UNIVERSITY OF WROCŁAW

FACULTY OF SOCIAL SCIENCE

INSTITUTE OF INTERNATIONAL STUDIES

MASTER THESIS

NAVIGATING THE CHANGING LANDSCAPE OF CROSS-BORDER TERRORISM: ASSESSING INTERNATIONAL COUNTER-TERRORISM COOPERATION IN THE FACE OF NEWLY EMERGING THREATS

BAŞAK DALGIN

PROF. JAROSŁAW JARZĄBEK

WROCŁAW, POLAND

31.07.2023

THIS PAGE IS LEFT BLANK INTENTIONALLY

NAVIGATING THE CHANGING LANDSCAPE OF CROSS-BORDER TERRORISM: ASSESSING CROSS-BORDER COUNTER-TERRORISM COOPERATION IN THE FACE OF NEWLY EMERGING THREATS

KEYWORDS: Counter-Terrorism Cooperation, Cross-Border Terrorism, Transnational Extremist networks, Online Radicalization, Lone Wolf Attacks, Emerging Technologies, Terrorism Financing, Cyberterrorism

RESEARCH OBJECTIVES

1. Analyze the newly emerging cross-border threats in the realm of terrorism, including transnational extremist networks, online radicalization, lone wolf attacks, emerging technologies, Financing methods, cyberterrorism, CBRN terrorism, and Hybrid threats.
2. Assess the effectiveness of current cross-border counter-terrorism cooperation frameworks in addressing newly emerging threats in cross-border terrorism.
3. Identify the challenges and obstacles faced in countering newly emerging threats and evaluate their impact on international cooperation efforts.
4. Explore opportunities for adapting and strengthening international counter-terrorism cooperation to effectively address newly emerging cross-border threats, including the role of technology, regional partnerships, public-private collaborations, and hybrid threat responses.
5. Evaluate the strengths and weaknesses of existing cooperative frameworks and mechanisms in addressing newly emerging threats.

I. Introduction

ABSTRACT

This thesis aims to navigate the changing landscape of cross-border terrorism by assessing international counter-terrorism cooperation in the face of newly emerging threats. The research analyzes the development of international terrorist threats and identifies the new dangers posed by transnational extremist networks, cyberterrorism, CBRN terrorism, hybrid threats, online radicalization, lone wolf attacks, and emerging technology. It assesses the efficacy of present frameworks for international collaboration and examines the advantages and disadvantages of existing platforms for cooperation. The study also examines the difficulties and barriers faced in addressing recently emerged concerns, such as jurisdictional issues, disparate national priorities, resource limitations, and technology difficulties. Additionally, it looks into ways to improve cooperation, including boosting regional alliances, enhancing public-private partnerships, and fortifying legal frameworks. The study concludes with policy recommendations to enhance international cooperation in countering newly emerging international terrorism threats.

RATIONALE

Terrorism that crosses borders is a serious danger to world stability and security. An assessment of global counterterrorism cooperation is required due to the evolving nature of these threats, which are characterized by the appearance of new and complex forms of terrorism. It is essential to comprehend how cross-border terrorism is changing in order to develop effective defenses against recently discovered threats. The need to evaluate the efficiency of current cooperative arrangements and pinpoint areas for development is what spurred this research. This study aims to contribute to the creation of comprehensive and proactive approaches to global counterterrorism efforts by assessing difficulties encountered in addressing recently emerging threats and investigating prospects for increased cooperation. The findings and policy recommendations of this research will provide valuable insights to policymakers, practitioners, and scholars in the field of counter-terrorism, ultimately contributing to the global fight against terrorism.

RESEARCH METHODOLOGY

This study's research methodology uses a mixed-methods strategy that combines qualitative and quantitative research techniques. It starts off with a thorough analysis of the body of research on cross-border terrorism, frameworks for international counterterrorism cooperation, and recently emerged threats. Understanding the research topic and finding knowledge gaps is based on the literature review. Document analysis and content analysis of relevant reports, policy papers, and academic publications are part of the qualitative data collection process. These resources offer insightful information on the difficulties, possibilities, and efficiency of international cooperation in countering newly developing threats. To find patterns, themes, correlations, and trends, the obtained qualitative and quantitative data will be evaluated using thematic analysis and case studies, respectively. Comparative analysis will be conducted to evaluate the effectiveness of existing international cooperation frameworks by examining case studies and comparing different approaches. Finally, based on the research findings, policy recommendations will be formulated to enhance international cooperation in countering newly emerging cross-border terrorism threats. This research methodology provides a comprehensive and rigorous approach to addressing the research objectives without relying on interviews.

