the United Kingdom, but its bilateral relations affect its activities at the regional level.

In conclusion, this study offers that given the consistent performance of the KNN model across different metrics, machine learning algorithms can be effectively used to detect potential politically motivated cyber disruption attacks targeting the United Kingdom, which is one of the focuses of this research. The model was developed as a prototype for the UK and has not been tested for other countries. However, this method has the potential to be applied in other countries as well. Furthermore, this model could pave the way for the development of a more complex and advanced version, such as a real-time automated predictive model. This advanced model would collect news and information about cyber-attacks in real time. In this way, it could evaluate the level of conflict or cooperation between states and make predictions about cyber-attacks in that country. The development of such a model for possible significant cyber-attacks could be a useful tool for countries to enable the necessary mechanisms to react/respond to possible significant cyber-attacks. Therefore, by improving the readiness of public institutions, citizens and private companies against cyber-attacks, this model could contribute to states and societies becoming more resilient. Moreover, the creation of a more integrated model that includes different countries, such as the UK and Germany, which have a significant correlation in terms of being the target of DDoS attacks over the last decade, would also facilitate the development of not only country-based models but also region-based models that contribute to regional security. In this context, the development of this promising AI-based early warning system not only fosters interdisciplinary research but also significantly contributes to the literature by serving as a versatile tool for analysing the complex relationship between cyber-attacks and foreign policy across various contexts.

BIBLIOGRAPHY

Documents & Reports

BARAN, Paul, “On Distributed Communications Networks,” *RAND Corporation*, 1962. Retrieved from: https://www.rand.org/pubs/papers/P2626.html (Accessed 14 October 2023).

CORDESMAN, Anthony H., and Grace HWANG, "Chronology of Possible Chinese Gray Area and Hybrid Warfare Operations," *Center for Strategic and International Studies (CSIS)*, 2020. Retrieved from: https://www.jstor.org/stable/resrep25228.

CULLEN, Patrick J., and Erik REICHBORN-KJENNERUD, “Understanding Hybrid Warfare,” *MCDC Countering Hybrid Warfare Project (A Multinational Capability Development Campaign)*, 2017. Retrieved from: https://assets.publishing.service.gov.uk/media/5a8228a540f0b62305b92caa/dar_mcdc_hybrid_warfare.pdf (Accessed 18 January 2024).

CURTIS, John, “Taiwan: History, Politics and UK Relations,” *House of Common Library*, 28 April 2024. Retrieved from: https://researchbriefings.files.parliament.uk/documents/CBP-9254/CBP-9254.pdf (Accessed 10 May 2024).

DOLEV, Boaz, and David SIMAN-TOV, "Iranian Cyber Influence Operations against Israel Disguised as Ransomware Attacks," *The Institute for National Security Studies*, 27 January 2022. Retrieved from: https://www.inss.org.il/wp-content/uploads/2022/01/special-publication-27012022-1.pdf (Accessed 18 October 2023).

ELLIS, James, David FISHER, Thomas A. LONGSTAFF, Linda PESANTE, and Richard D. PETHIA, “Report to the President’s Commission on Critical Infrastructure Protection,” *Software Engineering Institute*, 1997. Retrieved from: https://insights.sei.cmu.edu/documents/1907/1997_003_001_16538.pdf (Accessed 27 October 2023).

FOXALL, Andrew, “How Russia ‘Positions’ the United Kingdom,” *Council on Geostrategy*, 2021. Retrieved from: https://www.geostrategy.org.uk/app/uploads/2021/04/Policy-Paper-SBIPP02-07042021.pdf (Accessed 30 April 2024).

GALEOTTI, Mark, "The Minsk Accords: Should Britain Declare Them Dead?" *Council on Geostrategy*, 2021. Retrieved from: https://www.geostrategy.org.uk/britains-world/the-minsk-accords-should-britain-declare-them-dead/ (Accessed 6 May 2024).

GOWER, Melanie, and Esme KIRK-WADE, "Hong Kong British National (Overseas) Visa," *United Kingdom House of Commons*, 5 May 2021. Retrieved from: https://researchbriefings.files.parliament.uk/documents/CBP-8939/CBP-8939.pdf (Accessed 14 May 2024).

HUMMEL, Richard, and Roland DOBBINS, "War, Religion, and Politics: A Battleground For DDoS," *NETSCOUT DDoS Threat Intelligence Report*, September 2022.

HUMMEL, Richard, Roland DOBBINS, Chris CONRAD, Filippo VITALE, Chad ROBERTSON, Roman LARA, and others, "NETSCOUT DDoS Threat Intelligence Report: Complete Network Visibility Enables Total Network Control," *NETSCOUT*, February 2023.

KAVANAGH, Camino, "New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?" *Carnegie Endowment for International Peace*, 2019. Retrieved from: https://carnegieendowment.org/research/2019/08/new-tech-new-threats-and-new-governance-challenges-an-opportunity-to-craft-smarter-responses?lang=en (Accessed 6 June 2024).

KENNAN, George F., "Policy Planning Staff Memorandum," *RG 273, Records of the National Security Council, NSC 10/2, U.S. National Archives and Records Administration*, 1948. Retrieved from: http://academic.brooklyn.cuny.edu/history/johnson/65ciafounding3.htm (Accessed 4 March 2024).

KOFMAN, Michael, Anya FINK, Dmitry GORENBURG, Mary CHESNUT, Jeffrey EDMONDS, and Julian WALLER, "Russian Military Strategy: Core Tenets and Operational Concepts," *Center for Naval Analyses (CNA)*, 2021. Retrieved from: https://www.cna.org/reports/2021/10/Russian-Military%20-Strategy-Core-Tenets-and-Operational-Concepts.pdf (Accessed 25 February 2024).

LIEBERTHAL, Kenneth, and Peter W. SINGER, "Cybersecurity and U.S.-China Relations," *21St Century Defense Initiative at Brookings*, 2012. Retrieved from: https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf (Accessed 1 November 2023).

LOFT, Philip, "Iran's Influence in the Middle East," *House of Common Library*, 14 April 2023. Retrieved from: https://researchbriefings.files.parliament.uk/documents/CBP-9504/CBP-9504.pdf (Accessed 10 May 2024).

MATROSOV, Aleksandr, Eugene RODIONOV, David HARLEY, and Juraj MALCHO, "Stuxnet Under the Microscope," *ESET*, 20 January 2011.

Retrieved from: https://scadahacker.com/library/Documents/Cyber_Events/ESET%20-%20Stuxnet%20Under%20the%20Microscope%20v1.1.pdf (Accessed 19 September 2023).

MCCLELLAND, Charles, "World Event/Interaction Survey, 1966-1978," *Inter-university Consortium for Political and Social Research*, 1978. Retrieved from: https://www.cs.rice.edu/~devika/conflict/papers/05211-Codebook.pdf (Accessed 12 January 2023).

MILLS, Claire, "Military Assistance to Ukraine 2014-2021," *United Kingdom House of Commons*, 4 March 2022. Retrieved from: https://commonslibrary.parliament.uk/research-briefings/sn07135/ (Accessed 6 May 2024).

MILLS, Claire, "Detailed Timeline of UK Military Assistance to Ukraine (February 2022- Present)," *United Kingdom House of Commons*, 1 May 2024a. Retrieved from: https://researchbriefings.files.parliament.uk/documents/CBP-9914/CBP-9914.pdf (Accessed 15 May 2024).

MILLS, Claire, "Military Assistance to Ukraine since the Russian Invasion," *United Kingdom House of Commons*, 2 May 2024b. Retrieved from: https://commonslibrary.parliament.uk/research-briefings/cbp-9477/ (Accessed 6 May 2024).

MILLS, Claire, "Sanctions against Russia," *United Kingdom House of Commons*, 28 February 2024c. Retrieved from: https://researchbriefings.files.parliament.uk/documents/CBP-9481/CBP-9481.pdf (Accessed 6 May 2024).

MUELLER, Grace B., Benjamin JENSEN, Brandon VALERIANO, Ryan C. MANESS, and Jose M. MACIAS, "Cyber Operations during the Russo-Ukrainian War," *The Center for Strategic and International Studies*, 13 July 2023. Retrieved from: https://www.jstor.org/stable/resrep52130 (Accessed 12 February 2024).

NYE, Joseph S., "Cyber Power," *Harvard Kennedy School Belfer Center for Science and International Affairs*, 2010. Retrieved from: https://www.belfercenter.org/publication/cyber-power (Accessed 1 November 2023).

RIETJENS, Sebastiaan, "A Warning System for Hybrid Threats – Is It Possible?" *Hybrid CoE Strategic Analysis (The European Centre of Excellence for Countering Hybrid Threats)*, June 2020. Retrieved from: https://www.hybridcoe.fi/wp-content/uploads/2020/06/Strategic-Analysis_22_WarningSystem-1.pdf (Accessed 30 May 2024).

RUMER, Eugene, "The Primakov (Not Gerasimov) Doctrine in Action," *Carnegie Endowment for International Peace*, 5 June 2019. Retrieved from: https://carnegieendowment.org/2019/06/05/primakov-not-gerasimov-doctrine-in-action-pub-79254 (Accessed 20 January 2024).

SCHRODT, Philip A., "TABARI: Textual Analysis by Augmented Replacement Instructions," *Manuel*, 2011. Retrieved from: https://parusanalytics.com/eventdata/tabari.dir/tabari.manual.0.7.6.pdf (Accessed 16 November 2023).

MONAGHAN, Sean, "MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare: Conceptual Foundations and Implications for Defence Forces," 2019. Retrieved from: https://assets.publishing.service.gov.uk/media/5da9a79ae5274a5ca507c6bb/20190401-MCDC_CHW_Information_note_-_Conceptual_Foundations.pdf (Accessed 10 February 2024).

SESKURIA, Natia, "Russia's "Hybrid Aggression" against Georgia: The Use of Local and External Tools," *Center for Strategies & International Studies*, 21 September 2021. Retrieved from: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210921_Seskuria_Russia_Georgia.pdf?VersionId=__d9rw2TtaDba9xaHASf6lCEmJ.oqhA7 (Accessed 31 January 2024).

TREVERTON, Gregory F., Andrew THVEDT, Alicia R. CHEN, Kathy LEE, and Madeline McCUE, "Addressing Hybrid Threats," *Swedish Defence University*, 2018. Retrieved from: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Treverton-AddressingHybridThreats.pdf (Accessed 30 May 2024).

VOO, Julia, Irfan HEMANI, and Daniel CASSIDY, "National Cyber Power Index 2022, Cyber Project," *Harvard Kennedy School Belfer Center for Science and International Affairs*, September 2022. Retrieved from: https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf (Accessed 10 June 2024).

VOO, Julia, Irfan HEMANI, Simon JONES, Winnona DeSOMBRE, Daniel CASSIDY, and Anina SCHWARZENBACH, "National Cyber Power Index 2020: Methodology and Analytical Considerations," *China Cyber Policy Initiative: Harvard Kennedy School Belfer Center for Science and International Affairs*, September 2020. Retrieved from: https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf (Accessed 2 June 2024).

WALKER, Nigel, "Conflict in Ukraine: A Timeline (2014 - Eve of 2022 Invasion)," *House of Common Library*, 23 August 2023. Retrieved from: https://researchbriefings.files.parliament.uk/documents/CBP-9476/CBP-9476.pdf (Accessed 1 May 2024).

"2023/24 Israel-Hamas Conflict: UK and International Response," *UK House of Commons Library Specialists*, 3 April 2024. Retrieved from: https://researchbriefings.files.parliament.uk/documents/CBP-9874/CBP-9874.pdf (Accessed 11 May 2024).

"China and the Rules-Based International System," *United Kingdom House of Commons Foreign Affairs Committee*, 26 March 2019. Retrieved from: https://publications.parliament.uk/pa/cm201719/cmselect/cmfaff/612/612.pdf (Accessed 8 May 2024).

"Developments in the Field of Information and Telecommunications in the Context of International Security A/RES/53/70," *United Nations General Assembly*, 4 December 1998. Retrieved from: https://disarmament.unoda.org/ict-security/ (Accessed 30 October 2023).

"Factsheet - Countering Hybrid Threats," *European Commission*, March 2022. Retrieved from: https://defence-industry-space.ec.europa.eu/document/download/3b90af44-dbf6-4ea7-a24a-b6c60305c9be_en?filename=Factsheet%20-%20Countering%20Hybrid%20Threats.pdf (Accessed 21 April 2024).

"Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy," *United Kingdom Government*, 16 March 2021. Retrieved from: https://assets.publishing.service.gov.uk/media/60644e4bd3bf7f0c91eababd/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf (Accessed 8 May 2024).

"Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174)," *United Nations General Assembly*, 22 July 2015. Retrieved from: https://digitallibrary.un.org/record/799853 (Accessed 30 October 2023).

"Hybrid Warfare," *U.S. Government Accountability Office*, 10 September 2010. Retrieved from: https://www.gao.gov/assets/gao-10-1036r.pdf (Accessed 19 January 2024).

"Integrated Review Refresh 2023 Responding to a More Contested and Volatile World," *United Kingdom Government*, 13 March 2023a. Retrieved from: https://assets.publishing.service.gov.uk/media/641d72f45155a2000c6ad5d5/11857435_NS_IR_Refresh_2023_Supply_AllPages_Revision_7_WEB_PDF.pdf (Accessed 10 May 2024).

"JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Joint Framework on Countering Hybrid Threats a European Union Response," *European Commission*, JOIN/2016/018. Retrieved from: 6 April 2016. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018 (Accessed 22 January 2024).

"Munich Security Index 2023," *Munich Security Conference*, 2023. Retrieved from: https://securityconference.org/assets/01_Bilder_Inhalte/03_Medien/02_Publikationen/2023/Munich_Security_Index_2023.pdf (Accessed 14 May 2023).

"Munich Security Report 2015: Collapsing Order, Reluctant Guardians?," *Munich Security Conference*, 25 January 2015. Retrieved from: https://securityconference.org/assets/02_Dokumente/01_Publikationen/MunichSecurityReport_2015.pdf (12 November 2023).

"NATO 2022 Strategic Concept," *NATO*, 202a2. Retrieved from: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf (12 November 2023).

"National Cyber Strategy 2022: Annual Progress Report 2022 - 2023," *United Kingdom Cabinet Office*, 2023b. Retrieved from: https://assets.publishing.service.gov.uk/media/64e60e4b1ff6f3000d70ae7c/14.283_CO_National_Cyber_Strategy_Progress_Report_Web_v3.pdf (Accessed 31 March 2024).

"NCSC Annual Review 2023," *United Kingdom National Cyber Security Centre*, 14 November 2023b. Retrieved from: https://www.ncsc.gov.uk/pdfs/reports/Annual_Review_2023.pdf (Accessed 28 May 2024).

"Quadrennial Defense Review Report," *U.S. Department of Defence*, 2010. Retrieved from: https://history.defense.gov/Portals/70/Documents/quadrennial/QDR2010.pdf?ver=vVJYRVwNdnGb_00ixF0UfQ%3d%3d (Accessed 31 January 2024).

"Russia," *United Kingdom Intelligence and Security Committee of Parliament*, 21 July 2020. Retrieved from: https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf (Accessed 15 May 2024).

"Strategic Trends Programme: Future Character of Conflict," *UK Ministry of Defence's Development*, 2010. Retrieved from: https://assets.publishing.service.gov.uk/media/5a80698aed915d74e33fa481/20151210-Archived_DCDC_FCOC.pdf (Accessed 31 January 2024).

"The Near-Term Impact of AI on the Cyber Threat," *United Kingdom National Cyber Security Centre*, 24 January 2024a. Retrieved from: https://www.ncsc.gov.uk/pdfs/report/impact-of-ai-on-cyber-threat.pdf (Accessed 31 May 2024).

"The UK and China's Security and Trade Relationship: A Strategic Void," *United Kingdom House of Lords International Relations and Defence Committee*, 10 September 2021. Retrieved from: https://committees.parliament.uk/publications/7214/documents/75842/default/ (Accessed 8 May 2024).

"UK Calls out China State-Affiliated Actors for Malicious Cyber Targeting of UK Democratic Institutions and Parliamentarians," *National Cyber Security Centre*, 2024b. Retrieved from: https://www.ncsc.gov.uk/pdfs/news/china-state-affiliated-actors-target-uk-democratic-institutions-parliamentarians.pdf (Accessed 10 May 2024).

Books & Books Chapters

ABRAHAMIAN, Ervand, **The Coup: 1953, the CIA, and the Roots of Modern U.S.-Iranian Relations**, New York: The New Press, 2013.

ARISTOTLE, **Metaphysics**, Translated by C.D.C. Reeve, Hackett Publishing, 2016.

ARNAB, Raghunath, "Complex Survey Design", in **Survey Sampling Theory and Applications**, London San Diego, CA: AP, Academic Press. 2017, pp. 673–89.

AWAD, Mariette, and Rahul KHANNA, "Support Vector Machines for Classification", in **Efficient Learning Machines**, Berkeley, CA: Apress, 2015, pp. 39–66.

BAYLIS, John, Steve SMITH, and Patrica OWENS, **The Globalization of World Politics: An Introduction to International Relations**, Sixth Edition, Oxford; New York, NY: Oxford University Press, 2014.

BAYUK, Jennifer L., **Cyber Security Policy Guidebook**, Hoboken, NJ: Wiley, 2012.

BETZ, David, and Tim STEVENS, **Cyberspace and the State: Toward a Strategy for Cyber-Power**, Adelphi, 424, IISS, The International Institute for Strategic Studies, 2011.

BUZAN, Barry, and Ole WÆVER, **Regions and Powers: The Structure of International Security**, Cambridge: Cambridge University Press, 2003.

BRAW, Elisabeth, **The Defender's Dilemma: Identifying and Deterring Gray-Zone Aggression**, Washington, DC: American Enterprise Institute, 2022.

BRODIE, Bernard (ed.), **The Absolute Weapon: Atomic Power and World Order**, New York: Harcourt, Brace and Company, 1946.

BUCHANAN, Ben, **The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics**, Cambridge, Massachusetts: Harvard University Press, 2020.

CHAMBERS, John, **Countering Gray-Zone Hybrid Threats: An Analysis of Russia's 'New Generation Warfare' and Implications for the US Army**, Modern War Institute at West Point, 2016.

CLARK, Christopher, **Uyurgezerler**, translated by Cem Demirkan, Pegasus Yayınları, 2017.

CLARKE, Richard A., and Robert KNAKE, **Cyber War: The Next Threat to National Security and What to Do About It**, First Edition, New York: Ecco, 2010.

CLAUSEWITZ, Carl von, **On War**, translated by Michael Howard and Peter Paret, Princeton, N.J: Princeton University Press, 1976.

DUNN CAVELTY, Myriam, **Cyber-Security and Threat Politics: US Efforts to Secure the Information Age**, New York, NY: Routledge. 2007

FAIZI, Nafis, and Yasir ALVI, "Regression and Multivariable Analysis", in **Biostatistics Manual for Health Research**, San Diego, CA: Academic Press, 2023, pp. 213–47.

FENG, Zhong-ping, **British Government's China Policy, 1945-1950**, Edinburgh: Edinburgh University Press, 1994.

FERDINAND, Peter, "UK Policy Towards China", in **Europe, China and the Two SARs: Towards a New Era**, edited by Miguel Santos NEVES and Brian BRIDGES, Palgrave Macmillan, 2000, pp. 29–62.

FLEMING, Brian P., **Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art**, Army Command and General Staff College, Fort Leavenworth, KS: School of Advanced Military Studies, 2011.

FISCHERKELLER, Michael P., Emily O. GOLDMAN and Richard J. HARKNETT, **Cyber Persistence Theory: Redefining National Security in Cyberspace**, Oxford: Oxford University Press, 2022.

FREIER, Nathan P., Charles R. BURNETT, William J. CAIN Jr., Christopher D. COMPTON, Sean M. HANKARD, Robert S. HUME, Gary R. KRAMLICH II, J. Matthew LISSNER, Tobin A. MAGSIG, and Daniel E. MOUTON, **Outplayed: Regaining Strategic Initiative in the Gray Zone, A Report Sponsored by the Army Capabilities Integration Center in Coordination with Joint Staff J-39/Strategic Multi-Layer Assessment Branch**, Carlisle, PA: US Army War College Press, 2016.