1. Literature Review

1.1. Cross-border Terrorism vs. International Terrorism: Definitions and characteristics

As our world changes, traditional security threats also evolve and develop. Terrorism has always been one of the constantly changing threats to global security. Today, the concepts of "cross-border terrorism" and "international terrorism" pose significant challenges to 21st-century global security understanding and necessitate practical international counter-terrorism cooperation. In an increasingly interconnected world, the threat landscape is changing every day, with newly emerging forms of inter and cross-national terrorism presenting unique complexities. The questions we should answer first are: What are cross-border terrorism and international terrorism and what is the difference? Although they are related and often used interchangeably they have crucial differences for this thesis. International terrorism is the act of terrorism that involves different terrorist groups or terrorist organizations from multiple countries. These acts are planned and executed by terrorists across one or multiple national boundaries. Terror attacks can be designed and executed by citizens of one country with the collaboration of people from other countries' citizens or they can operate these attacks in multiple countries simultaneously (Ganor, 2002). The key characteristic of international terrorism is the involvement of people, and groups from various countries. In contrast, the act of cross-border terrorism originates only in one country and directs toward another particular country. It is often seen in regions with weak governance, and ethnic or religious tension, and the objective groups aim to harm or destabilize the target country with their attacks. Albeit aiming to create fear, using violence to harm the target can be seen as a common trait of terrorism in general The most distinguishing factor is the geographical scope and the actors involved in the difference between international and cross-border terrorism (Badey, 1998). It can be useful to note that as the difference is not clear-cut they can overlap from time to time. Some of the acts and attacks of cross-border terrorism can be considered international terrorism as they evolve for example if they choose to collaborate with groups or people from different nationalities. Thus the motivation and objectives should be calculated and analyzed carefully to forecast their tactics as strategies

To counter terrorism, the first step is to know the concept of cross-border terrorism. Cross-border terrorism has distinguished characteristics that need special attention and care from law enforcement to take into delicate consideration. The first one is the ability of the groups to operate transnational operations. Terrorist groups or organizations that can perform cross-border operations are most noticeably known for their ability to plan, coordinate, and

execute their terrorist activities across their national border. To make their operations easier, terrorist organizations can use open borders, smuggling routes, and safe havens in other nations (Hoffman, 1999). The exploitation of safe havens is another important characteristic of these groups. They generally choose governments that are poorly governed or ungoverned to establish safe havens. These havens allow or facilitate them to organize and conduct their attacks from across the border they are in as well as escaping from security forces. Support networks are one of the important tools they use. They enable terrorist groups to establish logistical systems but more importantly recruitment and funding. These networks are being formed with the efforts of individuals who sympathize with the group's aim or cause in different countries. Recruitment is the backbone of every terror organization in the world. Without an audience and followers, a terrorist group can't exist. That's why forming online platforms and social networks is important for international recruitment. Utilizing social media and online platforms to connect with potential supporters and attract people from different nations to their cause is an important part of cross-border terrorism. They mostly succeed in connecting with people by exploiting ethnic, religious, or ideological divisions to incite violence (Hoffman, 1999). Another backbone is of course economic support. To acquire financial support and resources, they use mostly unlawful ways such as the movement of funds, weapons, and drugs. Terrorist groups engage in illegal activity, take advantage of flaws in financial institutions, and look to outside sources of financing to support their operations (Freeman, 2013). Understanding these characteristics is very important to form effective counter-terrorism strategies internationally and fostering collaboration among nations to guard global security.

1.2. Evolution of cross-border terrorism threats

As we mentioned terrorism and countering terrorism have been some of the challenges to national and international security. As the understanding of international security changed threats also evolved alongside. Terrorist organizations can easily adapt themselves to this changing environment and have become "learning organizations" by altering their patterns of behavior in an environment in which they hold an asymmetric position compared to states that are legitimate actors that possess larger human resources as well as wider inventories (Dumankaya & Yalçınkaya, 2022). Technology is the biggest influence on our changing environment. It become an inseparable part of our lives but it also become the biggest threat in some cases. This forced us to reevaluate how terror organizations might use the tools and to

what extent they can reach out to people or even the government to affect the already unstable situations in countries or between groups. Unfortunately, improving many technological means is not always on our side when it comes to countering terrorism. So, how have these threats evolved? Not surprisingly the emergence of Al-Qaeda stands as a turning point in this case as they are one of the pioneer terrorist groups performing on a global scale and cross-border attacks. The turning point for cross-border terrorism was the 9/11 attacks in 2001. The attack was and still is proof that terror organizations are capable of carrying out attacks on a global scale. These attacks caused a fundamental shift in the understanding of international terrorism and countering it (O'Brien, 2011). But what we will discuss mostly in this thesis is more relevant to the advancement of technology. Online platforms started to be used to recruit and radicalize people from across the globe and offered them reliable platforms to meet and communicate with already radicalized people. It became much easier for geographically extremist people and groups to coordinate and enabled them to spread their radical ideology (Ferrara, 2017). Regardless of the difficulty in pointing out the exact moment they started shifting, we should be able to evaluate how these threats evolved and what triggered this change. As we saw in the fall of the Soviet Union or the Arab Uprising, immense and prompt changes in the geopolitical dynamics affected the change of the threats. Political boundaries, territorial disputes, and conflicts between nations necessitate a more sensitive approach to cross-border terrorism (Hoffman, 1999). Maybe the most drastic change came with the technological advancement of the new century. Alongside the internet and social media, we mentioned earlier that advancements in transportation and communication technologies contributed to terror groups logistically, especially between international borders. Financing methods are also affected by the radical advancement of technology. Cryptocurrency technology stands as a serious threat to law enforcement in fighting funding terrorism. This new technology provides an anonymous and decentralized method for exchanging money. They are used primarily for fundraising, donation, or illicit transactions. The nature of cryptocurrency fits perfectly with terrorist groups' need for tacitness. New ways of funding terror organizations are one of the crucial threats of this century (Dumankaya & Yalçınkaya, 2022). This topic will be evaluated deeper in the coming chapters. Over time tactic and strategy of these groups has also evolved. They adapted themselves, their attacks to the changing needs of our time and current political vulnerabilities. They have improved their ability to take advantage of gaps in border security by employing strategies like an infiltration, the smuggling of explosives and weapons, and recruiting local supporters. Among all these physical changes, we can also observe a shift in the ideology of terror groups. The change from separatist to

transnational extremism such as Salafism and Jihadism is a serious result of the global spread of cross-border terrorism. Understanding these threats and their evolution over time is crucial to fight with them (Crenshaw, 2020). All these factors created a need to better and increase international cooperation for countering both international and cross-border terrorism. The increase in intelligence sharing, law enforcement collaboration, and diplomatic efforts are indisputably needed to fight these groups.

1.3. Newly emerging threats in cross-border terrorism

As we mentioned the characteristics of cross-border terrorism and the nature of evolving these threats this chapter will focus on eight important up-to-date threats of cross-border terrorism. These threats are transnational extremist networks, online radicalization, lone wolf attacks, emerging technologies, financing methods, cyberterrorism, CBRN terrorism, and hybrid threats. This section will explore each of the eight threats in depth. It is important to understand and evaluate these new threats as they pose a greater threat than conventional terror acts in the context of both national and international security. Only by understanding and correctly interpreting the innovative tactics of terror groups we can conduct effective counter-terror strategies and be ahead of the terrorist groups. I want to explain why and how these threats are more dangerous than conventional methods before diving into the threats themselves. First and foremost is the global impact. With these newly formed threats, the impact of terrorist attacks has risen drastically. Due to the nature of the globalized world, a terrorist attack or activity can affect other neighboring or any other countries, or even the whole region on a breakneck. The 9/11 attacks in 2001 changed the course of world history, The 2015 Paris Attacks changed the European Union's whole agenda on terrorism and became a wake-up call for the whole world again. Each case again showed us the impact of the interconnectedness of the world and how terrorist attacks go beyond the targeted country (Coolsaet, 2016) Unlike past threats, the weapons and harmful materials used in the new area can potentially cause mass casualties and human crises. Using chemical, biological, radiological, and nuclear materials has serious threats of mass destruction and long-term environmental consequences. Lastly, international terrorist attacks can have serious socioeconomic consequences. They have the power to create fear and result in losing people's confidence in democratic institutions, interfere with daily life and business, and create deep societal disagreement (Dumankaya & Yalçınkaya, 2022). Thus, recognizing these threats is more important than ever before. Policymakers, law enforcement bodies, and researchers can

gain a deep understanding of the developing strategies, objectives, and capabilities of terrorist organizations by investigating these threats deeply. In an increasingly connected world, this knowledge is the basis for creating effective counterterrorism policies, fostering international cooperation, and preserving global security and stability.

1.3.1. Transnational extremist networks

The first threat that emerged lately is transnational extremist networks. These groups are interconnected organizations that share a common goal, are mostly extremist, and perform across national borders. They can be characterized by most importantly their ability to recruit members from different countries, mobilize their resources internationally, and perform their attacks in the countries crossing their national borders (Ferrera, 2017). Their decentralized and fluid character makes it harder for law enforcement to detect and intervene in these organizations' activities. When we talk about transnational extremism, one of the first organizations we think of is probably Al-Qaeda. Al-Qeda is an ideology-based terrorist group aiming to establish a global caliphate. Since its establishment in 1988 in Pakistan the group performed many terrorist attacks across the works. The way the group operates is through regional affiliates and cells that constantly change but never without a central base. This is how they organize and carry out the attacks which makes it harder for them to be followed and identified (Coolsaet, 2016). Another transnational extremist organization is the Islamic State of Iraq and Syria (ISIS). Having emerged in the early 2010s ISIS quickly became the most influential terrorist organization in the world. They took control over big territories in Iraq and Syria. They recruited thousands of people from all around the world mostly by using their social media platforms by spreading their extremist Islamic ideology (Ferrera, 2017). Even though it lost most of its influence in the territories it still poses a threat through its global networks of sympathizers and affiliates around the world. As we see in the examples of ISIS and Al-Qaeda, transnational extremist networks rely mostly on multiple sources based internationally to support their operations. These can be from illicit activities such as drug and human trafficking, and kidnapping as well as from their social and economic circles (Freeman, 2013) Thus, countering transnational extremist networks requires coordinated and multifaceted approaches as well as breaking the influence of the local communities that have the potential to support these networks. Moreover, countering these particularly transnational extremist networks comes with disadvantages that make it more difficult to fight with and they pose great importance for detecting and countering these networks. One of the greatest challenges of

countering transnational extremist networks is their ability to adapt and evolve to the time and necessities of the place they exist. Their decentralized nature makes it easy to change or shift their centers, leaders, tactics, and strategies very quickly in the need of counter-action (Ferrara, 2017). As we mentioned nature makes it harder for law enforcement to follow up on their strategies. Additionally, it is difficult to monitor and follow their activities due to their use of social media and encrypted communication platforms. Also, transnational extremist networks have a global reach as they are highly skilled at using Internet platforms to spread their ideas and recruit people worldwide. These networks can broadcast propaganda and contact prospective recruits almost safely on the internet (Ferrara, 2017). Lastly, they can mobilize their resource internationally by using multiple means of illicit activities that need high intentional cooperation to fight with.