FRITZ, Mike, and Paul D. BERGER, "Will Anybody Buy? Logistic Regression", in **Improving the User Experience Through Practical Data Analytics**, Morgan Kaufmann, 2015, pp. 271–304.

GRAY, Colin S. Dr., **Categorical Confusion? The Strategic Implications of Recognizing Challenges Either as Irregular or Traditional**, US Army War College Press, 2012.

GEORGE, Alexander L., "Coercive Diplomacy: Definitions and Characteristics", in **The Limits of Coercive Diplomacy**, edited by Alexander L. GEORGE and William E. SIMONS, Second Edition, Boulder, San Francisco, Oxford: Westview Press, 1991, pp. 7–11.

GEORGE, Alexander L., **Forceful Persuasion: Coercive Diplomacy as an Alternative to War**, Washington, D.C.: Institute of Peace Press, 1991.

GORUNESCU, Florin, **Data Mining: Concepts, Models and Techniques, Intelligent Systems Reference Library,** Vol. 12, Berlin, Heidelberg: Springer Berlin Heidelberg, 2011.

HARRELL, Frank E., **Regression Modeling Strategies: With Applications to Linear Models, Logistic Regression, and Survival Analysis**, New York, NY: Springer, 2001.

HOFFMAN, Frank G., **Conflict in the 21st Century: The Rise of Hybrid Wars**, Arlington, VA: Potomac Institute for Policy Studies, 2007.

İNALCIK, Halil, **Âyânlar, Tanzimat, Meşrutiyet**, İstanbul: Türkiye İş Bankası Kültür Yayınları, 2016.

KAHN, Herman, **On Escalation: Metaphors and Scenarios**, New Brunswick, N.J.: Transaction Publishers, 2010.

LAWSON, Sean T., **Cybersecurity Discourse in the United States: Cyber-Doom Rhetoric and Beyond**, London; New York: Routledge, Taylor & Francis Group, 2021.

KELLO, Lucas, **The Virtual Weapon and International Order**, New Haven: Yale University Press, 2017.

KLIMBURG, Alexander**, The Darkening Web: The War for Cyberspace**, New York: Penguin Press, 2017.

LASCONJARIAS, Guillaume, and Jeffrey Arthur LARSEN (eds.), **NATO's Response to Hybrid Threats**, Rome: NATO Defense College, Research Division, 2015.

LIANG, Qiao, and Wang XIANGSUI, **Unrestricted Warfare**, Beijing: PLA Literature and Arts Publishing House, 1999.

LIBICKI, Martin C., **Cyberdeterrence and Cyberwar**, Santa Monica, CA: RAND Corporation, 2009.

LIBICKI, Martin C., **Brandishing Cyberattack Capabilities**, Santa Monica, CA: RAND Corporation, 2013.

LIEBERTHAL, Kenneth, and Peter W. SINGER, "**Cybersecurity and U.S.-China Relations**", Brookings, 2012.

LIU, Yanli, Yourong WANG, and Jian ZHANG, "New Machine Learning Algorithm: Random Forest", in **Information Computing and Applications**, edited by Baoxiang LIU, Maode MA, and Jincai CHANG, Vol. 7473, Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 246–52.

LONERGAN, Erica D., and Shawn W. LONERGAN, **Escalation Dynamics in Cyberspace**, New York, NY: Oxford University Press, 2023.

MARSH, Christopher, "The Grey Zone and Hybrid Conflict: A Conceptual Introduction", in **Hybrid Threats and Grey Zone Conflict: The Challenge to Liberal Democracies**, edited by Mitt REGAN and Aurel SARI, Oxford: Oxford University Press, 2024.

MAZARR, Michael J., **Mastering the Gray Zone: Understanding a Changing Era of Conflict**, US Army War College Press, 2015.

MEARSHEIMER, John J**., The Tragedy of Great Power Politics**, New York: Norton, 2001.

MERTLER, Craig A., **Introduction to Educational Research**, Third Edition, Los Angeles, California: SAGE Publications, Inc., 2021.

MITCHELL, Lincoln A., "Russia", in **The Color Revolutions**, University of Pennsylvania Press, 2012, pp. 92–114.

MOCKAITIS, Thomas R., **British Counterinsurgency in the Post-Imperial Era, War, Armed Forces, and Society**, Manchester: Manchester University Press, 1995.

MONTE, Matthew, **Network Attacks & Exploitation: A Framework,** Indianapolis, IN: John Wiley & Sons, Incorporated, 2015.

NAJŽER, Brin, **The Hybrid Age: International Security in the Era of Hybrid Warfare**, London; New York; Oxford; New Delhi; Sydney: I.B. Tauris, 2020.

RASCHKA, Sebastian, **Python Machine Learning**, Second Edition, Birmingham: Packt Publishing Ltd., 2015.

ROBIN, Ron T., **The Making of the Cold War Enemy: Culture and Politics in the Military-Intellectual Complex**, Princeton, NJ: Princeton University Press, 2003.

SANGER, David E., **Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power**, New York, NY: Crown, 2012.

SCHELLING, Thomas C., **Arms and Influence**, New Haven, Conn.: Yale University Press, 1966.

SCHMITT, Michael N. (ed.), **Tallinn Manual on the International Law Applicable to Cyber Warfare**, Cambridge: Cambridge University Press, 2013.

SCHMITT, Michael N. (ed.), **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, Second Edition, Cambridge: Cambridge University Press, 2017.

SERGEEV, Evgeny, **The Great Game, 1856 - 1907: Russo-British Relations in Central and East Asia**, Washington, DC: Woodrow Wilson Center Press, 2014.

SHARMA, Deepak Kumar, Mayukh CHATTERJEE, Gurmehak KAUR, and Suchitra VAVILALA, "Deep Learning Applications for Disease Diagnosis", in **Deep Learning for Medical Applications with Unique Data**, edited by Deepak GUPTA, Ashish KHANNA, Utku KOSE and Valentina Emilia BALAS, Academic Press, 2022, pp. 31–51.

SNYDER, Glenn Herald, and Paul DIESING, **Conflict Among Nations: Bargaining, Decision Making, and System Structure in International Crises**, Princeton: Princeton University Press, 1977.

SIEGEL, Andrew F., and Michael R. WAGNER, "Multiple Regression: Predicting One Variable from Several Others", in **Practical Business Statistics**, Eighth Edition, Academic Press, 2022, pp. 371–431.

TANRISEVER, Oktay, "Yöntem Sorunu: Geleneksekcilik-Davranışsalcılık Tartışması", in **Devlet, Sistem ve Kimlik Uluslararası İlişkilerde Temel Yaklaşımlar**, edited by Atilla Eralp, İstanbul: İletişim Yayınları, 2015.

VALERIANO, Brandon, and Benjamin JENSEN, "De-escalation Pathways and Disruptive Technology: Cyber Operations as Off-Ramps to War", in **Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace**, edited by Christopher ANKERSEN, Frederick DOUZET, and Scott J. SHACKELFORD, Cambridge: Cambridge University Press, 2022, pp. 64–93.

VALERIANO, Brandon, Benjamin M. JENSEN, and Ryan C. MANESS, **Cyber Strategy: The Evolving Character of Power and Coercion**, New York, NY: Oxford University Press, 2018.

WALTZ, Kenneth N., **Man, the State, and War: A Theoretical Analysis**, Anniversary Edition, New York: Columbia University Press, 2018.

WALTZ, Kenneth N., **Theory of International Politics**, New York: McGraw-Hill, 1979.

WAR, Geoffrey, "From 'Ally' to Enemy: Britain's Relations with the Soviet Union, 1941–8", in **The Soviet Union and Europe in the Cold War, 1943–53**, edited by Francesca GORI and Silvio PONS, London: Palgrave Macmillan UK, 1996, pp. 293–309.

Articles

AGRAFIOTIS, Ioannis, Jason R C NURSE, Michael GOLDSMITH, Sadie CREESE, and David UPTON, "A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate", **Journal of Cybersecurity**, Vol. 4, No. 1, 2018. https://doi.org/10.1093/cybsec/tyy006

AKGÜL, Fatih, "A Comparison between the Concepts of Gray Zone and Hybrid War: What Is New for International Security?", **Güvenlik Stratejileri Dergisi**, Vol. 17, No. 38, pp. 411–39. https://doi.org/10.17752/guvenlikstrtj.964066

AL-AMRI, Redhwan, Raja Kumar MURUGESAN, Mustafa MAN, Alaa Fareed ABDULATEEF, Mohammed A. AL-SHARAFI, and Ammar Ahmed ALKAHTANI, "A Review of Machine Learning and Deep Learning Techniques for Anomaly Detection in IoT Data", **Applied Sciences**, Vol. 11, No. 12, 2021. https://doi.org/10.3390/app11125320

ALKER, Hayward R., "The Long Road to International Relations Theory: Problems of Statistical Nonadditivity", **World Politics**, Vol. 18, No. 4, 1966, pp. 623–55. https://doi.org/10.2307/2009808

ALTMAN, Dan, "By Fait Accompli, Not Coercion: How States Wrest Territory from Their Adversaries", **International Studies Quarterly**, Vol. 61, No. 4, 2017, pp. 881–91. https://doi.org/10.1093/isq/sqx049

ARQUILLA, John, "Perils of the Gray Zone", **Prism**, Vol. 7, No. 3, 2018, pp. 118–29. https://www.jstor.org/stable/26470539

ARQUILLA, John and *David RONFELDT, "Cyberwar is Coming!"*, ***Comparative Strategy***, *Vol. 12, No. 2, 1993, pp. 141–165.*

AXELROD, Robert, and William D. HAMILTON, "The Evolution of Cooperation", Science, Vol. 211, No. 4489, 1981, pp. 1390–96. DOI: 10.1126/science.7466396

AZAD, Tahir Mahmood, Muhammad Waqas HAIDER, and Muhammad SADIQ, "Understanding Gray Zone Warfare from Multiple Perspectives", **World Affairs**, Vol. 186, No. 1, 2023, pp. 81–104. https://doi.org/10.1177/00438200221141101

BELO, Dani, and David CARMENT, "Grey-Zone Conflict: Implications for Conflict Management", **Canadian Global Affairs Institute**, 2019.

BLANK, Stephen, "Web War I: Is Europe's First Information War a New Kind of War?", **Comparative Strategy**, Vol. 27, No. 3, 2008, pp. 227–47. https://doi.org/10.1080/01495930802185312

BOLAT, Gökhan, "From Anglo-Persian Oil Company to British Petroleum: Britain's Oil Adventure in Iran", **History Studies International Journal of History**, Vol. 5, No. 2, 2013. https://doi.org/10.9737/historyS_846

BORGHARD, Erica D., and Shawn W. LONERGAN, "The Logic of Coercion in Cyberspace", **Security Studies**, Vol. 26, No. 3, 2017, pp. 452–81. https://doi.org/10.1080/09636412.2017.1306396

BORGHARD, Erica D., and Shawn W. LONERGAN, "Cyber Operations as Imperfect Tools of Escalation", **Strategic Studies Quarterly**, Vol. 13, No. 3, 2019, pp. 122–45.

BRANDS, Hal, "Paradoxes of the Gray Zone", **SSRN Scholarly Paper**, 2016. https://doi.org/10.2139/ssrn.2737593

BRENDON, Laura K., "Arpanet: An Efficient Machine as Social Discipline", **Science as Culture**, Vol. 10, No. 1, 2001, pp. 73–95. https://doi.org/10.1080/09505430020025500

BRESLIN, Shaun, "Beyond Diplomacy? UK Relations with China since 1997", **The British Journal of Politics and International Relations**, Vol. 6, No. 3, 2004, pp. 409–25. https://doi.org/10.1111/j.1467-856X.2004.00147.x

BUCHANAN, Ben, "Cyber Deterrence Isn't MAD; It's Mosaic", **Georgetown Journal of International Affairs**, 2014, pp. 130–40.

CALISKAN, Murat, and Paul Alexander CRAMERS, "What Do You Mean by 'Hybrid Warfare'? A Content Analysis on the Media Coverage of Hybrid Warfare Concept", **Horizon Insights**, Vol. 4, 2018, pp. 23–35.

CALISKAN, Murat, and Michel LIÉGEOIS, "The Concept of 'Hybrid Warfare' Undermines NATO's Strategic Thinking: Insights from Interviews with NATO Officials", **Small Wars & Insurgencies,** Vol. 32, No. 2, 2021, pp. 295–319. https://doi.org/10.1080/09592318.2020.1860374

CANTWELL, Douglas, "Hybrid Warfare: Aggression and Coercion in the Gray Zone", **American Society of International Law**, Vol. 21, No. 14, 2017.

CHARAP, Samuel, "The Ghost of Hybrid War", **Survival**, Vol. 57, No. 6, 2015, pp. 51–58. https://doi.org/10.1080/00396338.2015.1116147

CHEN, Rung-Ching, Christine DEWI, Su-Wen HUANG, and Rezzy Eko CARAKA, "Selecting Critical Features for Data Classification Based on Machine Learning Methods", **Journal of Big Data**, Vol. 7, No. 1, 2020, pp. 52. https://doi.org/10.1186/s40537-020-00327-4

CHIN, Warren, "Technology, War and the State: Past, Present and Future", **International Affairs**, Vol. 95, No. 4, 2019, pp. 765–83. https://doi.org/10.1093/ia/iiz106

COLLINS, Sean, and Stephen MCCOMBIE, "Stuxnet: The Emergence of a New Cyber Weapon and Its Implications", **Journal of Policing, Intelligence and Counter Terrorism**, Vol. 7, No. 1, 2012, pp. 80–91. https://doi.org/10.1080/18335330.2012.653198

DEUTSCH, Karl W., "The Place of Behavioral Sciences in Graduate Training in International Relations", **Behavioral Science**, Vol. 3, No. 1, 1958, pp. 278–84. https://doi.org/10.1002/bs.3830030123

DIXON, Paul, "'A Grand Strategic Error': The British Military Elite's Role in the Invasion of Iraq", **British Politics**, Vol. 19, No. 1, 2024, pp. 84–105. https://doi.org/10.1057/s41293-023-00250-1

DOWNS, George W., and David M. ROCKE, "Tacit Bargaining and Arms Control", **World Politics**, Vol. 39, No. 3, 1987, pp. 297–325. https://doi.org/10.2307/2010222

DUTTA, Vibekananda, Michał CHORAŚ, Marek PAWLICKI, and Rafał KOZIK, "A Deep Learning Ensemble for Network Anomaly and Cyber-Attack Detection", **Sensors**, Vol. 20, No. 16, 2020, pp. 4583. https://doi.org/10.3390/s20164583

EISEL, Reinhard, Britain's China Policy from 1949 to 2005: From an Idealistic Approach to Return to a Focus on the Economic Factor, **EU-China European Studies Centres Programme - CAP Working Paper**, 2007. http://www.cap.lmu.de/download/2007/2007_eu-china_eisel.pdf

ESHRAGHI, F., "Anglo-Soviet Occupation of Iran in August 1941", **Middle Eastern Studies**, Vol. 20, No. 1, 1984, pp. 27–52. https://doi.org/10.1080/00263208408700570

EVERA, Stephen, "Offense, Defense, and the Causes of War", **International Security**, Vol. 22, No. 4, 1998, pp. 5–43. https://doi.org/10.2307/2539239

FEARON, James D., "Rationalist Explanations for War", **International Organization**, Vol. 49, No. 3, 1995, pp. 379–414. https://doi.org/10.1017/S0020818300033324

FINNEMORE, Martha, and Kathryn SIKKINK, "International Norm Dynamics and Political Change", **International Organization**, Vol. 52, No. 4, 1998, pp. 887–917. https://doi.org/10.1162/002081898550789

FISCHERKELLER, Michael P., and Richard J. HARKNETT, "Deterrence Is Not a Credible Strategy for Cyberspace", **Orbis**, Vol. 61, No. 3, 2017, pp. 381–93. https://doi.org/10.1016/j.orbis.2017.05.003

FISCHERKELLER, Michael P., and Richard J. HARKNETT, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation", **The Cyber Defense Review**, 2019, pp. 267–87.

FORSYTH, James Wood, and Billy E. POPE, "Structural Causes and Cyber Effects: A Response to Our Critics", **Strategic Studies Quarterly**, Vol. 8, No. 4, 2014, pp. 112–28. https://www.jstor.org/stable/26270819

FREIER, Nathan, "The Defense Identity Crisis: It's a Hybrid World", **Parameters**, Vol. 39, No. 3, 2009. https://doi.org/10.55540/0031-1723.2483

GARTZKE, Erik, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth", **International Security**, Vol. 38, No. 2, 2013, pp. 41–73. https://doi.org/10.1162/ISEC_a_00136

GARTZKE, Erik, and Jon R. LINDSAY, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace**", Security Studies**, Vol. 24, No. 2, 2015, pp. 316–48. https://doi.org/10.1080/09636412.2015.1038188

GERASIMOV, Valery, "The Value of Science Is in the Foresight (Originally Published in Military-Industrial Kurier, 27 February 2013, Translated from Russian by Robert Coalson)", **US Army Military Review**, 2016, pp. 23–29.

GERNER, Deborah J., Philip A. SCHRODT, Ronald A. FRANCISCO, and Judith L. WEDDLE, "Machine Coding of Event Data Using Regional and International Sources", **International Studies Quarterly**, Vol. 38, No. 1, 1994, pp. 91–119. https://doi.org/10.2307/2600873

GLASER, Charles L., and Chaim KAUFMANN, "What Is the Offense-Defense Balance and Can We Measure It?", **International Security**, Vol. 22, No. 4, 1998, pp. 44–82. https://doi.org/10.2307/2539240

GLENN, Russell W., "Thoughts on Hybrid Conflict", **Small Wars Journal**, Vol. 2, No. 1, 2009, pp. 1–8.

GOCHMAN, Charles S., and Russell J. LENG, "Realpolitik and the Road to War: An Analysis of Attributes and Behavior", **International Studies Quarterly**, Vol. 27, No. 1, 1983, pp. 97–120. https://doi.org/10.2307/2600621

GOLDSTEIN, Joshua S., "A Conflict-Cooperation Scale for WEIS Events Data", The Journal of Conflict Resolution, Vol. 36, No. 2, 1992, pp. 369–85. https://doi.org/10.1177/0022002792036002007

GOODSON, Larry, and Marzena ŻAKOWSKA, "How Russia's Hybrid Warfare Is Changing", **Small Wars Journal**, 2023.

GORWA, Robert, and Max SMEETS, "Cyber Conflict in Political Science: A Review of Methods and Literature", **SocArXiv**, 2019. https://doi.org/10.31235/osf.io/fc6sg

GRAY, Christine, "The British Position in Regard to the Gulf Conflict", The International and Comparative Law Quarterly, Vol. 37, No. 2, 1988, pp. 420–28. https://doi:10.1093/iclqaj/37.2.447

GÜNEYLİOĞLU, Murat, "The Russia-Iran Alignment in the Middle East: The Main Dynamics and Limits of the Bilateral Security Cooperation", **Akdeniz İİBF Dergisi**, Vol. 23, No. 1, 2023, pp. 50–62. https://doi.org/10.25294/auiibfd.1170448

HALTERMAN, Andrew, Benjamin E. BAGOZZI, Andreas BEGER, Philip SCHRODT, and Grace SCRABOROUGH, "PLOVER and POLECAT: A New Political Event Ontology and Dataset", **SocArXiv**, 2023. https://doi.org/10.31235/osf.io/rm5dw

HALTERMAN, Andrew, Philip A. SCHRODT, Andreas BEGER, Benjamin E. BAGOZZI, and Grace I. SCARBOROUGH, "Creating Custom Event Data Without Dictionaries: A Bag-of-Tricks", **arXiv**, 2023. https://doi.org/10.48550/arXiv.2304.01331

HARKNETT, Richard J., and Max SMEETS, "Cyber Campaigns and Strategic Outcomes", **Journal of Strategic Studies**, Vol. 45, No. 4, 2022, pp. 534–67. https://doi.org/10.1080/01402390.2020.1732354

HAYES III, James E., "Beyond the Gray Zone: Special Operations in Multidomain Battle", **Joint Forces Quarterly**, Vol. 91, No. 91, 2018, pp. 60–66.