1.3.2. Online Radicalization

The role of digital media exists in every aspect of our lives in today's world. As it is very common its capacity to reach people makes it one of the concerns of terrorists as well. As we mentioned earlier social platforms and the internet provided extremist groups and terror organizations with a safe and undercover platform to perform most of their activities. Online radicalization refers to the process by which individuals are exposed to extremist ideologies and are influenced to adopt and support these ideologies through online platforms. It is the process of spreading extremist propaganda, recruitment tactics, and the creation of an online community to support their case. (Ferrara, 2017). The internet gives people a stage to access and interact with extremist material, meet and find other people with the same ideology and opinion, and take part in online forums and social media sites that help extremism spread (Wojcieszak, 2010). We can define online radicalization with several key features.

First to mention, similar to transnational extremist networks, the free and diversified process internet offers easy access to extremist content and gives space to radicalization without direct or physical contact with extremist or terror organizations as well as making it very difficult for law enforcement to track and monitor their actions. Another point is the anonymity problem that comes naturally with the internet culture such as using nicknames. With this anonymity provided by the internet, people are more likely to engage in radical activities without the fear of being discovered or having to bear any consequences, that result in growing online radicalization. Third and maybe the most effective one when it comes to countering cross-border terrorism is the possibility and escalation of spreading extremist

propaganda and recruiting as targeting parties can reach a large audience and potentially influence weaker people (Wojcieszak, 2010). We can mention several reasons and factors that affect online radicalization but the most significant one is being in an echo chamber and filter bubbles. That refers to being exposed to a limited range of information that is compatible with the opinions and mindset targeted people have already exposed in their daily life or ones that are easy to adapt to their lifestyle or characters (Wojcieszak, 2010). Extremist ideas may be strengthened and consolidated as a result of these. Additionally, the Internet gives those who might feel alone or unattached from their community a sense of connection and belonging, making them more vulnerable to radicalization. Additionally, extremist groups can more easily target and attract susceptible people due to their anonymity and accessibility of the Internet (Wojcieszak, 2010). For counterterrorism measures, the rise of internet radicalization creates many difficulties. The physical monitoring and intelligence gathering used in conventional counterterrorism methods may not be sufficient to fight the online aspect of radicalization (Ferrara, 2017). To prevent vulnerable people from becoming radicalized, authorities must implement effective techniques to monitor online extremist networks, identify and counter extremist material, and interact with vulnerable people. And of course, international collaboration is crucial to to address the challenges posed by online radicalization and to ensure safety.

1.3.3. Lone Wolf Attacks

Lone Wolf attacks have become one of the most important and dangerous threats of the new face of cross-border terrorism. What makes different lone wolves is their independence from terrorist organizations. Because they operate alone tracking and preventing the act is very difficult. They plan the act without guidance or support from a network or organization, based solely on their motivations and ideologies (Spaaij, 2010). The rise of the lone wolf attack presented many difficulties in countering cross-border terrorism. Unlike traditional terror attacks, lone wolves do not communicate with other members and operate under the radar which makes it difficult to identify and prevent their attack. Lone wolf attacks can be defined as acts of violence carried out by individuals who are not directly affiliated with any terrorist organization but are inspired by their ideologies (Spaaij, 2010). Lone wolf attackers frequently have certain traits that distinguish them from conventional terrorist groups. They might have undergone a radicalization process before in their life, which make it easier for them to embrace extreme ideologies and ideas. Or they might experience a sense of alienation from the society

they live with which might affect their decisions on committing violent acts. Another common characteristic of lone wolf attackers is the desire to be recognized and take revenge. Understanding these common characteristics and motivations is important to counter their strategy and potential attacks. Research shows that ideological actions, personal grudges, and a need for attention are the most seen traits of lone-wolf attackers. The attackers' motivations can be different from each other. Some can be motivated by ideological opinions and actions others can be motivated by political or religious or some can be due to their personal grudge like anger or resentment from the injustices they experienced to apply volience to reach their goals. The desire to be recognized and be famous for their action, no matter if it is positive or negative can also be a significant motivation as terrorists' especially the lone wolf attackers' biggest desire is to draw attention to and create a mark or create a fear with their deadly attacks (Spaaij, 2010).

As in the other forms of threats mentioned previously, radicalization and its process an important factors in the emergence of a lone wolf attacker. Radicalization can be defined as the process of embracing violent ideology and beliefs throughout a specific period of time. On the other hand, online radicalization is a significant facilitator that gives potential lone wolves access to extremist ideology and propaganda. It also creates a platform for finding other like-minded individuals and, as a result, poses the risk of an attack without any direct ties to recognized terrorist groups. So the key to stopping lone-wolf terror acts is to comprehend and stop people from becoming radicalized online. We can categorize the radicalization process into many stages for better analysis. Exposure to extreme propaganda is the initial stage. This occurs primarily through personal interactions with radical individuals or groups or through internet platforms, usually from someone the victim trusts. This exposure may encourage people to identify and resonate with the extreme ideology that is presented by the radicalizing channel. What is dangerous is the moment this radicalization gives them a sense of belonging and self-identification. Accepting and internalizing the radical belief comes as the next phase. Many things, including insecurities about oneself, grudges, and a search for meaning or purpose, might have an impact on this. People become increasingly disengaged from the realities of their societies and environment, which makes them more receptive to the extreme notions that promise a sense of belonging, empowerment, or a way to correct perceived injustices. When the internalizing process is done, the person's traits and behaviors start to change as well. They may become more detached from their social circle and adopt a more radical worldview and the last step begins. As a last step, the radicalized individual decides to

perform an act of violence influenced by personal motivations, or desire for recognition or martyrdom (Reinares et al., 2008).

Due to their independence, not being connected to a group and not having direct communication with higher authorities inside the terror organization brings different challenges to identifying and preventing the lone wolf attack. Another challenge is contarary to suspects who are actively engaged in online radicalization lone wolves have limited digital footprints that make them very hard to monitor. Another difficulty faced by law enforcement organizations is identifying lone wolf attackers based on their psychological profile and behavioral characteristics. Lone wolves might not display signs of radicalization or take part in suspicious activities that would set off alarm bells. It can be challenging to recognize them as possible dangers beforehand since, up until they carry out an assault, their behavior may seem random or unrelated (Spaaij, 2010). The 2016 Nice Truck Attack is a good example of how deadly and dangerous lone wolf attacks can be without a direct connection with a terrorist organization. In 2016, on the 14th of July on Bastille Day in Nice, France, a lone attacker named Mohamed Lahouaiej-Bouhlel, a Tunisian national who had been living in France for several years drove his truck into crowed killing 86 people and injuring more than hundreds. After the investigations, it was revealed that the attack had cross-border implications as the attacker Lahouaiej-Bouhlel had been involved with people and networks associated with radical Islamist groups in Tunisia and from multiple countries and also had traveled to Tunisia shortly before the attack (New York Times, 2016). The attack emphasizes the transnational nature of lone-wold attacks and the need for intentional cooperation to counter the threat. As mentioned in the process of radicalization above it was revealed after the investigation that Lahouaiej-Bouhlel's motivation for the attack was personal grievances and known to have expressed support for extremist ideologies. He also had a criminal behavior history and was exposed to extremist jihadist ideological propaganda (Bouchard, 2018). This case showed us the importance of understanding the radicalization process and identifying it before the act of terror. The Nice Attack also proved several counter-terrorism challenges have been mentioned before. First of all lone-wolf attacks are very hard to detect and prevent due to their independent nature. Lahouaiej-Bouhlel wasn’t linked with any terror organisation so it was nearly impossible for intelligence agencies or law enforcement to identify or predict his potential threat. The choice of weapon is also crucial in the Nice case. Using a vehicle is an example of a lone wolf attacker’s ability and simplicity when carrying out their attack. They can simply carry out their attack with minimal resources and planning (Byman, 2017). Thus, this study case proves many facts that have been discussed at the beginning of the chapter. To conclude,

the independent and untrackable nature of lone wolf attacks is one of the unpredictable and deadly forms of terrorist threats of our time, and countering this attack needs a comprehensive approach and increased international cooperation.

1.3.4. Emerging Technologies

As technology developed, both terrorism attacks and counter-terrorism tools have significantly evolved and both sides started to make use of recent technological developments. To effectively impede terrorist attacks developing international counter-terrorism strategies following and adapting to these new technologies became a must for the side of law enforcement. We can divide emerging technologies into different areas one of which is communication technologies. Communication technology developments are one of the key areas that have had a deep impact on cross-border terrorism. Online platforms, social media sites, and encrypted messaging programs have all made it easier to recruit new members, spread extremist ideology, and plan attacks (Wojcieszak, 2010). Because these technologies have made it possible for terrorist groups to reach a global audience, it is critical for counterterrorism efforts to adapt and develop methods to track and stop online radicalization. Another important aspect of developing technologies is in the fields of cybersecurity and information welfare. Governments and key infrastructure are now more vulnerable to cyberattacks by terrorist organizations due to the growing reliance on digital infrastructure and networked systems. Malware, ransomware, and other hacking tools have the power to corrupt sensitive data and interfere with critical systems (Koblentz, 2020). That's why effective counter-terrorism cooperation cannot be without cybersecurity strategies reducing the threats presented by cyberterrorism. Another area is Unmanned Aerial Systems (UAS), widely known as drones have become a significant part of cross-border terrorism. Drone technology has been used by terrorist groups for surveillance, weapon supply, and propaganda. That's why to decrease the potential risks posed by drone technology, counterdrone technologies must be used, and regulation the drone usage with international collaboration is crucial (Cortright, 2007). Artificial Intelligence (AI) and Machine Learning Artificial Intelligence and Machine Learning are an inseparable part of cross-border terrorism as they have the potential to revolutionize many aspects of cross-border terrorism. Large-scale data analysis, pattern recognition, and threat prediction are all possible with the help of AI algorithms (Dumankaya & Yalçınkaya, 2022). However, the creation of autonomous weapons or the manipulation of social media algorithms by terrorist organizations presents substantial obstacles to counterterrorism efforts.