HEALEY, Jason, "The Implications of Persistent (and Permanent) Engagement in Cyberspace", **Journal of Cybersecurity**, Vol. 5, No. 1, 2019, p. tyz008. https://doi.org/10.1093/cybsec/tyz008

HEALEY, Jason, and Robert JERVIS, "The Escalation Inversion and Other Oddities of Situational Cyber Stability", **Texas National Security Review**, Vol. 3, No. 4, 2020, pp. 30–53. https://doi.org/10.26153/TSW/10962

HEMMERT, Giselmar A. J., Laura M. SCHONS, Jan WIESEKE, and Heiko SCHIMMELPFENNIG, "Log-Likelihood-Based Pseudo-R2 in Logistic Regression: Deriving Sample-Sensitive Benchmarks", **Sociological Methods & Research**, Vol. 47, No. 3, 2018, pp. 507–31. https://doi.org/10.1177/0049124116638107

HOFFMAN, Frank G., "Complex Irregular Warfare: The Next Revolution in Military Affairs", **Orbis**, Vol. 50, No. 3, 2006, pp. 395–411. https://doi.org/10.1016/j.orbis.2006.04.002

HOFFMAN, Frank G., "Hybrid vs. Compound War", **Armed Forces Journal**, 2009a.

HOFFMAN, Frank G., "Hybrid Warfare and Challenges", **Joint Forces Quarterly**, No. 52, 2009b, pp. 34–39.

HOFFMAN, Frank G., "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges", **Prism**, Vol. 7, No. 4, 2018, pp. 30–47. https://www.jstor.org/stable/26542705

HOROWITZ, Michael C., "Do Emerging Military Technologies Matter for International Politics?", **Annual Review of Political Science**, Vol. 23, No. 1, 2020, pp. 385–400. https://doi.org/10.1146/annurev-polisci-050718-032725

HU, Bo, Jun SHAO, and Mari PALTA, "Pseudo-R2 in Logistic Regression Model", **Statistica Sinica**, Vol. 16, 2006, pp. 847–60. https://www.jstor.org/stable/24307577

INSISA, Aurelio, "Hybrid after All: The 'Grey Zone', the 'Hybrid Warfare' Debate, and the PLA's Science of Military Strategy", **Defence Strategic Communications**, Vol. 12, June 2023, pp. 165–86. https://doi.org/10.30966/2018.RIGA.12.8

IOANNOU, Christiana, and Vasos VASSILIOU, "Network Attack Classification in IoT Using Support Vector Machines", **Journal of Sensor and Actuator Networks**, Vol. 10, No. 3, 2021, pp. 58. https://doi.org/10.3390/jsan10030058

ITOO, Fayaz, Meenakshi, and Satwinder SINGH, "Comparison and Analysis of Logistic Regression, Naïve Bayes and KNN Machine Learning Algorithms for Credit Card Fraud Detection", **International Journal of Information Technology**, Vol. 13, No. 4, 2021, pp. 1503–11. https://doi.org/10.1007/s41870-020-00430-y

JERVIS, Robert, "Cooperation Under the Security Dilemma", **World Politics**, Vol. 30, No. 2, 1978, pp. 167–214. https://doi.org/10.2307/2009958

JIN, Feng, "The Gray Zone Issue: Implications for US-China Relations", **Pacific Forum, Issues & Insights Working Paper**, Vol. 19, No. 14, 2019.

JOHNSON, Robert, "Hybrid War and Its Countermeasures: A Critique of the Literature", **Small Wars & Insurgencies**, Vol. 29, No. 1, 2018, pp. 141–63. https://doi.org/10.1080/09592318.2018.1404770

JOUBERT, Vincent, "Five Years after Estonia's Cyber Attacks: Lessons Learned for NATO?", **NATO Defense College**, No. 76, 2012. https://www.jstor.org/stable/resrep10366

KÄIHKÖ, Ilmari, "The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession", **Parameters**, Vol. 51, No. 3, 2021. https://doi.org/10.55540/0031-1723.3084

KAKACHIA, Kornely K., "Between Russian Assertiveness and Insecurity: Georgia's Political Challenges and Prospect after the Conflict", **Uluslararası İlişkiler Dergisi**, Vol. 7, No. 26, 2010, pp. 87–103.

KARIMIPOUR, Hadis, Ali DEHGHANTANHA, Reza M. PARIZI, Kim-Kwang Raymond CHOO, and Henry LEUNG, "A Deep and Scalable Unsupervised Machine Learning System for Cyber-Attack Detection in Large-Scale Smart Grids", **IEEE Access**, Vol. 7, 2019, pp. 80778–88. https://doi.org/10.1109/ACCESS.2019.2920326

KIRSCH, Cassandra M., "Science Fiction No More: Cyber Warfare and the United States", **Denver Journal of International Law & Policy**, Vol. 40, No. 4, 2012, pp. 620–47.

KNAPP, Kenneth J., and William R. BOULTON, "Cyber-Warfare Threatens Corporations: Expansion into Commercial Environments", **Information Systems Management**, Vol. 23, No. 2, 2006, pp. 76–87. https://doi.org/10.1201/1078.10580530/45925.23.2.20060301/92675.8

KOSTYUK, Nadiya, and Erik GARTZKE, "Fighting in Cyberspace: Internet Access and the Substitutability of Cyber and Military Operations", 2019. http://www-personal.umich.edu/~nadiya/CCO_KG_10042019.pdf

LASCONJARIAS, Guillaume, "Deterrence through Resilience: NATO, the Nations and the Challenges of Being Prepared", **NATO Eisenhower Paper**, No. 7, May 2017, pp. 1–6.

LEVY, Jack S., "Deterrence and Coercive Diplomacy: The Contributions of Alexander George", **Political Psychology**, Vol. 29, No. 4, 2008, pp. 537–52. https://doi.org/10.1111/j.1467-9221.2008.00648.x

LIBICKI, Martin C., "Cyberspace Is Not a Warfighting Domain", **I/S A Journal of Law and Policy for the Information Society**, Vol. 8, No. 2, 2012, pp. 321–36.

LIBISELLER, Chiara, "'Hybrid Warfare' as an Academic Fashion", **Journal of Strategic Studies**, Vol. 46, No. 4, 2023, pp. 858–80. https://doi.org/10.1080/01402390.2023.2177987

LIFF, Adam P., "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War", **Journal of Strategic Studies**, Vol. 35, No. 3, 2012, pp. 401–28. https://doi.org/10.1080/01402390.2012.663252

LIFF, Adam P., "The Proliferation of Cyberwarfare Capabilities and Interstate War, Redux: Liff Responds to Junio", **Journal of Strategic Studies**, Vol. 36, No. 1, 2013, pp. 134–38. https://doi.org/10.1080/01402390.2012.733312

LINDSAY, Jon R., "Stuxnet and the Limits of Cyber Warfare", **Security Studies**, Vol. 22, No. 3, 2013, pp. 365–404. https://doi.org/10.1080/09636412.2013.816122

LIU, Fei Tony, Kai Ming TING, and Zhi-Hua ZHOU, "Isolation-Based Anomaly Detection", **ACM Transactions on Knowledge Discovery from Data**, Vol. 6, No. 1, 2012, pp. 3:1–3:39. https://doi.org/10.1145/2133360.2133363

LOBANOV-ROSTOVSKY, A., "Anglo-Russian Relations through the Centuries", **The Russian Review**, Vol. 7, No. 2, 1948, pp. 41–52. https://doi.org/10.2307/125518

LONERGAN, Erica D., and Shawn W. LONERGAN, "Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises", **Security Studies**, Vol. 31, No. 1, 2022, pp. 32–64. https://doi.org/10.1080/09636412.2022.2040584

LUPOVICI, Amir, "The 'Attribution Problem' and the Social Construction of 'Violence': Taking Cyber Deterrence Literature a Step Forward**",** **International Studies Perspectives**, August 2014. https://doi.org/10.1111/insp.12082

LUPOVICI, Amir, "The Dog That Did Not Bark, the Dog That Did Bark, and the Dog That Should Have Barked: A Methodology for Cyber Deterrence Research", **International Studies Review**, Vol. 23, No. 4, 2021, pp. 1672–98. https://doi.org/10.1093/isr/viab032

LYNN-JONES, Sean M., "Offense-Defense Theory and Its Critics", **Security Studies**, Vol. 4, No. 4, 1995, pp. 660–91. https://doi.org/10.1080/09636419509347600

MANESS, Ryan C., and Brandon VALERIANO, "The Impact of Cyber Conflict on International Interactions", **Armed Forces & Society**, Vol. 42, No. 2, 2016, pp. 301–23. https://doi.org/10.1177/0095327X15572997

MARTINASEK, Z., V. ZEMAN, L. MALINA, and J. MARTINASEK, "K-Nearest Neighbors Algorithm in Profiling Power Analysis Attacks", **Radioengineering**, Vol. 25, No. 2, 2016, pp. 365–82. https://doi.org/10.13164/re.2016.0365

MASCHMEYER, Lennart, "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations", **International Security**, Vol.46, No.2, 2021a, pp. 51–90. https://doi.org/10.1162/isec_a_00418

MASCHMEYER, Lennart, "A New and Better Quiet Option? Strategies of Subversion and Cyber Conflict", **Journal of Strategic Studies**, Vol. 46, No. 3, 2023a, pp. 570–94. https://doi.org/10.1080/01402390.2022.2104253

MASCHMEYER, Lennart, "Subversion, Cyber Operations, and Reverse Structural Power in World Politics", **European Journal of International Relations**, Vol. 29, No. 1, 2023b, pp. 79–103. https://doi.org/10.1177/13540661221117051

MASCHMEYER, Lennart, and Myriam Dunn CAVELTY, "Goodbye Cyberwar: Ukraine as Reality Check", **CSS Policy Perspectives**, Vol. 10, No. 3, 2022

MASCHMEYER, Lennart, Ronald J. DEIBERT, and Jon R. LINDSAY, "A Tale of Two Cybers - How Threat Reporting by Cybersecurity Firms Systematically Underrepresents Threats to Civil Society", **Journal of Information Technology & Politics**, Vol. 18, No. 1, 2021, pp. 1–20. https://doi.org/10.1080/19331681.2020.1776658

MATISEK, Jahara W., "Shades of Gray Deterrence: Issues of Fighting in the Gray Zone", Journal of Strategic Security, Vol. 10, No. 3, 2017, pp. 1–26. http://doi.org/10.5038/1944-0472.10.3.1589

MATTIS, James N., and Frank HOFFMAN, "Future Warfare: The Rise of Hybrid Wars", **United States Naval Institute Proceedings**, Vol. 131, No. 11, 2005. https://www.proquest.com/trade-journals/future-warfare-rise-hybrid-wars/docview/205977465/se-2?accountid=15955

MAZANEC, Brian M., "Why International Order in Cyberspace Is Not Inevitable", **Strategic Studies Quarterly**, Vol. 9, No. 2, 2015, pp. 78–98. http://www.jstor.org/stable/26271076

MAZANEC, Brian M., "Constraining Norms for Cyber Warfare Are Unlikely", **Georgetown Journal of International Affairs**, Vol. 17, No. 3, 2016, pp. 100–109.

MCCUEN, John J., "Hybrid Warfare", **Military Review**, 2008, pp. 107–13.

MCGRAW, Gary, "Cyber War Is Inevitable (Unless We Build Security In)", **Journal of Strategic Studies**, Vol. 36, No. 1, 2013, pp. 109–19. https://doi.org/10.1080/01402390.2012.742013

MUMFORD, Andrew, and Pascal CARLUCCI, "Hybrid Warfare: The Continuation of Ambiguity by Other Means", **European Journal of International Security**, Vol. 8, No. 2, 2023, pp. 192–206. https://doi.org/10.1017/eis.2022.19

MURADOV, Ibrahim, "The Russian Hybrid Warfare: The Cases of Ukraine and Georgia", **Defence Studies**, Vol. 22, No. 2, 2022, pp. 168–91. https://doi.org/10.1080/14702436.2022.2030714

NAHM, Francis Sahngun, "What the P Values Really Tell Us", **The Korean Journal of Pain**, Vol. 30, No. 4, 2017, pp. 241–42. https://doi.org/10.3344/kjp.2017.30.4.241

NATEKIN, Alexey, and Alois KNOLL, "Gradient Boosting Machines, a Tutorial**",** **Frontiers in Neurorobotics**, Vol. 7, 2013. https://doi.org/10.3389/fnbot.2013.00021

NAWIR, Mukrimah, Amiza AMIR, Ong Bi LYNN, Naimah YAAKOB, and R. Badlishah AHMAD, "Performances of Machine Learning Algorithms for Binary Classification of Network Anomaly Detection System", **Journal of Physics: Conference Series**, Vol. 1018, 2018. https://doi.org/10.1088/1742-6596/1018/1/012015

NILSSON, Niklas, "Between Russia's 'Hybrid' Strategy and Western Ambiguity: Assessing Georgia's Vulnerabilities", **The Journal of Slavic Military Studies**, Vol. 34, No. 1, 2021, pp. 50–68. https://doi.org/10.1080/13518046.2021.1923992

NORRIS, Clayton, Philip SCHRODT, and John BEIELER, "PETRARCH2: Another Event Coding Program", **Journal of Open Source Software**, Vol. 2, No. 9, 2017, p. 133. https://doi.org/10.21105/joss.00133

NYE, Joseph S., "Deterrence and Dissuasion in Cyberspace", **International Security**, Vol. 41, No. 3, 2017, pp. 44–71. https://doi.org/10.1162/ISEC_a_00266

ÖZLÜK, Erdem, "Gelenekselcilik-Davranışsalcılık Tartışmasını Bağlamında Anlamak", **Ankara Üniversitesi SBF Dergisi**, Vol. 64, No. 3, 2009, pp. 197–220. https://doi.org/10.1501/SBFder_0000002118

PATALANO, Alessio, "When Strategy Is 'Hybrid' and Not 'Grey': Reviewing Chinese Military and Constabulary Coercion at Sea", **The Pacific Review**, Vol. 31, No. 6, 2018, pp. 811–39. https://doi.org/10.1080/09512748.2018.1513546

PEDREGOSA, Fabian, Gaël VAROQUAUX, Alexandre GRAMFORT, Vincent MICHEL, Bertrand THIRION, Olivier GRISEL, Mathieu BLONDEL, et al., "Scikit-Learn: Machine Learning in Python", **The Journal of Machine Learning Research**, Vol. 12, 2012, pp. 2825-2830. https://doi.org/10.48550/ARXIV.1201.0490

POWELL, Robert, "Bargaining Theory and International Conflict", **Annual Review of Political Science**, Vol. 5, No. 1, 2002, pp. 1–30. https://doi.org/10.1146/annurev.polisci.5.092601.141138

REISINGER, Heidi, and Aleksandr GOLTS, "Russia's Hybrid Warfare - Waging War below the Radar of Traditional Collective Defence", **NATO Defense College**, No. 105, 2014.

RENZ, Bettina, "Russia and 'Hybrid Warfare'", **Contemporary Politics**, Vol. 22, No. 3, 2016, pp. 283–300. https://doi.org/10.1080/13569775.2016.1201316

RID, Thomas, "Cyber War Will Not Take Place", **Journal of Strategic Studies**, Vol. 35, No. 1, 2012, pp. 5–32. https://doi.org/10.1080/01402390.2011.608939

RID, Thomas, and Ben BUCHANAN, "Attributing Cyber Attacks", **Journal of Strategic Studies**, Vol. 38, No. 1–2, 2015, pp. 4–37. https://doi.org/10.1080/01402390.2014.977382

SALTZMAN, Ilai, "Cyber Posturing and the Offense-Defense Balance", **Contemporary Security Policy**, Vol. 34, No. 1, 2013, pp. 40–63. https://doi.org/10.1080/13523260.2013.771031

SAMONAS, Spyridon, and David COSS, "The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security", **Journal of Information Systems Security**, Vol. 10, No. 3, 2014, pp. 21–45.

SARKER, Iqbal H., "Machine Learning: Algorithms, Real-World Applications and Research Directions", **SN Computer Science**, Vol. 2, No. 3, 2021, pp. 160. https://doi.org/10.1007/s42979-021-00592-x

ŞATANA, Nil S., "Uluslararası İlişkilerde Bilimsellik, Metodoloji ve Yöntem", **Uluslararası İlişkiler Dergisi,** Vol. 12, No. 46, 2015, pp. 10–33. https://doi.org/10.33458/uidergisi.463026

SCHELLING, T. C., "Reciprocal Measures for Arms Stabilization", **Daedalus**, Vol. 89, No. 4, 1960, pp. 892–914. https://doi.org/10.1162/001152605774431455

SCHELLING, Thomas C., "Bargaining, Communication, and Limited War", **Negotiation and Conflict Management Research**, Vol. 1, No. 2, 2008, pp. 198–217. https://doi.org/10.1111/j.1750-4716.2008.00012.x

SCHRODT, Philip A., Shannon G. DAVIS, and Judith L. WEDDLE, "Political Science: KEDS—A Program for the Machine Coding of Event Data", **Social Science Computer Review**, Vol. 12, No. 4, 1994, pp. 561–87. https://doi.org/10.1177/089443939401200408

SCHRODT, Philip, and Jay YONAMINE, "A Guide to Event Data: Past, Present, and Future", **All Azimuth: A Journal of Foreign Policy and Peace**, Vol. 2, No. 2, 2016, pp. 5–22. https://doi.org/10.20991/allazimuth.167312

SCHROEDER, Paul W., "Did the Vienna Settlement Rest on a Balance of Power?", **The American Historical Review**, Vol. 97, No. 3, 1992, pp. 683–706. https://doi.org/10.2307/2164774

SCHWELLER, Randall L., "Bandwagoning for Profit: Bringing the Revisionist State Back In", **International Security**, Vol. 19, No. 1, 1994, pp. 72–107. https://doi.org/10.1162/isec.19.1.72

SHAKARIAN, Paulo, "Stuxnet: Cyberwar Revolution in Military Affairs", **Small Wars Journal**, 2011.

SHANDLER, Ryan, and Miguel Alberto GOMEZ, "The Hidden Threat of Cyber-Attacks – Undermining Public Confidence in Government", **Journal of Information Technology & Politics**, 2022, pp. 1–16. https://doi.org/10.1080/19331681.2022.2112796

SHIEH, Chin-Shiuh, Wan-Wei LIN, Thanh-Tuan NGUYEN, Chi-Hong CHEN, Mong-Fong HORNG, and Denis MIU, "Detection of Unknown DDoS Attacks with Deep Learning and Gaussian Mixture Model", **Applied Sciences**, Vol. 11, No. 11, 5213, 2021, https://doi.org/10.3390/app11115213

SINAGA, Kristina P., and Miin-Shen YANG, "Unsupervised K-Means Clustering Algorithm", **IEEE Access**, Vol. 8, 2020, pp. 80716–27. https://doi.org/10.1109/ACCESS.2020.2988796

SINGER, J. David, "The 'Correlates of War' Project: Interim Report and Rationale", **World Politics**, Vol. 24, No. 2, 1972, pp. 243–70. https://doi.org/10.2307/2009738

SINGH, Abhishek Kumar, Amit KUMAR, Biswajit RAHA, and Bibhas Kumar SHAHEE, "Detect And Assess the Cybersecurity Threats With Their Mitigation Approaches Using ML Algorithms", **International Journal of Novel Research and Development**, Vol. 8, No. 5, 2023, pp. 134–38.

SLAYTON, Rebecca, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment", **International Security**, Vol. 41, No. 3, 2017, pp. 72–109. https://doi.org/10.1162/ISEC_a_00267

SMEETS, Max, "The Strategic Promise of Offensive Cyber Operations", **Strategic Studies Quarterly**, Vol. 12, No. 3, 2018, pp. 90–113. http://www.jstor.org/stable/26481911

SOLMAZ, Tarik, "'Hybrid Warfare': A Dramatic Example of Conceptual Stretching**", National Security and the Future**, Vol. 23, No. 1, 2022a, pp. 89–102. https://doi.org/10.37458/nstf.23.1.5

SOLMAZ, Tarik, "Hybrid Warfare: One Term, Many Meanings**", Small Wars Journal**, 2022b.

STEVENS, Tim, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace", **Contemporary Security Policy**, Vol. 33, No. 1, 2012, pp. 148–70. https://doi.org/10.1080/13523260.2012.659597

STOKER, Donald, and Craig WHITESIDE, "Gray-Zone Conflict and Hybrid War-Two Failures of American Strategic Thinking", **Naval War College Review**, Vol. 73, No. 1, 2020, pp. 19–54.

TADDEO, Mariarosaria, "Deterrence and Norms to Foster Stability in Cyberspace", **Philosophy & Technology**, Vol. 31, No. 3, 2018a, pp. 323–29. https://doi.org/10.1007/s13347-018-0328-0

TADDEO, Mariarosaria, "The Limits of Deterrence Theory in Cyberspace", **Philosophy & Technology,** Vol. 31, No. 3, 2018b, pp. 339–55. https://doi.org/10.1007/s13347-017-0290-2

TADDEO, Mariarosaria, and Luciano FLORIDI, "Regulate Artificial Intelligence to Avert Cyber Arms Race", **Nature**, Vol. 556, No. 7701, 2018, pp. 296–98. https://doi.org/10.1038/d41586-018-04602-6

TOR, Uri, "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence", **Journal of Strategic Studies**, Vol. 40, No. 1–2, 2017, pp. 92–117. https://doi.org/10.1080/01402390.2015.1115975

TÜR, Özlem, and Nuri SALIK, "Uluslararası İlişkilerde 'Küçük Devletler': Gelişimi, Tanımı, Dış Politika ve İttifak Davranışları", **Uluslararası İlişkiler Dergisi**, Vol. 14, No. 53, 2017, pp. 3–22. https://doi.org/10.33458/uidergisi.513054

VALERIANO, Brandon, and Ben JENSON, "The Myth of the Cyber Offense: The Case for Cyber Restraint", **Cato Institute Policy Analysis**, No. 862, 2019a. https://ssrn.com/abstract=3382340

VALERIANO, Brandon, and Ryan C. MANESS, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11", **Journal of Peace Research**, Vol. 51, No. 3, 2014, pp. 347–60. https://doi.org/10.1177/0022343313518940

VANEM, Erik, and Andreas BRANDSAETER, "Unsupervised Anomaly Detection Based on Clustering Methods and Sensor Data on a Marine Diesel Engine", **Journal of Marine Engineering & Technology**, Vol. 20, No. 4, 2021, pp. 217–34. https://doi.org/10.1080/20464177.2019.1633223

WALT, Stephen M., "Alliance Formation and the Balance of World Power", **International Security**, Vol. 9, No. 4, 1985, pp. 3–43. https://doi.org/10.2307/2538540

WIRTZ, James J., "Life in the 'Gray Zone': Observations for Contemporary Strategists", **Defense & Security Analysis**, Vol. 33, No. 2, 2017, pp. 106–14. https://doi.org/10.1080/14751798.2017.1310702

WITHER, James K., "Hybrid Warfare Revisited: A Battle of 'Buzzwords'", **Connections: The Quarterly Journal**, Vol. 1, 2023, pp. 7–27. https://doi.org/10.11610/Connections.22.1.02

YEŞİLBURSA, Behçet K., “CENTO: The Forgotten Alliance in the Middle East (1959-1979)”, **Middle Eastern Studies,** Vol. 56, No. 6, 2020, pp. 854–77. https://doi.org/10.1080/00263206.2020.1755841

YODER, Brandon K., “Can Cyberattacks Reassure? Half Measures as a De-Escalation Strategy”, **Security Studies**, Vol. 31, No. 4, 2022, pp. 757–63. https://doi.org/10.1080/09636412.2022.2140600

Electronic Sources

AFARY, Janet, Khosrow MOSTOFI, and Peter William AVERY, "Rise of Reza Khan", *Encyclopaedia Britannica*, 2024, Retrieved from: https://www.britannica.com/place/Iran/Rise-of-Reza-Khan (Accessed 20 May 2024).

ALLAN, Duncan, "Managed Confrontation UK Policy Towards Russia After the Salisbury Attack", *Chatham House*, 2018, Retrieved from: https://www.chathamhouse.org/sites/default/files/publications/research/2018-10-30-managed-confrontation-uk-russia-salisbury-allan-final.pdf (Accessed 14 May 2024).

ALLAN, Duncan, and Ian BOND, "A New Russia Policy for Post-Brexit Britain: The UK Must Abandon Its Delusions to Deal Effectively with Russia", *Chatham House*, 2022, Retrieved from: https://www.chathamhouse.org/sites/default/files/2022-01/2022-01-27-russia-policy-post-brexit-britain-allan-bond.pdf (Accessed 30 April 2024).

ARAYA, Daniel, "Huawei’s 5G Dominance In The Post-American World", *Forbes*, 2019, Retrieved from: https://www.forbes.com/sites/danielaraya/2019/04/05/huaweis-5g-dominance-in-the-post-american-world/ (Accessed 19 May 2024).

AZEEM, Atheeb, "9 Effective Ways to Overcome The Fear of The Unknown", *Medium*, 27 June 2022, Retrieved from: https://medium.com/@byatheebazeem/9-effective-ways-to-overcomethe-fear-of-the-unknown-97ce02330437 (Accessed 20 September 2023).

BACHEGA, Hugo, and James GREGORY, "Massive Drone Attack on Black Sea Fleet - Russia", *BBC News*, 29 October 2022, Retrieved from: https://www.bbc.com/news/world-europe-63437212 (Accessed 16 May 2024).

BADSHAH, Nadeem, "Chinese Embassy Calls Liz Truss’s Trip to Taiwan a 'Dangerous Political Stunt'", *The Guardian*, 16 May 2023, Retrieved from: https://www.theguardian.com/world/2023/may/16/china-brands-liz-trusss-trip-to-taiwan-a-dangerous-political-stunt (Accessed 10 May 2024).

BAJAJ, Vardaan, "Unsupervised Learning For Anomaly Detection", *Medium*, 2020, Retrieved from: https://towardsdatascience.com/unsupervised-learning-for-anomaly-detection-44c55a96b8c1 (Accessed 29 November 2023).

BAKER, Kurt, "What Is Cyber Espionage", *CrowdStrike*, 2023, Retrieved from: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/ (Accessed 30 November 2023).

BARAN, Paul, "On Distributed Communications Networks", *RAND Corporation*, 1 September 1962, Retrieved from: https://www.rand.org/pubs/papers/P2626.html (Accessed 26 October 2023).

BARNES, Julian E., "Allied Spy Chiefs Warn of Chinese Espionage Targeting Tech Firms", *The New York Times*, 18 October 2023, Retrieved from: https://www.nytimes.com/2023/10/18/us/politics/china-spying-technology.html (Accessed 14 November 2023).

BARNO, David, and Nora BENSHAHAL, "A New Generation of Unrestricted Warfare", *War on the Rocks*, 2016, Retrieved from: https://warontherocks.com/2016/04/a-new-generation-of-unrestricted-warfare/ (Accessed 21 September 2023).

BERG, Raffi, Tom SPENDER, and Jonathan BEALE, "Why Have Israel and Iran Attacked Each Other?", *BBC News*, 19 April 2024, Retrieved from: https://www.bbc.com/news/world-middle-east-68811276 (Accessed 11 May 2024).

BERGMAN, Ronen, and David M. HALBFINGER, "Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks", *The New York Times*, 20 May 2020, Retrieved from: https://www.nytimes.com/2020/05/19/world/middleeast/israel-iran-cyberattacks.html (Accessed 3 October 2023).

BERMAN, Lazar, "After Cutting Ties with Iran, Albanian PM Arrives in Israel to Talk Cybersecurity", *The Times of Israel*, 2022, Retrieved from: https://www.timesofisrael.com/after-cutting-ties-with-iran-albanian-pm-arrives-in-israel-to-talk-cybersecurity/ (Accessed 16 October 2023).

BERMAN, Noah, "Two Years of War in Ukraine: Are Sanctions Against Russia Making a Difference?", *Council on Foreign Relations*, 2024, Retrieved from: https://www.cfr.org/in-brief/two-years-war-ukraine-are-sanctions-against-russia-making-difference (Accessed 15 May 2024).

BIELIESKOV, Mykola, "The Russian and Ukrainian Spring 2021 War Scare", *CSIS Understanding the Russian Military Today, Center for Strategic & International Studies*, 21 September 2021, Retrieved from: https://www.csis.org/analysis/russian-and-ukrainian-spring-2021-war-scare (Accessed 6 May 2024).

BILAL, Arsalan, "Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote", *NATO Review*, 2021, Retrieved from: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html (Accessed 24 January 2024).

BIRTLES, Bill, "Xi Announces Plans to Allow Chinese Military to Undertake 'Armed Forces Operations' Abroad", *ABC News*, 14 June 2022, Retrieved from: https://www.abc.net.au/news/2022-06-14/xi-jinping-expands-china-military-influence-abroad/101152154 (Accessed 10 May 2024).

BLACKALL, Molly, "Rushdie Attack Leads to Calls to Re-Evaluate US and UK Relations with Iran", *INEWS*, 2022, Retrieved from: https://inews.co.uk/news/world/salman-rushdie-attack-us-uk-iran-relations-sanctions-iran-1794769 (Accessed 20 May 2024).

BLAIR, David, "Gordon Brown Warns Iran in Address to Israeli Parliament", *The Telegraph*, 2008, Retrieved from: https://www.telegraph.co.uk/news/worldnews/middleeast/iran/2438647/Gordon-Brown-warns-Iran-in-address-to-Israeli-parliament.html (Accessed 25 May 2024).

BOND, Ian, "Russia's War in Ukraine: Is Minsk the End, or Just the Start?", *Centre for European Reform*, 2015, Retrieved from: https://www.cer.eu/insights/russias-war-ukraine-minsk-end-or-just-start (Accessed 6 May 2024).

BORGER, Julian, and Martin CHULOV, "US Kills Iran General Qassem Suleimani in Strike Ordered by Trump", *The Guardian*, 3 January 2020, Retrieved from: https://www.theguardian.com/world/2020/jan/03/baghdad-airport-iraq-attack-deaths-iran-us-tensions (Accessed 21 May 2024).

BOWLER, Tim, "Huawei: Why Is It Being Banned from the UK's 5G Network?", *BBC News*, 14 July 2020, Retrieved from: https://www.bbc.com/news/newsbeat-47041341 (Accessed 19 May 2024).

BOYLE, Martin, "Why Did Liz Truss Visit Taiwan?", *The Diplomat*, May 2023, Retrieved from: https://thediplomat.com/2023/05/why-did-liz-truss-visit-taiwan/ (Accessed 10 May 2024).

BOZORGMEHR, Najmeh, "Iran Nuclear Chief Announces Enrichment Programme Expansion", *Financial Times*, 2022, Retrieved from: https://www.ft.com/content/8cfc9214-e835-4c58-beeb-4af3d38df276 (Accessed 10 May 2024).

BRENNAN, Margaret, Camilla SCHICK, and Tucker REALS, "Ukraine Hit with Cyberattack, a Tactic It 'Expected' to Precede a 'Full Invasion' by Russia", *CBS News*, 2022, Retrieved from: https://www.cbsnews.com/news/ukraine-cyber-attack-russia-us-nato-donbas-war-amabssador-markarova/ (Accessed 24 September 2023).

BROWN, Larisa, "Russian Ambassador's Chilling Warning", *Mail Online*, 2020, Retrieved from: https://www.dailymail.co.uk/news/article-8593329/Putins-man-London-says-mud-slinging-means-relationship-Moscow-close-frozen.html (Accessed 30 April 2024).

BRUNSON, Jonathan, "Implementing the Minsk Agreements Might Drive Ukraine to Civil War. That's Been Russia's Plan All Along", *War on the Rocks*, 2019, Retrieved from: https://warontherocks.com/2019/02/implementing-the-minsk-agreements-might-drive-ukraine-to-civil-war-thats-been-russias-plan-all-along/ (Accessed 6 May 2024).

BUMILLER, Elisabeth, and Thom SHANKER, "Panetta Warns of Dire Threat of Cyberattack on U.S.", *The New York Times*, 12 October 2012, Retrieved from: https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html (Accessed 19 September 2023).

BURGERS, Tobias, and Scott ROMANIUK, "Is China Done With Salami Slicing?", *The Diplomat*, 2021, Retrieved from: https://thediplomat.com/2021/04/is-china-done-with-salami-slicing/ (Accessed 12 February 2024).

BURGESS, Matt, "A Hacking Spree Against Iran Spills Out Into the Physical World", *Wired*, 30 November 2021, Retrieved from: https://www.wired.co.uk/article/iran-israel-hacking-infrastructure (Accessed 3 October 2023).

BUTCHARD, Patrick, "Ukraine Crisis: Recognition, Military Action, and International Law", *Research Briefing, United Kingdom House of Commons*, 24 March 2022, Retrieved from: https://commonslibrary.parliament.uk/research-briefings/cbp-9470/ (Accessed 6 May 2024).

BYMAN, Daniel, and Kennath M. POLLACK, "The Persian-Russian Connection", *Lawfare*, 2023, Retrieved from: https://www.lawfaremedia.org/article/the-persian-russian-connection (Accessed 11 May 2024).

CAFIEROV, Nazim, "Rusya'nın Ukrayna'ya Askeri Müdahalesine Nasıl Gelindi?-Nazim Caferov (Cafersoy)", *Panorama*, 2022, Retrieved from: https://www.uikpanorama.com/blog/2022/03/29/rusya-askeri-mudahale/ (Accessed 31 October 2023).

CAFIFERO, Giorgio, "Iran's Stakes in the Hamas-Israel Conflict", *Carnegie Endowment for International Peace*, 2023, Retrieved from: https://carnegieendowment.org/sada/2023/10/irans-stakes-in-the-hamas-israel-conflict?lang=en (Accessed 21 May 2024).

CATTLER, David, and Daniel BLACK, "The Myth of the Missing Cyberwar", *Foreign Affairs*, 6 April 2022, Retrieved from: https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar (Accessed 15 September 2023).

CHAPPELL, Bill, "Russia Holds a Massive Military Exercise with Belarus, Raising Concerns in Ukraine", *NPR*, 10 February 2022, Retrieved from: https://www.npr.org/2022/02/10/1079888622/russia-military-exercise-belarus-ukraine (Accessed 7 May 2024).

CHESHIRE, Tom, "China Accuses British Navy of 'Evil Intentions' as UK Warship Sails through Taiwan Strait", *Sky News*, 2021, Retrieved from: https://news.sky.com/story/china-accuses-british-navy-of-evil-intentions-as-uk-warship-sails-through-taiwan-strait-12419546 (Accessed 10 May 2024).

CHEUNG, Helier, and Roland HUGHES, "Why Are There Protests in Hong Kong? All the Context You Need", *BBC News*, 21 May 2020, Retrieved from: https://www.bbc.com/news/world-asia-china-48607723 (Accessed 17 May 2024).

CHRISTIE, Edward Hunter, "Artificial Intelligence at NATO: Dynamic Adoption, Responsible Use", *NATO Review*, 2020, Retrieved from: https://www.nato.int/docu/review/articles/2020/11/24/artificial-intelligence-at-nato-dynamic-adoption-responsible-use/index.html (Accessed 5 January 2024).

COATES, Sam, "China Hacked Ministry of Defence, Sky News Learns", *Sky News*, 2024, Retrieved from: https://news.sky.com/story/china-hacked-ministry-of-defence-sky-news-learns-13130757 (Accessed 10 May 2024).

COBAIN, Ian, Matthew TAYLOR, and Luke HARDING, "I Am Plotting a New Russian Revolution", *The Guardian*, 13 April 2007, Retrieved from: https://www.theguardian.com/world/2007/apr/13/topstories3.russia (Accessed 14 May 2024).

CONVERSATIONS with History: Kenneth Waltz, dir. by *University of California Television (UCTV)*, 2008, Retrieved from: https://www.youtube.com/watch?v=F9eV5gPlPZg (Accessed 15 September 2023).

CORDESMAN, Anthony H., and Grace HWANG, *Chronology of Possible Chinese Gray Area and Hybrid Warfare Operations*, *Center for Strategic and International Studies (CSIS)*, 2020, Retrieved from: https://www.jstor.org/stable/resrep25228 (Accessed 16 February 2024).

COURTNEY, William, and Peter A. WILSON, "If Russia Invaded Ukraine", *RAND Corporation*, 2021, Retrieved from: https://www.rand.org/blog/2021/12/expect-shock-and-awe-if-russia-invades-ukraine.html (Accessed 24 September 2023).

DANCHEV, Dancho, "Coordinated Russia vs Georgia Cyber Attack in Progress", *ZDNET*, 2008a, Retrieved from: https://www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/ (Accessed 22 September 2023).

DANCHEV, Dancho, "Georgia President's Web Site under DDoS Attack from Russian Hackers", *ZDNET*, 2008b, Retrieved from: https://www.zdnet.com/article/georgia-presidents-web-site-under-ddos-attack-from-russian-hackers/ (Accessed 28 October 2023).

DAVAR, Faramarz, "Remembering Seven Decades of the Queen's Encounters with Iran", *IranWire*, 2022, Retrieved from:

https://iranwire.com/en/politics/107377-remembering-seven-decades-of-the-queens-encounters-with-iran/ (Accessed 3 June 2024).

DAVIDSON, Helen, "China-Taiwan Relations: What's behind the Tensions – in 30 Seconds", *The Guardian*, 3 August 2022, Retrieved from: https://www.theguardian.com/world/2022/aug/01/china-and-taiwan-whats-behind-the-tensions-in-30-seconds (Accessed 10 May 2024).

DAVIS, Joshua, "Hackers Take Down the Most Wired Country in Europe", *Wired*, 21 August 2007, Retrieved from: https://www.wired.com/2007/08/ff-estonia/ (Accessed 28 October 2023).

DEHGHAN, Saeed Kamali, "Iran's Parliament Votes to Expel British Ambassador", *The Guardian*, 27 November 2011, Retrieved from: https://www.theguardian.com/world/2011/nov/27/iran-votes-expel-british-ambassador (Accessed 21 May 2024).

DERIAN, James Der, "Cyber-Deterrence", *Wired*, 1994, Retrieved from: https://www.wired.com/1994/09/cyber-deter/ (Accessed 9 November 2023).

DICKINSON, Peter, "How Ukraine's Orange Revolution Shaped Twenty-First Century Geopolitics", *Atlantic Council*, 2020, Retrieved from: https://www.atlanticcouncil.org/blogs/ukrainealert/how-ukraines-orange-revolution-shaped-twenty-first-century-geopolitics/ (Accessed 14 May 2024).

DICKINSON, Peter, "The 2008 Russo-Georgian War: Putin's Green Light", *Atlantic Council*, 2021, Retrieved from: https://www.atlanticcouncil.org/blogs/ukrainealert/the-2008-russo-georgian-war-putins-green-light/ (Accessed 22 September 2023).

DONALDSON, Kitty, and Joe MAYES, "No 'Business As Usual' With China After Covid-19, U.K. Says", *Bloomberg*, 16 April 2020, Retrieved from: https://www.bloomberg.com/news/articles/2020-04-16/no-business-as-usual-with-china-after-coronavirus-u-k-says (Accessed 9 May 2024).

EL-GHOBASHY, Tamer, Michael BIRNBAUM, and Carol MORELLO, "Iran Announces It Will Stop Complying with Parts of Landmark Nuclear Deal", *Washington Post*, 9 May 2019, Retrieved from: https://www.washingtonpost.com/world/iran-to-take-steps-to-reduce-its-commitment-to-landmark-nuclear-deal/2019/05/07/90cc3b1c-70fe-11e9-9331-30bc5836f48e_story.html (Accessed 21 May 2024).

ELEZI, Elona, "Albania Blames Iran for Cyberattacks", *Deutsche Welle*, 2022, Retrieved from: https://www.dw.com/en/albania-once-again-the-target-of-cyberattacks-after-cutting-diplomatic-ties-with-iran-and-expelling-diplomats/a-63146285 (Accessed 16 October 2023).