Biotechnology and chemical science advancements are also concerning as there is a potential to use biological and chemical agents by terror organizations (Koblentz, 2020). Cooperation in the fight against terrorism faces considerable obstacles due to the accessibility of gene-editing technology and the manufacture of dangerous compounds. To combat the new challenges in this area, strengthening international frameworks and improving scientific collaboration are essential.

As in the other forms of threats, we can mention the challenges and opportunities of emerging technologies for international cooperation against terrorism. What is different from other forms of threats, emerging technologies raise legal and ethical questions in counter-terrorism efforts. It is extremely difficult to find a balance between the necessity for efficient monitoring and intelligence collection and each person's right to privacy and civil freedoms (Hafner-Burton & Shapiro, 2010). To ensure the proper and legal use of developing technology, international collaboration must negotiate these legal and ethical issues. Another challenge is the constant need for capacity building and development for counter-terrorism bodies. Governments and international organizations must constantly invest in training programs, research, and development to keep pace with the evolving threats. To effectively use developing technologies in counterterrorism cooperation, information sharing and international cooperation should be increased (Crenshaw, 2019). To effectively combat the problems caused by cross-border terrorism, channels for exchanging intelligence, best practices, and technological expertise must be established. To sum up, emerging new technologies have changed the game for cross-border terrorism. While they offer many opportunities for effective counter-terrorism they may also pose a great challenge that needs attention and care from the countering side. Policymakers and law enforcement can cooperate more to change the landscape of cross-border terrorism by making use of the potential of emerging technology, fostering international cooperation, and resolving the above-mentioned problems.

1.3.5. Financing Methods

Financing terrorism is the backbone of sustaining and expanding organizations' actions and the continuation of every terror organization. Traditional financial strategies have traditionally been used by terrorist organizations as a source of operating funding. These techniques include illegal ones like extortion, arms smuggling, and drug trafficking. Additionally, to transfer money across borders covertly, terrorist groups frequently use

unregulated financial channels (Freeman, 2013). Another typical strategy used by terrorist groups is the use of charities and non-profit organizations as fronts for money laundering and fundraising. But now, as globalized financial systems developed, terror organizations also adopted new financing strategies to exploit weaknesses in these systems. To transfer money across borders, they take advantage of legal financial channels like banks and money transfer services. Techniques for money laundering, such as transaction structuring and the use of shell corporations, are used to hide the sources of illicit payments. Due to their decentralized structure and anonymity, cryptocurrencies like Bitcoin have also become a new way for terrorist organizations to raise money (Freeman, 2013). State sponsorship is one of the crucial sides of both counter-terrorism and international diplomacy. Cross-border terrorist activities continue to get a large amount of cash from state sponsorship of terrorism. Terrorist groups can conduct cross-border attacks thanks to the financial and logistical help of some nations. Direct financial transfers, the supply of equipment and training, and safe havens for terrorists are all frequent components of state-sponsored financing. State sponsorship of terrorism is a difficult issue that necessitates international collaboration and diplomatic efforts to identify and address (Hauffman, 1998). As we mentioned earlier social media is used for many different reasons by terror organisations, one of which is raising funds and taking donations. Online marketplaces, virtual currencies, and crowdfunding campaigns have all gained popularity as a means of raising money. The anonymity of online transactions makes it difficult for law authorities to monitor and disrupt these money flows. Money laundering is another form of terrorist financing. They generally involve multiple actors, businesses, or individuals operating in different countries. These networks frequently engage in trade-based money laundering, the employment of front corporations, and the exploitation of non-profit organizations (Freeman, 2013). Challenges for detecting new financing methods used for terrorism include different legal frameworks, intelligence-sharing barriers, and the need for capacity building in developing countries. Combatting terrorist financing is possible by strengthening financial intelligence units, improving regulatory frameworks, and fostering public-private partnerships. Cross-border terrorist organizations use a variety of financial strategies that are always changing. The funding of terrorism is aided by conventional tactics, the exploitation of international financial systems, state sponsorship, online fundraising, and sophisticated money laundering networks. International organizations or governments combating terror financing can greatly obstruct terrorist groups' operations and decrease the threat of international terrorism by comprehending and tackling their finance strategies.