ELKUS, Adam, "50 Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense", *War on the Rocks*, 2015, Retrieved from: https://warontherocks.com/2015/12/50-shades-of-gray-why-the-gray-wars-concept-lacks-strategic-sense/ (Accessed 23 January 2024).

ENGSTRÖM, Mattias, "Hybrid Warfare and the Effects From Hybrid Threats on Cyber Security", *Truesec*, 2022, Retrieved from: https://www.truesec.com/hub/blog/hybrid-warfare-and-cyber-security (Accessed 5 January 2024).

ERLANGER, Steven, "Iran and U.S. Agree on Path Back to Nuclear Deal", *The New York Times*, 6 April 2021, Retrieved from: https://www.nytimes.com/2021/04/06/world/europe/iran-nuclear-deal.html (Accessed 21 May 2024).

ERLANGER, Steven, "Rushdie Has Lived under an Iranian Death Sentence since 1989", *The New York Times*, 12 August 2022, Retrieved from: https://www.nytimes.com/2022/08/12/nyregion/salman-rushdie-fatwa-satanic-verses.html (Accessed 20 May 2024).

FARHAT, Beatrice, "Iran Slaps Sanctions on US, UK Entities over Support for Israel's War Effort", *Al-Monitor*, 2024, Retrieved from: https://www.al-monitor.com/originals/2024/05/iran-slaps-sanctions-us-uk-entities-over-support-israels-war-effort (Accessed 11 May 2024).

FAULCONBRIDGE, Guy, and Sachin RAVIKUMAR, "Russia Says UK Navy Blew up Nord Stream, London Denies Involvement", *Reuters*, 29 October 2022, Retrieved from: https://www.reuters.com/world/europe/russia-says-british-navy-personnel-blew-up-nord-stream-gas-pipelines-2022-10-29/ (Accessed 16 May 2024).

FELTON, Alex, and Marie-Louise GUMUCHIAN, "U.N. General Assembly Resolution Calls Crimean Referendum Invalid", *CNN*, 2014, Retrieved from: https://www.cnn.com/2014/03/27/world/europe/ukraine-crisis/index.html (Accessed 2 May 2024).

FISCHERKELLER, Michael P, and Richard J. HARKNETT, "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace", *Lawfare*, 2018, Retrieved from: https://www.lawfaremedia.org/article/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace (Accessed 19 October 2023).

FISCHERKELLER, Michael P, Emily O. GOLDMAN, and Richard J. HARKNETT, "Cyber Persistence Theory in the Russo-Ukrainian War", *Binding Hook*, 2023, Retrieved from: https://bindinghook.com/articles-book-binder/cyber-persistence-theory-in-the-russo-ukrainian-war/ (Accessed 9 November 2023).

FISCHERKELLER, Michael P, "The Fait Accompli and Persistent Engagement in Cyberspace", *War on the Rocks*, 2020, Retrieved from: https://warontherocks.com/2020/06/the-fait-accompli-and-persistent-engagement-in-cyberspace/ (Accessed 5 November 2023).

FORREST, Adam, and Archie MITCHELL, "Tory Backlash after Cameron Calls for Palestinian State to End Gaza Conflict", *The Independent*, 2024, Retrieved

from: https://www.independent.co.uk/news/uk/politics/israel-palestine-david-cameron-gaza-conflict-b2487208.html (Accessed 11 May 2024).

GARAMONE, Jim, "Iran Shoots Down U.S. Global Hawk Operating in International Airspace", *U.S. Department of Defense*, 2019, Retrieved from: https://www.defense.gov/News/News-Stories/article/article/1882497/iran-shoots-down-us-global-hawk-operating-international-airspace/https%3A%2F%2Fwww.defense.gov%2FNews%2FNews-Stories%2FArticle%2FArticle%2F1882497%2Firan-shoots-down-us-global-hawk-operating-international-airspace%2F (Accessed 17 October 2023).

GARDNER, Frank, "Aukus Submarine Deal: Is Conflict with China Getting Closer?", *BBC News*, 14 March 2023, Retrieved from: https://www.bbc.com/news/world-asia-china-64959500 (Accessed 10 May 2024).

GILES, Keir, "Putin Does Not Need to Invade Ukraine to Get His Way", *Chatham House*, 2021, Retrieved from: https://www.chathamhouse.org/2021/12/putin-does-not-need-invade-ukraine-get-his-way (Accessed 24 September 2023).

GILLETT, Francesca, "US Says Strikes on Iran-Linked Targets in Iraq and Syria Just 'the Beginning'", *BBC News*, 2024, Retrieved from: https://www.bbc.co.uk/news/live/world-68144478 (Accessed 11 May 2024).

GORDON CORERA, "For All the Talk about 'Cyber War', Today Shows That When Conflict Escalates to This Point It Is Secondary. If You Want to Take Out Infrastructure Then Missiles Are More Straightforward than Using Computer Code. Cyber's Main Role Now Is Perhaps to Sow Confusion about Events", *X (formerly Twitter)*, 2022, Retrieved from: https://twitter.com/gordoncorera/status/1496805147271471117 (Accessed 31 October 2023).

GRADY, John, "U.K. Defence Secretary: 'Never Underestimate My Nation'", *U.S. Naval Institute News*, 2018, Retrieved from: https://news.usni.org/2018/08/07/u-k-defence-secretary-never-underestimate-nation (Accessed 17 May 2024).

GRAHAM-HARRISON, Emma, Luke HARDING, and Andrew ROTH, "Confusion over UK Claim That Putin Plans Coup in Ukraine", *The Guardian*, 22 January 2022, Retrieved from: https://www.theguardian.com/world/2022/jan/22/confusion-over-uk-claim-that-putin-plans-coup-in-ukraine (Accessed 7 May 2024).

GRAMER, Robbie, and Amy MACKINNON, "Iran and Russia Are Closer Than Ever Before", *Foreign Policy*, 2023, Retrieved from: https://foreignpolicy.com/2023/01/05/iran-russia-drones-ukraine-war-military-cooperation/ (Accessed 11 May 2024).

GREENBERG, Andy, "How an Entire Nation Became Russia's Test Lab for Cyberwar", *Wired*, 20 June 2017, Retrieved from:

https://www.wired.com/story/russian-hackers-attack-ukraine/ (Accessed 19 September 2023).

GRITTEN, David, "Albania Severs Diplomatic Ties with Iran over Cyber-Attack", *BBC News*, 7 September 2022, Retrieved from: https://www.bbc.com/news/world-europe-62821757 (Accessed 16 October 2023).

GROLL, Elias, "Stuxnet Was a Cyber Hiroshima", *Australian Financial Review*, 2016, Retrieved from: https://www.afr.com/technology/stuxnet-was-a-cyber-hiroshima-20160606-gpcuno (Accessed 22 September 2023).

GROSS, Judah Ari, "After Alleged Iranian Cyberattack, Israel's Water Authority Beefs up Defenses", *The Times of Israel*, 2021, Retrieved from: https://www.timesofisrael.com/after-alleged-iranian-cyberattack-israels-water-authority-beefs-up-defenses/ (Accessed 3 October 2023).

HADDICK, Robert, "America Has No Answer to China's Salami-Slicing", *War on the Rocks*, 2014, Retrieved from: https://warontherocks.com/2014/02/america-has-no-answer-to-chinas-salami-slicing/ (Accessed 12 February 2024).

HAFEZI, Parisa, John IRISH, Tom BALMFORTH, and Jonathan LANDAY, "Exclusive: Iran Sends Russia Hundreds of Ballistic Missiles", *Reuters*, 21 February 2024, Retrieved from: https://www.reuters.com/world/iran-sends-russia-hundreds-ballistic-missiles-sources-say-2024-02-21/ (Accessed 27 May 2024).

HALE, Erin, "Hong Kong: China Will No Longer Recognise British National Overseas Citizens", *The Guardian*, 29 January 2021, Retrieved from: https://www.theguardian.com/world/2021/jan/29/britain-launches-visa-scheme-for-hong-kong-citizens (Accessed 9 May 2024).

HARDING, Luke, and Matthew WEAVER, "Barack Obama Calls for 'Reset' in US-Russia Relations", *The Guardian*, 7 July 2009, Retrieved from: https://www.theguardian.com/world/2009/jul/07/barack-obama-russia-moscow-speech (Accessed 14 May 2024).

HARKNETT, Richard J., Michael P. FISCHERKELLER, and Emily O. GOLDMAN, "U.K. National Cyber Force, Responsible Cyber Power, and Cyber Persistence Theory", *Lawfare*, 2023, Retrieved from: https://www.lawfaremedia.org/article/uk-national-cyber-force-responsible-cyber-power-and-cyber-persistence-theory (Accessed 18 October 2023).

HEALEY, Jason, "Preparing for Inevitable Cyber Surprise", *War on the Rocks*, 2022, Retrieved from: https://warontherocks.com/2022/01/preparing-for-inevitable-cyber-surprise/ (Accessed 24 September 2023).

HEARST, David, "Court Told of Plot to Murder Tycoon", *The Guardian*, 2003, Retrieved from: https://www.theguardian.com/uk/2003/sep/13/russia.world (Accessed 14 May 2024).

HELM, Toby, "Sunak Promises Israel 'Unqualified Support in Face of Evil' – but Makes No Mention of Gaza's Plight | Israel-Gaza War", *The Guardian*, 2023, Retrieved from: https://www.theguardian.com/world/2023/oct/14/sunak-promises-israel-unqualified-support-in-face-of-evil-but-fails-to-mention-plight-of-gaza (Accessed 31 March 2024).

HYBRID CoE, "Hybrid CoE", n.d., Retrieved from: https://www.hybridcoe.fi/ (Accessed 22 January 2024).

JENNINGS, Ralph, "French, British Ships to Sail Disputed Asian Sea, Rile China", *Voice of America*, 2018, Retrieved from: https://www.voanews.com/a/france-britain-ships-south-china-sea-china/4440197.html (Accessed 8 May 2024).

JENSEN, Benjamin, and David BANKS, "Cyber Warfare May Be Less Dangerous than We Think", *Washington Post*, 7 December 2021, Retrieved from: https://www.washingtonpost.com/news/monkey-cage/wp/2018/04/26/what-can-cybergames-teach-us-about-cyberattacks-quite-a-lot-in-fact/ (Accessed 3 October 2023).

JORDÁN, Javier, "Hybrid Warfare: A Catch-all Concept", *Global Strategy*, 2017, Retrieved from: https://global-strategy.org/hybrid-warfare-a-catch-all-concept/ (Accessed 9 February 2024).

JUN, Jenny, "How Will AI Change Cyber Operations?", *War on the Rocks*, 2024, Retrieved from: https://warontherocks.com/2024/04/how-will-ai-change-cyber-operations/ (Accessed 2 June 2024).

JUNEAU, Thomas, "How Iran Helped Houthis Expand Their Reach", *War on the Rocks*, 2021, Retrieved from: https://warontherocks.com/2021/08/how-iran-helped-houthis-expand-their-reach/ (Accessed 17 October 2023).

KAIMAN, Jonathan, "Hong Kong's Umbrella Revolution", *The Guardian*, 30 September 2014, Retrieved from: https://www.theguardian.com/world/2014/sep/30/-sp-hong-kong-umbrella-revolution-pro-democracy-protests (Accessed 8 May 2024).

KALIN, Stephan, and Rania EL GAMEL, "Saudi Oil Facilities Attacked, U.S. Sees Threat in Iraq from Iran-Backed Forces", *Reuters*, 14 May 2019, Retrieved from: https://www.reuters.com/article/us-saudi-oil-usa-iran-idUSKCN1SK0YM (Accessed 17 October 2023).

KARATNYCKY, Adrian, "Ukraine's Orange Revolution", *Foreign Affairs*, 1 March 2005, Retrieved from: https://www.foreignaffairs.com/articles/russia-fsu/2005-03-01/ukraines-orange-revolution (Accessed 14 May 2024).

KEATE, Noah, and Stefan BOSCIA, "Thousands of UK Troops Hit in Suspected Chinese Hack on Defense Ministry", *POLITICO*, 2024, Retrieved from: https://www.politico.eu/article/suspected-china-hack-hits-uks-defense-ministry/ (Accessed 10 May 2024).

KELION, Leo, "Huawei Set for Limited Role in UK 5G Networks", *BBC News*, 28 January 2020, Retrieved from: https://www.bbc.com/news/technology-51283059 (Accessed 18 May 2024).

KINGSLEY, Patrick, "How Tiny Estonia Stepped out of USSR's Shadow to Become an Internet Titan", *The Guardian*, 15 April 2012, Retrieved from: https://www.theguardian.com/technology/2012/apr/15/estonia-ussr-shadow-internet-titan (Accessed 13 November 2023).

KITE, Melissa, and Damien MCELROY, "Georgia: David Cameron Flies into Tbilisi to Meet Country's Leaders", *The Telegraph*, 2008, Retrieved from: https://www.telegraph.co.uk/news/worldnews/europe/georgia/2569377/Georgia-David-Cameron-flies-into-Tbilisi-to-meet-countrys-leaders.html (Accessed 14 May 2024).

KOFMAN, Micheal, "Russian Hybrid Warfare and Other Dark Arts", *War on the Rocks*, 2016, Retrieved from: https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/ (Accessed 23 January 2024).

KOFMAN, Micheal, "Getting the Fait Accompli Problem Right in U.S. Strategy", *War on the Rocks*, 2020, Retrieved from: https://warontherocks.com/2020/11/getting-the-fait-accompli-problem-right-in-u-s-strategy/ (Accessed 20 October 2023).

KOSACHEV, Konstantin, "An Insult to Our War Dead", *The Guardian*, 6 March 2007, Retrieved from: https://www.theguardian.com/commentisfree/2007/mar/06/comment.secondworldwar (Accessed 29 October 2023).

KUO, Lily, and Helen DAVIDSON, "Hong Kong Crisis: China Presents Security Laws Banning Subversion and Separatism", *The Guardian*, 22 May 2020, Retrieved from: https://www.theguardian.com/world/2020/may/22/chinas-national-security-law-ban-subversion-and-separatism-hong-kong (Accessed 9 May 2024).

KUO, Lily, "This Is the End of Hong Kong: China Pushes Controversial Security Laws", *The Guardian*, 21 May 2020, Retrieved from: https://www.theguardian.com/world/2020/may/21/china-proposes-controversial-national-security-law-for-hong-kong (Accessed 9 May 2024).

KWAN, Rhoda, "Beijing Criticises UK for Creating 'Second-Class Citizens' with Hong Kong Visa Scheme", *The Guardian*, 16 December 2021, Retrieved from: https://www.theguardian.com/world/2021/dec/16/beijing-criticises-uk-for-creating-second-class-citizens-with-hong-kong-visa-scheme (Accessed 10 May 2024).

LAFRANIERE, Sharon, "Russia's Putin Calls Iraq War A 'Mistake'", *Washington Post*, 1 March 2024, Retrieved from: https://www.washingtonpost.com/archive/politics/2003/03/18/russias-putin-calls-iraq-war-a-mistake/7fff0ba1-bfda-4970-a1a9-f7c7afd6aaa2/ (Accessed 14 May 2024).

LANDLER, Mark, and John MARKOFF, "In Estonia, What May Be the First War in Cyberspace", *The New York Times*, 28 May 2007, Retrieved from: https://www.nytimes.com/2007/05/28/business/worldbusiness/28iht-cyberwar.4.5901141.html (Accessed 29 October 2023).

LANDLER, Mark, "Trump Abandons Iran Nuclear Deal He Long Scorned", *The New York Times*, 8 May 2018, Retrieved from: https://www.nytimes.com/2018/05/08/world/middleeast/trump-iran-nuclear-deal.html (Accessed 10 May 2024).

LAU, Stuart, "UK Parliament Calls Taiwan 'Independent Country' as Cleverly Visits China", *POLITICO*, 2023, Retrieved from: https://www.politico.eu/article/uk-parliament-calls-taiwan-independent-country-report-says-james-cleverly-visit-china/ (Accessed 10 May 2024).

LEE, Matthew, "Biden Repudiates Trump on Iran, Ready for Talks on Nuke Deal", *AP News*, 2021, Retrieved from: https://apnews.com/article/biden-iran-nuclear-deal-d261fbe927984d9328db0e0f74b62410 (Accessed 21 May 2024).

LEWIS, James Andrew, "Iran and Cyber Power", *Center for Strategic and International Studies*, 2019, Retrieved from: https://www.csis.org/analysis/iran-and-cyber-power (Accessed 1 June 2024).

LIN, Han, and Meng TAO, "70 Years of Diplomacy: How PR China Claimed Its Lawful Seat in the UN", *CGTN*, 2019, Retrieved from: https://news.cgtn.com/news/2019-09-24/70-years-of-diplomacy-How-PR-China-claimed-its-lawful-seat-in-the-UN-KeWvv1hrLa/index.html (Accessed 16 May 2024).

LINN, Herb, "Oft-Neglected Cost Drivers of Cyber Weapons", *Council on Foreign Relations*, 2016, Retrieved from: https://www.cfr.org/blog/oft-neglected-cost-drivers-cyber-weapons (Accessed 1 November 2023).

LOCK, Samantha, Lauren GAMBINO, Jem BARTHOLOMEW, Rebecca RATCLIFFE, Jane CLINTON, Samantha LOCK (now), and others, "EU Praises 'Restraint' of Kyiv Government; Blinken Denounces Kremlin Claims – as It Happened", *The Guardian*, 20 February 2022, Retrieved from: https://www.theguardian.com/world/live/2022/feb/19/russia-ukraine-news-crisis-latest-putin-biden-kyiv-russian-invasion (Accessed 7 May 2024).

LONERGAN, Erica D., "The Cyber-Escalation Fallacy", *Foreign Affairs*, 15 April 2022, Retrieved from: https://www.foreignaffairs.com/articles/russian-federation/2022-04-15/cyber-escalation-fallacy (Accessed 17 September 2023).

LYNN, William J., "Defending a New Domain", *Foreign Affairs*, 1 September 2010, Retrieved from: https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain (Accessed 19 September 2023).

MACASKILL, Ewen, and Chris MCGREAL, "Israel Should Be Wiped off Map, Says Iran's President", *The Guardian*, 26 October 2005, Retrieved from:

https://www.theguardian.com/world/2005/oct/27/israel.iran (Accessed 21 May 2024).

MAIZLAND, Lindsay, and Clara FONG, "Hong Kong's Freedoms: What China Promised and How It's Cracking Down", *Council on Foreign Relations*, 2024, Retrieved from: https://www.cfr.org/backgrounder/hong-kong-freedoms-democracy-protests-china-crackdown (Accessed 8 May 2024).

MARGOLIN, Josh, John SANTUCCI, and Katherine FAULDERS, "Trump Says He Stopped Iran Strike with Just 10 Minutes to Spare Because He Was Concerned about Casualties", *ABC News*, 2019, Retrieved from: https://abcnews.go.com/Politics/president-trump-ordered-military-strike-iran-reversed-sources/story?id=63853570 (Accessed 17 October 2023).

MARKS, Joseph, "Here's What Cyber Pros Are Watching in the Ukraine Conflict", *Washington Post*, 24 February 2022, Retrieved from: https://www.washingtonpost.com/politics/2022/02/24/heres-what-cyber-pros-are-watching-ukraine-conflict/ (Accessed 24 September 2023).

MARTIN, Ciaran, "Cyber Realism in a Time of War", *Lawfare*, 2022, Retrieved from: https://www.lawfaremedia.org/article/cyber-realism-time-war (Accessed 15 September 2023).

MASCHMEYER, Lennart, and Kostyuk NADIYA, "There Is No Cyber 'Shock and Awe': Plausible Threats in the Ukrainian Conflict", *War on the Rocks*, 2022, Retrieved from: https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/ (Accessed 15 September 2023).

MASCHMEYER, Lennart, "Persistent Engagement Neglects Secrecy at Its Peril", *Lawfare*, 2020, Retrieved from: https://www.lawfaremedia.org/article/persistent-engagement-neglects-secrecy-its-peril (Accessed 4 September 2023).

MASCHMEYER, Lennart, "Why Cyber War Is Subversive, and How That Limits Its Strategic Value", *War on the Rocks*, 2021b, Retrieved from: https://warontherocks.com/2021/11/why-cyber-war-is-subversive-and-how-that-limits-its-strategic-value/ (Accessed 4 September 2023).

MASON, Rowena, "Theresa May Accuses Russia of Interfering in Elections and Fake News", *The Guardian*, 14 November 2017, Retrieved from: https://www.theguardian.com/politics/2017/nov/13/theresa-may-accuses-russia-of-interfering-in-elections-and-fake-news (Accessed 15 May 2024).

MCELROY, Damien, "Britain Complains after Ayatollah Khamenei Describes UK as 'Evil'", *The Telegraph*, 2009, Retrieved from: https://www.telegraph.co.uk/news/worldnews/middleeast/iran/5580734/Britain-complains-after-Ayatollah-Khamenei-describes-UK-as-evil.html (Accessed 19 May 2024).

MCGUINNESS, Damien, "How a Cyber Attack Transformed Estonia", *BBC News*, 27 April 2017, Retrieved from: https://www.bbc.com/news/39655415 (Accessed 29 October 2023).

MCKEW, Molly K., "The Gerasimov Doctrine", *POLITICO Magazine*, 2020, Retrieved from: https://politi.co/2KZQlKd (Accessed 2 February 2024).

MEAD, Walter Russell, "'Lights Out,' by Ted Koppel", *The New York Times*, 20 November 2015, Retrieved from: https://www.nytimes.com/2015/11/22/books/review/lights-out-by-ted-koppel.html (Accessed 20 September 2023).

MEHDI, Syed Zafar, "Iran Summons British Envoy over Media Coverage of Protests", *Anadolu Agency*, 2022, Retrieved from: https://www.aa.com.tr/en/middle-east/iran-summons-british-envoy-over-media-coverage-of-protests/2694241 (Accessed 11 May 2024).

MEYER, Henry, Daryna KRASNOLUTSKA, and Kateryna CHURSINA, "Russia Stages Mass Military Drills as Ukraine Tensions Climb", *Bloomberg*, 6 April 2021, Retrieved from: https://www.bloomberg.com/news/articles/2021-04-06/russia-stages-mass-military-drills-amid-tensions-with-ukraine (Accessed 7 May 2024).

MICROSOFT, "DoS vs. DDoS Attacks: What's The Difference?", *Microsoft 365*, 2023, Retrieved from: https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/dos-vs-ddos-attacks-whats-the-difference (Accessed 30 November 2023).

MILLER, Maggie, "Russian Invasion of Ukraine Could Redefine Cyber Warfare", *POLITICO*, 2022, Retrieved from: https://www.politico.com/news/2022/01/28/russia-cyber-army-ukraine-00003051 (Accessed 15 September 2023).

MITCHELL, Robbie, "How Resilient Is Your Country's Internet", *Internet Society Pulse*, 2023, Retrieved from: https://pulse.internetsociety.org/blog/how-resilient-is-your-countrys-internet (Accessed 13 June 2024).

MOTAMEDI, Maziar, "Iran and Israel: From Allies to Archenemies, How Did They Get Here?", *Al Jazeera*, 2023, Retrieved from: https://www.aljazeera.com/news/2023/11/6/iran-and-israel-from-allies-to-archenemies-how-did-they-get-here (Accessed 25 May 2024).

MULHOLLAND, Hélène, "Vladimir Putin and David Cameron Find Common Ground but No Action on Syria", *The Guardian*, 2 August 2012, Retrieved from: https://www.theguardian.com/politics/2012/aug/02/cameron-putin (Accessed 14 May 2024).

MURGIA, Madhumita, "Could Cyberattack on Turkey Be a Russian Retaliation?", *The Telegraph*, 2015, Retrieved from: https://www.telegraph.co.uk/technology/internet-security/12057478/Could-

cyberattack-on-Turkey-be-a-Russian-retaliation.html (Accessed 2 November 2023).

NAKASHIMA, Ellen, and Joby WARRICK, "Stuxnet Was Work of U.S. and Israeli Experts, Officials Say", *Washington Post*, 2 June 2012, Retrieved from: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html (Accessed 11 June 2024).

NATO Cooperative Cyber Defence Centre of Excellence, "2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law", *NATO Cooperative Cyber Defence Centre of Excellence*, Retrieved from: https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/ (Accessed 30 October 2023).

NICHOLSON, Kate, "China's Media Spokesperson Dragged The UK With Just 4 Brutal Points About Britain", *HuffPost UK*, 2023, Retrieved from: https://www.huffingtonpost.co.uk/entry/china-drag-uk-trade-points-lbc-andrew-marr_uk_650178a1e4b034d7e74176ad (Accessed 2 June 2024).

OBAMA, Barack, "Barack Obama: Taking the Cyberattack Threat Seriously", *Wall Street Journal*, 19 July 2012, Retrieved from: http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html (Accessed 29 October 2023).

ORYSZCZUK, Stephen, "UK-Israel: 70 Years of Relations", *Jewish News*, 2020, Retrieved from: https://www.jewishnews.co.uk/uk-israel-70-years-of-relations/ (Accessed 31 March 2024).

PELHAM, Lipika, "Mahsa Amini: Iran Responsible for 'Physical Violence' Leading to Death, UN Says", *BBC News*, 2024, Retrieved from: https://www.bbc.com/news/world-middle-east-68511112 (Accessed 21 May 2024).

PITAS, Costas, and Estelle SHIRBON, "Britain Expels 23 Russian Diplomats over Chemical Attack on Ex-Spy", *Reuters*, 14 March 2018, Retrieved from: https://www.reuters.com/article/idUSKCN1GQ1QG/ (Accessed 6 May 2024).

POLITICO, "U.S. Admiral Says China Has Fully Militarized Islands", *POLITICO*, 2022, Retrieved from: https://www.politico.com/news/2022/03/20/china-islands-militarized-missiles-00018737 (Accessed 10 May 2024).

POMERLEAU, Mark, and Andrew EVERSDEN, "What to Make of US Cyber Activities in Iran", *C4ISRNet*, 2019, Retrieved from: https://www.c4isrnet.com/dod/2019/06/25/why-trump-may-have-opted-for-a-cyberattack-in-iran/ (Accessed 17 October 2023).

POURPARSA, Parham, "Why Is Britain an 'Old Fox' in Iranian Media Rhetoric?", *BBC News*, 25 August 2015, Retrieved from:

https://www.bbc.com/news/world-middle-east-34052821 (Accessed 19 May 2024).

PROCTOR, Kate, "Johnson: Huawei Critics 'Must Tell Us What's the Alternative'", *The Guardian*, 14 January 2020, Retrieved from: https://www.theguardian.com/technology/2020/jan/14/johnson-huawei-critics-must-tell-us-whats-the-alternative (Accessed 9 May 2024).

PUYVELDE, Damien Van, "Hybrid War – Does It Even Exist?", *NATO Review*, 2015, Retrieved from: https://www.nato.int/docu/review/articles/2015/05/07/hybrid-war-does-it-even-exist/index.html (Accessed 9 February 2024).

REGAN, Helen, Hamdi ALKHSHALI, and Tamara QIBLAWI, "Iran Vows Revenge as It Accuses Israel of Deadly Airstrike on Syria Consulate in Deepening Middle East Crisis", *CNN*, 2024, Retrieved from: https://www.cnn.com/2024/04/02/middleeast/iran-response-israel-damascus-consulate-attack-intl-hnk/index.html (Accessed 21 May 2024).

REYNOLDS, James, "Iran IAEA Nuclear Report Deepens Concerns", *BBC News*, 8 November 2011, Retrieved from: https://www.bbc.com/news/world-middle-east-15642021 (Accessed 21 May 2024).

RID, Thomas, "Why You Haven't Heard About the Secret Cyberwar in Ukraine", *The New York Times*, 18 March 2022, Retrieved from: https://www.nytimes.com/2022/03/18/opinion/cyberwar-ukraine-russia.html (Accessed 24 September 2023).

ROBERTSON, Jordan, and Micheal RILEY, "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar", *Bloomberg*, 10 December 2014, Retrieved from: https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar (Accessed 22 September 2023).

ROBINSON, Kali, and Will MERROW, "Iran's Regional Armed Network", *Council on Foreign Relations*, 2024, Retrieved from: https://www.cfr.org/article/irans-regional-armed-network (Accessed 21 May 2024).

ROBINSON, Kali, "What Is the Iran Nuclear Deal?", *Council on Foreign Relations*, 2023, Retrieved from: https://www.cfr.org/backgrounder/what-iran-nuclear-deal (Accessed 10 May 2024).

ROBINSON, Nick, "A Small Island No-One Pays Attention To", *BBC News*, 6 September 2013, Retrieved from: https://www.bbc.com/news/uk-politics-23982829 (Accessed 30 April 2024).

ROSENBERG, Steve, "EU Referendum: What Does Russia Gain from Brexit?", *BBC News*, 26 June 2016, Retrieved from: https://www.bbc.com/news/world-europe-36629146 (Accessed 15 May 2024).

RUY, Donatienne, "Did Russia Influence Brexit?", *Center for Strategic and International Studies*, 2020, Retrieved from:

https://www.csis.org/blogs/brexit-bits-bobs-and-blogs/did-russia-influence-brexit (Accessed 6 May 2024).

RÜHLE, Michael, and Clare ROBERTS, "Enlarging NATO's Toolbox to Counter Hybrid Threats", *NATO Review*, 2021, Retrieved from: https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html (Accessed 5 January 2024).

SABBAGH, Dan, and David PEGG, "Russian Elite Must Reveal How They Paid for UK Property, Say MPs", *The Guardian*, 17 March 2018, Retrieved from: https://www.theguardian.com/uk-news/2018/mar/17/russian-elite-must-reveal-how-they-paid-for-uk-property-say-mps (Accessed 6 May 2024).

SABBAGH, Dan, "Using Huawei in UK 5G Networks Would Be 'Madness', US Says", *The Guardian*, 13 January 2020, Retrieved from: https://www.theguardian.com/technology/2020/jan/13/using-huawei-in-uk-5g-networks-would-be-madness-us-says (Accessed 9 May 2024).

SANDLE, Paul, and Guy FAULCONBRIDGE, "UK to Purge Huawei from 5G by End of 2027, Siding with Trump over China", *Reuters*, 14 July 2020, Retrieved from: https://www.reuters.com/article/idUSKCN24E30P/ (Accessed 18 May 2024).

SIDDIQUE, Haroon, Tom MCCARTHY, and Alan YUHAS, "Crimean Parliament Seizure Inflames Russian-Ukrainian Tensions – Live", *The Guardian*, 27 February 2014, Retrieved from: https://www.theguardian.com/world/2014/feb/27/ukraine-pro-russian-gunmen-seize-crimea-parliament-live-updates (Accessed 2 May 2024).

SIDDIQUI, Zeba, "Five Eyes Intelligence Chiefs Warn on China's 'Theft' of Intellectual Property", *Reuters*, 2023, Retrieved from: https://www.reuters.com/world/five-eyes-intelligence-chiefs-warn-chinas-theft-intellectual-property-2023-10-18/ (Accessed 30 November 2023).

SILVA, João da, "US Revokes Licences for Sales of Some Chips to China's Huawei", *BBC News*, 2024, Retrieved from: https://www.bbc.com/news/articles/cgxwpql2e82o (Accessed 17 May 2024).

SINGH, Rahul, "De-Escalation in Ladakh Still a Long Way off: General Naravane", *Hindustan Times*, 2021, Retrieved from: https://www.hindustantimes.com/india-news/deescalation-in-ladakh-still-a-long-way-off-general-naravane-101614174743801.html (Accessed 12 February 2024).

SMEETS, Max, "Cyber Command's Strategy Risks Friction With Allies", *Lawfare*, 2019, Retrieved from: https://www.lawfaremedia.org/article/cyber-commands-strategy-risks-friction-allies (Accessed 20 October 2023).

SMITH, Ben, and Timothy ROBINSON, "The Salisbury Incident", *United Kingdom Parliament*, 2024, Retrieved from:

https://commonslibrary.parliament.uk/research-briefings/cdp-2018-0204/ (Accessed 6 May 2024).

SMITH, Brad, "The Need for a Digital Geneva Convention", *Microsoft*, 2017, Retrieved from: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/ (Accessed 30 October 2023).

SMITH, David, "Trump and May Appear at Odds over Russia Sanctions at White House Visit", *The Guardian*, 27 January 2017, Retrieved from: https://www.theguardian.com/us-news/2017/jan/27/theresa-may-donald-trump-white-house-visit-russia-sanctions (Accessed 15 May 2024).

SMITH, David, "WikiLeaks Emails: What They Revealed about the Clinton Campaign's Mechanics", *The Guardian*, 2016, Retrieved from: https://www.theguardian.com/us-news/2016/nov/06/wikileaks-emails-hillary-clinton-campaign-john-podesta (Accessed 30 November 2023).

SOO, Zen, "Hong Kong in Limbo 25 Years after British Handover to China", *AP News*, 2022, Retrieved from: https://apnews.com/article/voting-rights-china-hong-kong-932009be8d2a91ef2f84e6e406d290b4 (Accessed 31 March 2024).

STEWART, Heather, and Dan SABBAGH, "UK Huawei Decision Appears to Avert Row with US", *The Guardian*, 28 January 2020, Retrieved from: https://www.theguardian.com/technology/2020/jan/28/boris-johnson-gives-green-light-for-huawei-5g-infrastructure-role (Accessed 9 May 2024).

STUBBS, Jack, and Alexandra ALPER, "Shot across the Bow: U.S. Increases Pressure on UK Ahead of Key Huawei Decision", *Reuters*, 8 January 2020, Retrieved from: https://www.reuters.com/article/idUSKBN1Z70WA/ (Accessed 18 May 2024).

SWAINE, Jon, "Georgia: Russia 'Conducting Cyber War'", *The Telegraph*, 2008, Retrieved from: https://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html (Accessed 22 September 2023).

TAIT, Robert, "Foreign Office Protests after Khamenei Singles out 'Evil Britain'", *The Guardian*, 19 June 2009, Retrieved from: https://www.theguardian.com/world/2009/jun/19/khamemei-iran-protests-diplomat (Accessed 21 May 2024).

TANI, Max, "Wall Street Journal Reporters Split over Iran Story", *Semafor*, 2023, Retrieved from: https://www.semafor.com/article/10/15/2023/wall-street-journal-reporters-split-over-iran-story (Accessed 21 May 2024).

TAZMINI, Ghoncheh, "Russia and Iran – a Strategic Alliance or Something More?", *The London School of Economics and Political Science*, 2021, Retrieved from: https://www.lse.ac.uk/research/research-for-the-world/politics/russia-and-iran-a-strategic-alliance-or-something-more (Accessed 11 May 2024).

TESLOVA, Elena, "Russia Issues List of Countries, Considering Their 'Unfriendly Actions'", *Anadolu Agency*, 2022, Retrieved from: https://www.aa.com.tr/en/russia-ukraine-crisis/russia-issues-list-of-countries-considering-their-unfriendly-actions/2526541 (Accessed 7 May 2024).

THOMSON, Iain, "Georgia Gets Allies in Russian Cyberwar", *Itnews*, 2008, Retrieved from: https://www.itnews.com.au/news/georgia-gets-allies-in-russian-cyberwar-119422 (Accessed 29 October 2023).

TOBIN, James, "AUKUS Security Partnership", *United Kingdom Parliament*, 2024, Retrieved from: https://lordslibrary.parliament.uk/aukus-security-partnership/ (Accessed 10 May 2024).

TOBIN, James, "Iran, Negotiations on Its Nuclear Capabilities, and Its Wider Regional Influence", *United Kingdom Parliament*, 2022, Retrieved from: https://lordslibrary.parliament.uk/iran-negotiations-on-its-nuclear-capabilities-and-its-wider-regional-influence/ (Accessed 10 May 2024).

TRAN, Mark, "Britain Expels Four Russian Diplomats", *The Guardian*, 16 July 2007, Retrieved from: https://www.theguardian.com/uk/2007/jul/16/russia.politics (Accessed 14 May 2024).

TRAYNOR, Ian, Paul LEWIS, Kim WILLSHER, and Patrick WINTOUR, "Ukraine Crisis: Crimea Announces Referendum on Joining Russia", *The Guardian*, 6 March 2014, Retrieved from: https://www.theguardian.com/world/2014/mar/06/ukraine-crisis-european-leaders-emergency-summit (Accessed 2 May 2024).

TRAYNOR, Ian, "US Campaign behind the Turmoil in Kiev", *The Guardian*, 26 November 2004, Retrieved from: https://www.theguardian.com/world/2004/nov/26/ukraine.usa (Accessed 14 May 2024).

TRIANTAPHYLLOU, Dimitrios, "The Wheels Are Coming Off - Dimitrios Triantaphyllou", *GA Panorama*, 24 December 2023, Retrieved from: https://www.uikpanorama.com/blog/2023/12/24/d/ (Accessed 25 December 2023).

URQUHART, Conal, and Barry NEILD, "Ukraine: Tymoshenko Freed as President Denounces 'Coup' - 22 February as It Happened", *The Guardian*, 23 February 2014, Retrieved from: https://www.theguardian.com/world/2014/feb/22/ukraine-crisis-uncertainty-after-yanukovych-signs-deal-live-updates (Accessed 1 May 2024).

VAKIL, Sanam, and Bilal SAAB, "Iran's Attack on Israel Was Not the Failure Many Claim but It Has Ended Israel's Isolation, *Chatham House*, 15 April 2024, Retrieved from: https://www.chathamhouse.org/2024/04/irans-attack-israel-was-not-failure-many-claim-it-has-ended-israels-isolation (Accessed 11 May 2024).

VAKIL, Sanam, "Iran's Regional Strategy Is Raising the Stakes of Hamas-Israel War, *Chatham House*, 10 November 2023, Retrieved from: https://www.chathamhouse.org/2023/11/irans-regional-strategy-raising-stakes-hamas-israel-war (Accessed 21 May 2024).

VALERIANO, Brandon, and Benjamin M. JENSEN, "How Cyber Operations Can Help Manage Crisis Escalation with Iran", *Washington Post*, 24 June 2019b, Retrieved from: https://www.washingtonpost.com/politics/2019/06/25/how-cyber-operations-can-help-manage-crisis-escalation-with-iran/ (Accessed 17 October 2023).

VALERIANO, Brandon, "Why Can't Cyber Scholars Move Beyond the Basics?", *The National*, 2022e, Retrieved from: https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/why-can%E2%80%99t-cyber-scholars-move-beyond (Accessed 25 September 2023).

VALERIANO, Brandon, "War Is Still War: Don't Listen to the Cult of Cyber", *The National Interest* (The Center for the National Interest, 2022), Retrieved from: https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/war-still-war-don%E2%80%99t-listen-cult-cyber (Accessed 25 September 2023).

VICENS, A. J., "AI Is Helping US Spies Catch Stealthy Chinese Hacking Ops, NSA Official Says", *CyberScoop*, 2024, Retrieved from: https://cyberscoop.com/ai-china-hacking-operations/ (Accessed 12 June 2024).

VOROTNYUK, Maryna, "Security Cooperation between Ukraine and the UK", *Royal United Services Institute* (RUSI), 10 November 2021, Retrieved from: https://rusi.orghttps://rusi.org (Accessed 29 May 2024).

WAITZMAN, Eren, "UK-China Relations", 3 July 2023, Retrieved from: https://lordslibrary.parliament.uk/uk-china-relations/ (Accessed 8 May 2024).

WAITZMAN, Eren, "UK-Ukraine Credit Support Agreement", *United Kingdom Parliament*, 16 December 2021, Retrieved from: https://lordslibrary.parliament.uk/uk-ukraine-credit-support-agreement/ (Accessed 15 May 2024).

WALKER, Peter, "UK Pledges to Back Sweden and Finland against Russian Threats", *The Guardian*, 11 May 2022, Retrieved from: https://www.theguardian.com/politics/2022/may/11/uk-pledges-to-back-sweden-and-finland-against-russian-threats-nato (Accessed 30 May 2024).

WALKER, Shaun, Oksana GRYTSENKO, and Howard AMOS, "Ukraine: Pro-Russia Separatists Set for Victory in Eastern Region Referendum", *The Guardian*, 12 May 2014, Retrieved from: https://www.theguardian.com/world/2014/may/11/eastern-ukraine-referendum-donetsk-luhansk (Accessed 2 May 2024).