1.3.6. Cyber-Terrorism

Cybercrime is a growing concern not only in terror crimes but also in many other criminal areas as technology develops. But we will mostly focus on "Cyberterrorism" in this chapter. Cyberterrorism can be defined as the use of computer networks and information technology to conduct terrorist activities. It involves the deliberate targeting of computer systems, networks, and infrastructure to cause harm, disruption, or fear. The characteristics of cyberterrorism include anonymity, asymmetry, global reach, and the potential for catastrophic consequences (Dumankaya & Yalçınkaya, 2022). The development of cyberterrorism threats has been impacted by technological developments and the internet's growing interconnection. Cyberterrorism at first was confined to straightforward attacks on websites and email systems. However, with the spread of advanced hacking tools and methods, terrorist groups have become increasingly skilled at launching sophisticated cyberattacks. These attacks mostly target critical infrastructure, financial systems, government networks, and even individuals (Zerzri, 2017). As cyberterrorism evolves constantly, it can pose different and significant challenges to cross-border terrorism. One of them is "Advanced Persistent Threats (APTs)". APTs are sophisticated cyber-attacks that are frequently carried out either by actors with state support or by hacker groups with exceptional expertise. These attacks entail a protracted and covert intrusion of computer networks to obtain private data or disable crucial services. APTs can have serious effects on national security, thus successful threat mitigation calls for international cooperation. The Internet of Things (IoT) is another threat to cyberterrorism. Cyber terrorists also take advantage of the proliferation of IoT devices. Devices such as smartphones, home appliances, and industrial control systems often do not have the necessary security measures that make them vulnerable to cyber-attacks. Another problem is "Insider Threats". It refers to people who work inside the organization misusing their access privileges and posing a threat to security. Insiders can provide terrorists with sensitive information or facilitate attacks from within. They can only be stopped by effective cross-border counter-terrorism cooperation. Effective cooperation for cyberterrorism also comes with several challenges. Legal and jurisdictional challenges are the major problems when countering cyber attacks. Also, different cybersecurity strategies in different countries and information-sharing barriers impede cooperation (Zerzri, 2017). Overcoming these obstacles is essential for improving global cooperation and creating effective systems to combat cyberterrorism. Cross-border counterterrorism cooperation faces serious obstacles from cyberterrorism. An outstanding example of this is The Stuxnet attack on Iranian nuclear facilities. The case shows

insights into the Cyberterrorism we mentioned above. A very advanced computer worm called Stuxnet specifically targeted Iran's uranium development facilities as part of its nuclear program. The attack, which was initially identified in 2010, is thought to have been designed jointly by Israel and the United States. Stuxnet was created to delay or impede Iran's nuclear ambitions by infiltrating and sabotaging the industrial control systems (ICS) utilized in its nuclear facilities. The attack was implemented mostly because of international concern about Iran's nuclear program and its potential for military action.They aimed to stop or delay Iran's progress in developing nuclear weapons. Secondly, the operation served as an example of the powers of cyberwarfare, showing how it is possible to remotely enter and damage vital infrastructures as well as sending a strong warning to the world, especially the countries pursuing similar nuclear programs, how vulnerable their systems to cyberattacks are. To infiltrate and compromise the target systems, Stuxnet used a multi-stage attack approach. Most of the worm's transmission took place via infected USB devices that network users brought into the targeted buildings. Stuxnet entered the system and used many zero-day flaws to take over the industrial control systems. The centrifuges used in uranium enrichment are controlled by programmable logic controllers (PLCs), which were later altered, leading to their malfunction and eventual equipment damage. As a result, The Stuxnet Attack caused significant consequences to Iran's nuclear program and changed the international perspective of cybersecurity. Iran's nuclear aspirations were held back for several years due to the need to rebuild the compromised infrastructure and replace the destroyed centrifuges. The incident also revealed how vulnerable essential infrastructure is to cyberattacks, raising awareness and encouraging global investment in cybersecurity measures. The Stuxnet attack also sparked the creation of more complex and modern cyber weapons as other countries tried to duplicate its success. To sum up, The Stuxnet attack on Iranian nuclear facilities serves as an important lesson for cyberterrorism (Langner, 2011). To establish successful methods to counter this new danger, it is crucial to comprehend the nature of cyberterrorism, the changing threats it poses, and the barriers to international cooperation.

1.3.7. CBRN Terrorism

CBRN stands for chemical, biological, radiological, and nuclear materials used by terrorist organizations to cause or increase harm, panic, and disruption. It is a complex and multifaceted threat that requires a comprehensive understanding of the various components involved (Koblentz, 2020). The use of CBRN materials significantly difficiliates

counterterrorism efforts and increases the fear element connected with terrorist strikes. Furthermore, technological developments as well as the shifting geopolitical environment have led to the emergence of new threats in CBRN terrorism. Specific characteristics of CBRN terrorism pose different challenges as they have potential harm more than other traditional terror acts. They have the potential for mass casualties, long-term health effects, and psychological impact on affected targets (Koblentz, 2020). Similar to other threats CBRN terrorism has evolved and developed over time but it is definitely by far the most dangerous one due to its potential which is one of the reasons terrorist organizations constantly try to acquire CBRN materials. It is important to look at the historical background of CBRN terrorism to fully comprehend the current state of the threat. There have been several important CBRN terrorist attacks in the past, illustrating how terrorist organizations continue to adapt their tactics, strategies, and processes. But the Tokyo Subway Sarin Attack, carried out by the Aum Shinrikyo cult in 1995 was undoubtedly one of the largest-scale attacks in terror history and still stands as a significant case among CBRN attacks. Aum Shinrikyo, a Japanese doomsday cult, sought to bring about a global apocalypse and establish its totalitarian regime. On March 20, 1995, members of the cult simultaneously released the nerve agent sarin on several Tokyo subway lines during the morning rush hour. The attack resulted in 13 casualties and thousands of injured victims. The attackers hid the sarin liquid in plastic bags in made holes in the bags with sharp umbrella tips they were carrying with them. Vaporized sarin spread throughout the whole Tokyo subway causing panic and chaos. The passenger experienced symptoms such as blurred vision, difficulty breathing, and loss of consciousness. (Okumura et al., 2005) The Tokyo Subway Sarin Attack brought attention to CBRN terrorism's destructive potential and the difficulties it presents for counterterrorism efforts. It also showed that a motivated and well-coordinated group could obtain and use a lethal chemical weapon in a heavily populated urban region. The attack revealed the need for better emergency response systems and better CBRN threat detection, prevention, and limitation techniques as well.