WALKER, Shaun, "Things Aren't Easy between Us: Boris Johnson Spars with Russian Counterpart", *The Guardian*, 22 December 2017, Retrieved from:

https://www.theguardian.com/politics/2017/dec/22/boris-johnson-meets-russian-counterpart-sergei-lavrov-moscow (Accessed 15 May 2024).

WATT, Nicholas, Paul LEWIS, and Tania BRANIGAN, "US Anger at Britain Joining Chinese-Led Investment Bank AIIB", *The Guardian*, 13 March 2015, Retrieved from: https://www.theguardian.com/us-news/2015/mar/13/white-house-pointedly-asks-uk-to-use-its-voice-as-part-of-chinese-led-bank (Accessed 8 May 2024).

WATTS, Joe, "Russia Responsible for Syria Chemical Attack, UK Defence Secretary Michael Fallon Says", *The Independent*, 9 April 2017, Retrieved from: https://www.independent.co.uk/news/uk/politics/michael-fallon-russia-syria-chemical-weapons-attack-air-strikes-donald-trump-vladimir-putin-a7674831.html (Accessed 15 May 2024).

WATTS, Jonathan, "Protests in Tibet Erupt into Violence", *The Guardian*, 14 March 2008, Retrieved from: https://www.theguardian.com/world/2008/mar/14/tibet.china1 (Accessed 16 May 2024).

WAUGH, Paul, "Putin Visits Britain and Is Accorded All Royal Pomp, but Chechen Protesters Question the Circumstance", *The Independent*, 23 June 2003, Retrieved from: https://www.independent.co.uk/news/uk/politics/putin-visits-britain-and-is-accorded-all-royal-pomp-but-chechen-protesters-question-the-circumstance-110156.html (Accessed 14 May 2024).

WEAVER, Matthew, and Tom MCCARTHY, "Ukraine Crisis: Deadly Clashes Shatter Truce – Thursday 20 February", *The Guardian*, 20 February 2014, Retrieved from: https://www.theguardian.com/world/blog/2014/feb/20/ukraine-crisis-new-clashes-strain-truce-live-updates (Accessed 1 May 2024).

WEAVER, Matthew, "British-Iranian Journalists in UK Warned of Death Threats from Iran", *The Guardian*, 8 November 2022, Retrieved from: https://www.theguardian.com/media/2022/nov/08/british-iranian-journalists-uk-warned-of-death-threats-from-iran (Accessed 22 May 2024).

WESTBROOK, Tom, and Ron KAYE, "China's Huawei Slams Australia 5G Mobile Network Ban as 'Politically Motivated'", *Reuters*, 24 August 2018, Retrieved from: https://www.reuters.com/article/idUSKCN1L72GC/ (Accessed 19 May 2024).

WINTOUR, Patrick, "Vladimir Putin Agrees to Moscow Meeting with David Cameron", *The Guardian*, 8 September 2011, Retrieved from: https://www.theguardian.com/world/2011/sep/08/vladimir-putin-david-cameron-moscow (Accessed 14 May 2024).

WINTOUR, Patrick, "David Cameron: UK May Be a Small Island but It Has the Biggest Heart", *The Guardian*, 6 September 2013, Retrieved from: https://www.theguardian.com/politics/2013/sep/06/david-cameron-uk-small-island (Accessed 30 April 2024).

WINTOUR, Patrick, "Saudi Arabia Says Iran behind Houthi Missile Attack on Airport", *The Guardian*, 12 June 2019a, Retrieved from: https://www.theguardian.com/world/2019/jun/12/yemen-houthi-rebel-missile-attack-injures-26-saudi-airport (Accessed 17 October 2023).

WINTOUR, Patrick, "Saudi Oil Tankers Show 'Significant Damage' after Attack – Riyadh", *The Guardian*, 13 May 2019b, Retrieved from: https://www.theguardian.com/world/2019/may/12/uae-four-merchant-ships-reported-sabotaged (Accessed 17 October 2023).

WINTOUR, Patrick, "Iran Arrests British-Iranian Citizen for 'Communicating' with Foreign News Channels", *The Guardian*, 23 November 2022, Retrieved from: https://www.theguardian.com/world/2022/nov/23/iran-arrests-british-iranian-citizen-for-communicating-with-foreign-news-channels (Accessed 11 May 2024).

WINTOUR, Patrick, "Iran Executes British-Iranian National Alireza Akbari Accused of Spying", *The Guardian*, 14 January 2023a, Retrieved from: https://www.theguardian.com/world/2023/jan/14/iran-executes-british-iranian-national-alireza-akbari-report (Accessed 22 May 2024).

WINTOUR, Patrick, "UK and Israel Sign Deal Strengthening Tech, Trade and Security Ties", *The Guardian*, 21 March 2023b, Retrieved from: https://www.theguardian.com/uk-news/2023/mar/21/uk-and-israel-to-sign-deal-strengthening-tech-trade-and-security-ties (Accessed 11 May 2024).

WINTOUR, Patrick, and Julian BORGER, "Two Oil Tankers Attacked in Gulf of Oman", *The Guardian*, 13 June 2019, Retrieved from: https://www.theguardian.com/world/2019/jun/13/oil-tankers-blasts-reports-gulf-of-oman-us-navy (Accessed 17 October 2023).

WOODCOCK, Andrew, "Boris Johnson Bans Huawei from UK's 5G Network in Major U-Turn", *The Independent*, 14 July 2020, Retrieved from: https://www.independent.co.uk/news/uk/politics/huawei-uk-ban-boris-johnson-5g-network-oliver-dowden-today-a9617886.html (Accessed 17 May 2024).

XIAMING, Liu, "Banning Huawei Would Leave Britain Trailing behind on Technology", *The Telegraph*, 4 January 2020, Retrieved from: https://www.telegraph.co.uk/politics/2020/01/04/banning-huawei-would-leave-britain-trailing-behind-technology/ (Accessed 9 May 2024).

YOUNG, Andrew, "Isolation Forest Is the Best Anomaly Detection Algorithm for Big Data Right Now", *Medium*, 13 November 2020, Retrieved from: https://towardsdatascience.com/isolation-forest-is-the-best-anomaly-detection-algorithm-for-big-data-right-now-e1a18ec0f94f (Accessed 26 November 2023).

ZINETS, Natalia, "Ukraine Hit by 6,500 Hack Attacks, Sees Russian 'Cyberwar'", *Reuters*, 29 December 2016, Retrieved from:

https://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN14I1QC (Accessed 19 September 2023).

"2030 Roadmap for UK-Israel Bilateral Relations", *United Kingdom Foreign & Commonwealth Office*, 2023. Retrieved from: https://www.gov.uk/government/publications/2030-roadmap-for-uk-israel-bilateral-relations/2030-roadmap-for-uk-israel-bilateral-relations (Accessed 11 May 2024).

"A Draft Bill Would Allow Hong Kong to Hand Suspects to China's Police", *The Economist*, 4 April 2019. Retrieved from: https://www.economist.com/china/2019/04/04/a-draft-bill-would-allow-hong-kong-to-hand-suspects-to-chinas-police (Accessed 17 May 2024).

"A Letter From Concerned Scientists", *PBS*, 2003. Retrieved from: https://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/etc/letter.html (Accessed 21 September 2023).

"Address at the Opening Ceremony of the Munich Security Conference", *United Nations Secretary-General*, 16 February 2018. Retrieved from: https://www.un.org/sg/en/content/sg/speeches/2018-02-16/address-opening-ceremony-munich-security-conference (Accessed 22 September 2023).

"Address by the President of the Russian Federation", *President of Russia*, 2022. Retrieved from: http://en.kremlin.ru/events/president/news/67843 (Accessed 7 May 2024).

"Alexander Litvinenko Died of Radiation Poisoning 15 Years Ago", *Euronews*, 2021. Retrieved from: https://www.euronews.com/2021/11/23/alexander-litvinenko-15-years-since-former-russian-spy-died-of-poisoning (Accessed 14 May 2024).

"Ambassador Liu Xiaoming Gives Exclusive Live Interview to BBC Newsnight", *Embassy of the People's Republic of China in UK*, 2019. Retrieved from: http://gb.china-embassy.gov.cn/eng/ambassador/201906/t20190613_3281363.htm (Accessed 9 May 2024).

"Anglo-Russian Entente", *Encyclopaedia Britannica*. Retrieved from: https://www.britannica.com/event/Anglo-Russian-Entente (Accessed 13 May 2024).

"Aukus: UK, US and Australia Launch Pact to Counter China", *BBC News*, 15 September 2021. Retrieved from: https://www.bbc.com/news/world-58564837 (Accessed 10 May 2024).

"Be Afraid: Cyberattack in Ukraine Targets Government Websites", *Al Jazeera*, 2022. Retrieved from: https://www.aljazeera.com/news/2022/1/14/be-afraid-cyberattack-in-ukraine-targets-government-websites (Accessed 6 May 2024).

"Britain's Brown Warns Iran It Faces Isolation", *Voice of America*, 2009. Retrieved from: https://www.voanews.com/a/a-13-2008-07-21-voa19/350745.html (Accessed 25 May 2024).

"British Envoy to Tehran Summoned over Publication of "Irresponsible Content"", *The Islamic Republic of Iran Ministry of Foreign Affairs*, 2023. Retrieved from: https://en.mfa.ir/portal/newsview/727024/British-envoy-to-Tehran-summoned-over-publication-of-'irresponsible-content' (Accessed 11 May 2024).

"British Navy's HMS Albion Warned over South China Sea "Provocation"", *BBC News*, 6 September 2018. Retrieved from: https://www.bbc.com/news/uk-45433153 (Accessed 17 May 2024).

"Bucharest Summit Declaration Issued by NATO Heads of State and Government (2008)", *NATO*, 2008. Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_8443.htm (Accessed 28 October 2023).

"Can Huawei Survive an Onslaught of Bans and Restrictions Abroad?", *The Economist*, 15 December 2018. Retrieved from: https://www.economist.com/business/2018/12/15/can-huawei-survive-an-onslaught-of-bans-and-restrictions-abroad (Accessed 19 May 2024).

"Carrie Lam: Hong Kong Extradition Bill Withdrawal Backed by China", *BBC News*, 5 September 2019a. Retrieved from: https://www.bbc.com/news/world-asia-china-49589440 (Accessed 17 May 2024).

"China Complains over British Warship Sailing through Disputed South China Sea", *The Guardian*, 6 September 2018. Retrieved from: https://www.theguardian.com/world/2018/sep/06/china-complains-over-british-warship-sailing-through-disputed-south-china-sea (Accessed 8 May 2024).

"China Says Military Development of Islands within Its Rights", *AP News*, 2022. Retrieved from: https://apnews.com/article/china-beijing-international-law-south-china-sea-4370828e295d2eec9a4804bba9940273 (Accessed 10 May 2024).

"China Tells Britain to Stop Efforts to 'Enhance' Ties with Taiwan", *Reuters*, 9 November 2023a, Retrieved from: https://www.reuters.com/world/china/china-tells-britain-stop-efforts-enhance-ties-with-taiwan-2023-11-09/ (Accessed 10 May 2024).

"China Warns UK Not to Offer Citizenship to Hong Kong Residents", *BBC News*, 23 October 2020a. Retrieved from: https://www.bbc.com/news/world-asia-china-54655285 (Accessed 9 May 2024).

"Chinese Civil War", *Encyclopaedia Britannica*, 2024a. Retrieved from: https://www.britannica.com/event/Chinese-Civil-War (Accessed 16 May 2024).

"CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor", *ABC News*, 2021. Retrieved from: https://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905 (Accessed 30 October 2023).

"Countering Hybrid Threats", *NATO*. Retrieved from: https://www.nato.int/cps/en/natohq/topics_156338.htm (Accessed 22 January 2024).

"Crimea Referendum: Voters "Back Russia Union"", *BBC News*, 16 March 2014a, section Europe. Retrieved from: https://www.bbc.com/news/world-europe-26606097 (Accessed 2 May 2024).

"Cyber Defence", *NATO*, 2023. Retrieved from: https://www.nato.int/cps/en/natohq/topics_78170.htm (Accessed 28 October 2023).

"Department of Commerce Announces the Addition of Huawei to the Entity List", *U.S. Embassy & Consulates in China*, 17 May 2019. Retrieved from: https://china.usembassy-china.org.cn/department-of-commerce-announces-the-addition-of-huawei-to-the-entity-list/ (Accessed 19 May 2024).

"E3 Foreign Ministers' Statement on the JCPoA: 14 January 2020", *United Kingdom Foreign & Commonwealth Office*, 2020. Retrieved from: https://www.gov.uk/government/news/e3-foreign-ministers-statement-on-the-jcpoa-14-january-2020 (Accessed 21 May 2024).

"EU AI Act: First Regulation on Artificial Intelligence", *European Parliament*, 2023. Retrieved from: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence (Accessed 30 May 2024).

"Foreign Affairs Committee (Hong Kong Visit)", *United Kingdom Parliament*, 2 December 2014. Retrieved from: https://hansard.parliament.uk/commons/2014-12-02/debates/14120247000001/ForeignAffairsCommittee(HongKongVisit) (Accessed 8 May 2024).

"Foreign Secretary Condemns Russia's Recognition of Crimea as a "Sovereign State"", *United Kingdom Foreign & Commonwealth Office*, 2014. Retrieved from: https://www.gov.uk/government/news/foreign-secretary-condemns-russias-recognition-of-crimea-as-a-sovereign-state (Accessed 2 May 2024).

"Foreign Secretary Discusses Foreign Policy Priorities and Trade with China", *United Kingdom Foreign & Commonwealth Office*, 2016. Retrieved from: https://www.gov.uk/government/news/foreign-secretary-discusses-foreign-policy-priorities-and-trade-with-china (Accessed 8 May 2024).

"Foreign Secretary Reaffirms UK's Solidarity with Ukraine on Seventh Anniversary of Illegal Annexation of Crimea", *Foreign, Commonwealth & Development Office*, 2021. Retrieved from: https://www.gov.uk/government/news/foreign-

secretary-reaffirms-uks-solidarity-with-ukraine-on-seventh-anniversary-of-illegal-annexation-of-crimea (Accessed 6 May 2024).

"Foreign Secretary Summons Iranian Chargé d'Affaires over Threats to Journalists in the UK", *United Kingdom Foreign & Commonwealth Office*, 2022. Retrieved from: https://www.gov.uk/government/news/foreign-secretary-summons-iranian-charge-daffaires-over-threats-to-journalists-in-the-uk (Accessed 11 May 2024).

"Foreign Secretary Visits China", *United Kingdom Foreign & Commonwealth Office*, 2018a. Retrieved from: https://www.gov.uk/government/news/foreign-secretary-visits-china (Accessed 8 May 2024).

"Foreign Secretary Welcomes Russian Foreign and Defence Ministers to London", *United Kingdom Foreign & Commonwealth Office*, 2013. Retrieved from: https://www.gov.uk/government/news/foreign-secretary-welcomes-russian-foreign-and-defence-ministers-to-london (Accessed 14 May 2024).

"Glossary", *United Kingdom National Cyber Security Centre*, 2023a. Retrieved from: https://www.ncsc.gov.uk/section/advice-guidance/glossary (Accessed 13 November 2023).

"Gray Zone Project", *Center for Strategic & International Studies*. Retrieved from: https://www.csis.org/programs/gray-zone-project (Accessed 4 March 2024).

"Grey zone", *Cambridge Dictionary*, 2024a. Retrieved from: https://dictionary.cambridge.org/tr/s%C3%B6zl%C3%BCk/ingilizce/grey-zone (Accessed 11 February 2024).

"Hackers behind Ukraine Power Cuts, Says US Report", *BBC News*, 26 February 2016, section Technology. Retrieved from: https://www.bbc.com/news/technology-35667989 (Accessed 19 September 2023).

"Hong Kong - Volume 662: Debated on Tuesday 2 July 2019a", *United Kingdom Parliament*, 2 July 2019. Retrieved from: https://hansard.parliament.uk/Commons/2019-07-02/debates/9C7A3D6D-A7B1-42C4-9F3E-65D8C8A4C2EE/HongKong (Accessed 8 May 2024).

"Hong Kong British National (Overseas) Route (Accessible)", *United Kingdom Home Office*, 2024. Retrieved from: https://www.gov.uk/government/publications/hong-kong-british-national-overseas-route/hong-kong-british-national-overseas-route-accessible (Accessed 17 May 2024).

"Hong Kong National Security Law: What Is It and Is It Worrying?", *BBC News*, 22 May 2020b. Retrieved from: https://www.bbc.com/news/world-asia-china-52765838 (Accessed 17 May 2024).

"Hong Kong National Security Legislation: UK Response Volume 676: Debated on Tuesday 2 June 2020", *United Kingdom Parliament*, 2 June 2020. Retrieved from: https://hansard.parliament.uk/Commons/2020-06-

02/debates/C2C22A17-A1BA-4681-8775-346CD69B9BDF/HongKongNationalSecurityLegislationUKResponse (Accessed 9 May 2024).

"Huge Ukraine Rally over EU Agreement Delay", *BBC News*, 24 November 2013. Retrieved from: https://www.bbc.com/news/world-europe-25078952 (Accessed 1 May 2024).

"Hybrid", *Cambridge Dictionary*, 2024b. Retrieved from: https://dictionary.cambridge.org/dictionary/english/hybrid (Accessed 23 February 2024).

"IAEA Mulls Iran Atomic Resolution", *BBC News*, 13 September 2004. Retrieved from: http://news.bbc.co.uk/1/hi/world/middle_east/3650546.stm (Accessed 21 May 2024).

"Internet Resilience", *Internet Society Pulse*. Retrieved from: https://pulse.internetsociety.org/resilience (Accessed 13 June 2024).

"Iran Executes British-Iranian Accused of Spying", *Reuters*, 14 January 2023b, section Middle East. Retrieved from: https://www.reuters.com/world/middle-east/iran-executes-british-iranian-national-akbari-iranian-report-2023-01-14/ (Accessed 11 May 2024).

"Iran Failed to Comply With Nuclear NPT, IAEA Reports", *Arms Control Association*. Retrieved from: https://www.armscontrol.org/act/2003-07/iran-nuclear-briefs/iran-failed-comply-nuclear-npt-iaea-reports (Accessed 25 May 2024).

"Iran Protests "Going Nowhere", Says Mahmoud Ahmadinejad", *BBC News*, 15 February 2011a. Retrieved from: https://www.bbc.com/news/world-middle-east-12475824 (Accessed 21 May 2024).

"Iran Says US Made "new Demands" in Nuclear Talks", *France 24*, 2022. Retrieved from: https://www.france24.com/en/live-news/20220310-iran-says-us-made-new-demands-in-nuclear-talks (Accessed 11 May 2024).

"Iran Summons British Envoy Over Journalist Release Comments", *Iran International*, 2023. Retrieved from: https://www.iranintl.com/en/202308106434 (Accessed 11 May 2024).

"Iran Tests Longest Range Missiles", *BBC News*, 28 September 2009. Retrieved from: http://news.bbc.co.uk/2/hi/middle_east/8278026.stm (Accessed 21 May 2024).

"Iran "Fends off New Stuxnet Cyber Attack"", *BBC News*, 25 December 2012. Retrieved from: https://www.bbc.com/news/world-middle-east-20842113 (Accessed 21 May 2024).

"Iran: A Really Simple Guide to the Protests", *BBC News*, 14 October 2022a. Retrieved from: https://www.bbc.com/news/world-middle-east-63240911 (Accessed 11 May 2024).

"Iranian Embassy Siege", *National Army Museum*, n.d. Retrieved from: https://www.nam.ac.uk/explore/iranian-embassy-siege (Accessed 20 May 2024).

"Iron Curtain Speech", *Encyclopaedia Britannica*, 2024b. Retrieved from: https://www.britannica.com/topic/Iron-Curtain-Speech (Accessed 13 May 2024).

"Israel and Gaza: Ceasefire: Israel and Gaza: Ceasefire Volume 695", *United Kingdom Parliament*, 19 May 2021. Retrieved from: https://hansard.parliament.uk/commons/2021-05-19/debates/B3F55477-09D3-42A0-A2E8-27B9BB6014B4/IsraelAndGazaCeasefire (Accessed 31 May 2024).

"Joint Statement by Defence Secretary Ben Wallace and Ukraine Defence Minister Oleksii Yuriyovych Reznikov", *United Kingdom Ministry of Defence*, 2021. Retrieved from: https://www.gov.uk/government/news/joint-statement-by-defence-secretary-ben-wallace-and-ukraine-defence-minister-oleksii-yuriyovych-reznikov (Accessed 15 May 2024).

"KAVRAM AVCILARI: Siber Saldırı Nedir? - Doç.Dr. Salih Bıçakcı", dir. by *UIK*, 2019. Retrieved from: https://www.youtube.com/watch?v=w_-i3HS9rkk (Accessed 30 November 2023).

"Keynote Speech by NATO Secretary General Jens Stoltenberg at the Opening of the NATO Transformation Seminar", *NATO*, 2015. Retrieved from: http://www.nato.int/cps/en/natohq/opinions_118435.htm (Accessed 25 January 2024).

"Moscow's Relationship with Britain at All-Time Low – Russian Ambassador to UK", *RT International*, 2017. Retrieved from: https://www.rt.com/news/385085-russia-ambassador-uk-relationship/ (Accessed 15 May 2024).

"Opium Wars", *Encyclopaedia Britannica*, 2024c. Retrieved from: https://www.britannica.com/topic/Opium-Wars (Accessed 16 May 2024).

"Oral Answers to Questions - Volume 662: Debated on Wednesday 3 July 2019", *United Kingdom Parliament*, 3 July 2019b. Retrieved from: https://hansard.parliament.uk/commons/2019-07-03/debates/148BA72B-254A-44DE-B840-C7D6115FEDA4/OralAnswersToQuestions (Accessed 9 May 2024).

"Overview on China-UK Relations", *Embassy of the People's Republic of China in UK*, 2010. Retrieved from: http://gb.china-embassy.gov.cn/eng/ChinaUKRelations/introduction/201005/t20100510_3384299.htm (Accessed 16 May 2024).

"PM Call with President Xi on 19 April 2018", *United Kingdom Prime Minister's Office*, 2018. Retrieved from: https://www.gov.uk/government/news/pm-call-with-president-xi-on-19-april-2018 (Accessed 8 May 2024).

"PM Call with President Xi: 25 September 2017a", *United Kingdom Prime Minister's Office*, 2017. Retrieved from: https://www.gov.uk/government/news/pm-call-with-chinese-president-xi-25-september-2017 (Accessed 8 May 2024).

"PM Call with President Zelenskyy of Ukraine: 21 February 2022", *United Kingdom Prime Minister's Office*, 21 February 2022b. Retrieved from: https://www.gov.uk/government/news/pm-call-with-president-zelenskyy-of-ukraine-21-february-2022 (Accessed 7 May 2024).

"PM Call with President Zelenskyy: 5 April 2021", *United Kingdom Prime Minister's Office*, 5 April 2021a. Retrieved from: https://www.gov.uk/government/news/pm-call-with-president-zelenskyy-5-april-2021 (Accessed 6 May 2024).

"PM Leads Largest Ever Trade Delegation to China", *United Kingdom Prime Minister's Office*, 2010a. Retrieved from: https://www.gov.uk/government/news/pm-leads-largest-ever-trade-delegation-to-china (Accessed 16 May 2024).

"PM Meeting with Chinese State Councillor Yang Jiechi: 20 December 2016", *United Kingdom Prime Minister's Office*, 20 December 2016. Retrieved from: https://www.gov.uk/government/news/pm-meeting-with-chinese-state-councillor-yang-jiechi-20-december-2016 (Accessed 8 May 2024).

"PM Meeting with Prime Minister Netanyahu: 2 November 2017", *United Kingdom Prime Minister's Office*, 2017b. Retrieved from: https://www.gov.uk/government/news/pm-meeting-with-prime-minister-netanyahu-2-november-2017 (Accessed 31 May 2024).

"PM Reaffirms the UK's Staunch Commitment to Ukraine's Sovereignty", *United Kingdom Prime Minister's Office*, 8 October 2020. Retrieved from: https://www.gov.uk/government/news/pm-reaffirms-the-uks-staunch-commitment-to-ukraines-sovereignty (Accessed 6 May 2024).

"PM Speech at Balfour Centenary Dinner", *United Kingdom Prime Minister's Office*, 2 November 2017c. Retrieved from: https://www.gov.uk/government/speeches/pm-speech-at-balfour-centenary-dinner (Accessed 31 May 2024).

"PM Statement at Ukraine Press Conference: 1 February 2022a", *United Kingdom Prime Minister's Office Press Release*, 1 February 2022. Retrieved from: https://www.gov.uk/government/speeches/pm-statement-at-ukraine-press-conference-1-february-2022 (Accessed 7 May 2024).

"Press Conference by NATO Secretary General Jens Stoltenberg Following the Meeting of the NATO-Russia Council", *NATO*, 2022b. Retrieved from: https://www.nato.int/cps/en/natohq/opinions_190666.htm (Accessed 15 May 2024).

"Press Conference: The Prime Minister and President Vladimir Putin", *United Kingdom Prime Minister's Office*, 16 June 2013. Retrieved from:

https://www.gov.uk/government/speeches/press-conference-the-prime-minister-and-president-vladimir-putin (Accessed 14 May 2024).

"Prime Minister Deploys UK Military to Eastern Mediterranean to Support Israel", *United Kingdom Prime Minister's Office*, 13 October 2023. Retrieved from: https://www.gov.uk/government/news/prime-minister-deploys-uk-military-to-eastern-mediterranean-to-support-israel (Accessed 11 May 2024).

"Prime Minister: "We Want a Strong Relationship with China"", *United Kingdom Prime Minister's Office*, 10 November 2010b. Retrieved from: https://www.gov.uk/government/speeches/prime-minister-we-want-a-strong-relationship-with-china (Accessed 16 May 2024).

"Read the Full Transcript of Trump's Speech on the Iran Nuclear Deal", *The New York Times*, 8 May 2018. Retrieved from: https://www.nytimes.com/2018/05/08/us/politics/trump-speech-iran-deal.html (Accessed 10 May 2024).

"Readiness Action Plan", *NATO*. Retrieved from: https://www.nato.int/cps/en/natohq/topics_119353.htm (Accessed 2 February 2024).

"Russia Says Stuxnet Could Have Caused New Chernobyl", *The Moscow Times*, 2011. Retrieved from: https://www.themoscowtimes.com/2011/01/26/russia-says-stuxnet-could-have-caused-new-chernobyl-a4553 (Accessed 19 September 2023).

"Russian Spy Poisoning: What We Know so Far", *BBC News*, 7 March 2018. Retrieved from: https://www.bbc.com/news/uk-43315636 (Accessed 6 May 2024).

"Service Personnel (Ukraine)", *United Kingdom Parliament*, 2015a. Retrieved from: https://hansard.parliament.uk/commons/2015-02-25/debates/15022591000002/ServicePersonnel(Ukraine) (Accessed 6 May 2024).

"Significant Cyber Incidents", *Center for Strategic and International Studies*, 2023. Retrieved from: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (Accessed 24 October 2023).

"Stuxnet: Computer Worm Opens New Era of Warfare", *CBS News*, 2012. Retrieved from: https://www.cbsnews.com/news/stuxnet-computer-worm-opens-new-era-of-warfare-04-06-2012/ (Accessed 19 September 2023).

"Syria Conflict: "Chemical Attack" in Idlib Kills 58", *BBC News*, 4 April 2017, section Middle East. Retrieved from: https://www.bbc.com/news/world-middle-east-39488539 (Accessed 15 May 2024).

"Taiwan, UK Sign Milestone Trade Partnership Pact", *Taiwan Today, Ministry of Foreign Affairs, Republic of China (Taiwan)*, 2023. Retrieved from:

https://taiwantoday.tw/news.php?unit=2&post=244501 (Accessed 10 May 2024).

"The UK and China: A Framework for Engagement Volume 486: Debated on Thursday 22 January 2009", *United Kingdom Parliament*, 2009. Retrieved from: https://hansard.parliament.uk/Commons/2009-01-22/debates/09012247000018/TheUKAndChinaAFrameworkForEngagement (Accessed 18 May 2024).

"Tibet Volume 481: Debated on Wednesday 29 October 2008", *United Kingdom Parliament*, 2008. Retrieved from: https://hansard.parliament.uk/commons/2008-10-29/debates/08102940000010/Tibet (Accessed 16 May 2024).

"Tracking State-Sponsored Cyberattacks Around the World", *Council on Foreign Relations*, 2023. Retrieved from: https://www.cfr.org/cyber-operations (Accessed 24 October 2023).

"U.K. Condemns Russian Decision on Spy Murder Suspect", *Reuters*, 9 August 2007. Retrieved from: https://www.reuters.com/article/idUSL1078261/ (Accessed 14 May 2024).

"UK and Allies Reveal Global Scale of Chinese Cyber Campaign", *United Kingdom Foreign & Commonwealth Office*, 2018b. Retrieved from: https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign (Accessed 8 May 2024).

"UK and China Relationship "Seriously Poisoned", Says Beijing's Ambassador", *BBC News*, 30 July 2020c. Retrieved from: https://www.bbc.com/news/uk-politics-53595423 (Accessed 10 May 2024).

"UK Announces Plans to Join Asian Infrastructure Investment Bank", *United Kingdom HM Treasury*, 2015a. Retrieved from: https://www.gov.uk/government/news/uk-announces-plans-to-join-asian-infrastructure-investment-bank (Accessed 8 May 2024).

"UK Celebrates 45th Anniversary of Full Diplomatic Relations with China", *British Embassy Beijing*, 2017. Retrieved from: https://www.gov.uk/government/news/uk-celebrates-45th-anniversary-of-full-diplomatic-relations-with-china (Accessed 16 May 2024).

"UK Launches Multinational Training to Enhance Ukrainian Navy against Threats from the East", *United Kingdom Ministry of Defence*, 2020. Retrieved from: https://www.gov.uk/government/news/uk-launches-multinational-training-to-enhance-ukrainian-navy-against-threats-from-the-east (Accessed 15 May 2024).

"UK Severs Ties with Iranian Banks", *BBC News*, 21 November 2011b. Retrieved from: https://www.bbc.com/news/uk-politics-15823622 (Accessed 21 May 2024).

"UK Signs Founding Articles of Agreement of the Asian Infrastructure Investment Bank", *United Kingdom HM Treasury*, 2015b. Retrieved from: https://www.gov.uk/government/news/uk-signs-founding-articles-of-agreement-of-the-asian-infrastructure-investment-bank (Accessed 17 May 2024).

"UK to Expel All Iranian Diplomats over Embassy Attack", *BBC News*, 30 November 2011c. Retrieved from: https://www.bbc.com/news/uk-politics-15966628 (Accessed 21 May 2024).

"UK-China Joint Statement 2015", *United Kingdom Foreign & Commonwealth Office*, 2015. Retrieved from: https://www.gov.uk/government/news/uk-china-joint-statement-2015 (Accessed 8 May 2024).

"Ukraine and Pro-Russia Rebels Sign Ceasefire Deal", *BBC News*, 5 September 2014b. Retrieved from: https://www.bbc.com/news/world-europe-29082574 (Accessed 2 May 2024).

"Ukraine Crisis: Protesters Declare Donetsk "Republic"", *BBC News*, 7 April 2014c. Retrieved from: https://www.bbc.com/news/world-europe-26919928 (Accessed 2 May 2024).

"Ukraine Says Russia Has Nearly 100,000 Troops near Its Border", *Reuters*, 13 November 2021. Retrieved from: https://www.reuters.com/world/europe/ukraine-says-russia-has-nearly-100000-troops-near-its-border-2021-11-13/ (Accessed 7 May 2024).

"Ukraine-Russia Crisis: What Is the Minsk Agreement?", *Al Jazeera*, 2015. Retrieved from: https://www.aljazeera.com/news/2022/2/9/what-is-the-minsk-agreement-and-why-is-it-relevant-now (Accessed 14 May 2024).

"Ukraine: Operation Orbital", *United Kingdom Parliament*, 2015b. Retrieved from: https://questions-statements.parliament.uk/written-statements/detail/2015-10-12/HCWS218 (Accessed 6 May 2024).

"Ukraine: Putin Signs Crimea Annexation", *BBC News*, 21 March 2014d. Retrieved from: https://www.bbc.com/news/world-europe-26686949 (Accessed 2 May 2024).

"Ukraine: Russia Recalls Ambassador as Kiev Turns towards EU", *BBC News*, 24 February 2014e. Retrieved from: https://www.bbc.com/news/world-europe-26318816 (Accessed 2 May 2024).

"US and UK Issue Sanctions on Iran One Year on from Mahsa Amini's Death", *The Guardian*, 15 September 2023. Retrieved from: https://www.theguardian.com/world/2023/sep/15/us-and-uk-issue-sanctions-on-iran-one-year-on-from-mahsa-aminis-death (Accessed 11 May 2024).

"US Sends Aircraft Carrier and Bomber Task Force to "Warn Iran"", *BBC News*, 6 May 2019b. Retrieved from: https://www.bbc.com/news/world-us-canada-48173357 (Accessed 17 October 2023).

"Wales Summit Declaration Issued by NATO Heads of State and Government", *NATO*, 2014. Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_112964.htm (Accessed 20 January 2024).

"What Are the Minsk Agreements on the Ukraine Conflict?", *Reuters*, 21 February 2022. Retrieved from: https://www.reuters.com/world/europe/what-are-minsk-agreements-ukraine-conflict-2022-02-21/ (Accessed 2 May 2024).

"What Are the Sanctions on Russia and Have They Affected Its Economy?", *BBC News*, 27 January 2022b. Retrieved from: https://www.bbc.com/news/world-europe-60125659 (Accessed 15 May 2024).

"What is a DDoS Attack? - DDoS Meaning", *Kaspersky*, 2023. Retrieved from: https://www.kaspersky.com/resource-center/threats/ddos-attacks (Accessed 30 November 2023).

"What Is a Distributed Denial-of-Service (DDoS) Attack?", *Cloudflare*, 2023. Retrieved from: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (Accessed 30 November 2023).

"What's the Context? Foundation of the German Empire, 18 January 1871", *United Kingdom National Archives*, 2021. Retrieved from: https://history.blog.gov.uk/2021/01/20/whats-the-context-foundation-of-the-german-empire-18-january-1871/#_ftn1 (Accessed 13 May 2024).

Datasets

BOSCHEE, Elizabeth, Jennifer LAUTENSCHLAGER, Sean O'BRIEN, Steve SHELLMAN, James STARZ, and Michael WARD, "*Integrated Crises Early Warning System Coded Event Data*", Harvard Dataverse, 2023, https://doi:10.7910/DVN/28075

MCCLELLAND, Charles, "*World Event/Interaction Survey, 1966-1978*", Inter-university Consortium for Political and Social Research, 2006. https://doi.org/10.3886/ICPSR05211.v3.

SCARBOROUGH, Grace I., Benjamin E. BAGOZZI, Andreas BEGER, John BERRIE, Andrew HALTERMAN, Philip A. SCHRODT, Jevon SPIVEY, "*POLECAT Documentation*", Harvard Dataverse, 2023, https://doi:10.7910/DVN/LMFPIP

VALERIANO, Brandon, "*Dyadic Cyber Incident Dataset v2.0*", Harvard Dataverse, 2022, https://doi:10.7910/DVN/CQOMYV

"*Global Database of Events, Language, and Tone (GDELT) Project*", https://www.gdeltproject.org/data.html

"*NETSCOUT Cyber Threat Horizon*" https://horizon.netscout.com/?atlas=summary

"*Tracking State-Sponsored Cyberattacks Around the World*", Council on Foreign Relations, 2023, https://www.cfr.org/cyber-operations

Conference Papers & Presentations

DAVIES, John," All in the Lifetime of a Millennial: The Juxtaposition between Cyber Operations and Cyber Warfare", *EUACADEMY Conference "European Security: Challenges and Policies*, Online, 14 December 2023.

ELMRABIT, Nebrase, Feixiang ZHOU, Fengyin LI, and Huiyu ZHOU, "Evaluation of Machine Learning Algorithms for Anomaly Detection", *International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, Dublin, Ireland: 2020, pp. 1–8, https://*doi:10.1109/CyberSecurity49315.2020.9138871*

GERNER, Deborah J., Rajaa ABU-JABR, Philip A. SCHRODT, and Ömür YILMAZ. "Conflict and Mediation Event Observations (CAMEO): A New Event Data Framework for the Analysis of Foreign Policy Interactions", *The Annual Meeting of the International Studies Association*, New Orleans, United States of America: 2002, Retrieved from: https://parusanalytics.com/eventdata/papers.dir/gerner02.pdf

JENSEN, Benjamin, and Brandon VALERIANO, "Cyber Escalation Dynamics: Results from War Game Experiments", International Studies Association, Annual Meeting Panel: War Gaming and Simulations in International Conflict, Toronto, Ontario, Canada: March 27, 2019, Retrieved from: http://web.isanet.org/Web/Conferences/Toronto%202019-s/Archive/71e7820c-e61c-4187-ab8c-28de83dfd660.pdf

LEETARU, Kalev, and Philip A. SCHRODT. "GDELT: Global Data on Events, Location and Tone", *The Annual Meeting of the International Studies Association*, San Francisco, United States of America: April 2013, Retrieved from: http://data.gdeltproject.org/documentation/ISA.2013.GDELT.pdf

LIU, Fei Tony, Kai Ming TING, and Zhi-Hua ZHOU, "Isolation Forest", *The 2008 Eighth IEEE International Conference on Data Mining*, Pisa, Italy: 2008, pp. 413-422, https://doi:10.1109/ICDM.2008.17

OTTIS, Rain. "Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective", *The Proceedings of the 7th European Conference on Information Warfare and Security*, Reading: Academic Publishing Limited, 2008, pp. 163–68. Retrieved from: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

SOKOLIUK, Anton, Galyna KONDRATENKO, Ievgen SIDENKO, Yuriy KONDRATENKO, Anatoly KHOMCHENKO, and Igor ATAMANYUK. "Machine Learning Algorithms for Binary Classification of Liver Disease," *The 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology*, Kharkiv, Ukraine: 2020, pp. 417–21 https://doi.org/10.1109/PICST51311.2020.9468051

Dissertations & Theses

Nemeth, William J., **"Future War and Chechnya : A Case for Hybrid Warfare",** Master's Thesis, Monterey, CA: Naval Postgraduate School, 2002, Retrieved from: https://core.ac.uk/download/36699567.pdf

Jensen, Theodore, **"Restricted Hybrid Warfare: Confining the Gray Zone Debate",** Master's Thesis, Harvard Extension School, 2019, Retrieved from: https://dash.harvard.edu/handle/1/37364566

Walker, Robert G., **"SPEC FI: The United States Marine Corps and Special Operations"**, Master's Thesis, Monterey, CA: Naval Postgraduate School, 1998, Retrieved from: https://apps.dtic.mil/sti/pdfs/ADA359694.pdf

TEZ ONAY SAYFASI

Üniversite	: T.C. GALATASARAY ÜNİVERSİTESİ
Enstitü	: SOSYAL BİLİMLER ENSTİTÜSÜ
Hazırlayanın Adı Soyadı	: Atakan YILMAZ
Tez Başlığı	: Cyber Tools as Foreign Policy Instruments in Trilateral Relations: Analysing Cyber-Attacks Targeting the United Kingdom
Savunma Tarihi	: 10 / 07 / 2024
Danışman	: Doç. Dr. Menent SAVAŞ CAZALA

JÜRİ ÜYELERİ:

Unvan, Ad-Soyadı İmza

Doç. Dr. Menent SAVAŞ-CAZALA

Doç. Dr. Ali Faik DEMİR

Prof. Dr. Ebru Şule CANAN-SOKULLU

Dr. Öğr. Üyesi Tolga BİLENER

Dr. Öğr. Üyesi Ethem İLBİZ

Prof. Dr. Ulun AKTURAN
Enstitü Müdürü