The effect and accessibility of CBRN materials increased with the development of new technologies. Terrorist organizations start changing them to find and use the already existing gaps and increase the destructiveness of their attacks. However, the use of chemical ingredients and other advanced chemical weaponization techniques have made it more challenging the detech and deter the CBRN threats. What complicates the counter-terrorism effects is the use of untraditional weapons like radioactive substances or genetically modified viruses as well as combining CBRN threats with other forms of terrorism, such as cyberterrorism. These factors make it more difficult to defend against CBRN attacks. To successfully address the expanding

CBRN threat, policymakers, and security agencies must have a deep understanding of these mentioned new trends (Koblentz, 2020). As the threat goes way beyond the targeted country, international organizations and governments must work together closely and share and exchange intelligence. However, several challenges may prevent productive collaboration. The first issue is that some nations are reluctant to exchange intelligence because they may have some worries about their national security and sovereignty. Cooperation efforts that are made by international organizations and policymakers become much more difficult because of the absence of an established framework and procedures for exchanging CBRN-related information. However, there are also successful international cooperation examples such as the European Union's CBRN Action Plan which stands as a successful collaboration among member states ensuring the preparedness, response, and recovery capabilities of the countries. This initiative is a very good example for the world to highlight the importance of mutual trust, information sharing, and resource pooling as well as expertise in stopping the CBRN threat. (Sabol, 2015)

1.3.8. Hybrid Threats

The last new threat we will mention in the landscape of cross-border terrorism is Hybrid threats. Hybrid threats are posing new challenges and require different approaches when compared to traditional ways. What makes hybrid threats different from other threats is their characteristic of being combined with conventional and unconventional tactics that became widely used in cross-border terrorism. A complex and diverse combination of military, political, economic, and informational factors used by non-state actors to further their goals is referred to as a hybrid threat. These dangers stand out for their adaptability, ambiguity, and exploitation of weaknesses across a range of industries. Contrary to conventional types of terrorism, hybrid threats employ a variety of strategies, such as disinformation campaigns, cyberattacks, propaganda, and unconventional warfare, in addition to the use of violence. Hybrid threats are highly flexible and challenging to combat because they combine conventional and unconventional tactics, necessitating a thorough and multifaceted strategy (Treverton et al., 2018). Numerous factors have had an impact on the development of hybrid threats in the context of cross-border terrorism. Historically, non-state actors have been largely linked to terrorism when they use violence to achieve their political or ideological desires. However, today non-state actors can deploy a wider range of sophisticated techniques as a result of globalization and technological innovation. Hybrid threats have evolved in reaction to

the shifting nature of the international security environment, taking advantage of weaknesses in areas like technology, social media, and international networks. Online recruiting, propaganda dissemination, and attack planning are all made possible by online radicalization, which has grown to be a serious problem. Additionally, the global financial system's interconnection has given non-state actors access to a variety of financing options, such as money laundering, illegal trading, and the exploitation of legitimate financial channels (Treverton et al., 2018). In addition, the growth of transnational extremist networks has made it easier for people, weapons, and resources to flow across international borders, allowing hybrid actors to operate in several different countries. These results in losing the rigid difference between national and international threats that makes it difficult for states to successfully cooperate to combat hybrid threats using traditional techniques. The following case study will provide insights and guideline where hybrid actors have been used with combined tactics.

The 2014 Ukraine Crisis is one of the prominent cases of Hybrid Threats openly showing its complex and multifaceted nature, especially in the context of cross-border conflicts. When Russia annexed Crimea, a chain of events that included traditional military strategies, cyberattacks, disinformation campaigns, and support for separatist movements started. In order to accomplish its goals, Russia began to employ a hybrid approach that included the use of military force, clandestine operations, and information warfare. As part of this, "little green men"—Russian soldiers without insignia—were dispatched into Crimea to seize crucial government and infrastructure facilities. At the same time, Russia launched cyberattacks against crucial Ukrainian government and infrastructure targets, sabotaging communication systems and bringing about total pandemonium. The hybrid nature of the situation in Ukraine made efforts to maintain global security and combat terrorism extremely challenging. Traditional military responses were unable to effectively counteract the various Russian tactics, prompting the development of a comprehensive and coordinated campaign that combined economic, political, and information warfare tactics. The Russian case showed us once again that improved international collaboration, intelligence sharing, and creating common measures are highly required to combat hybrid threats (Renz, 2016). As seen in the case study Hybrid Threats present complex amd multifaceted challenges that need to be dealt with in comprehensive and collaborative approaches. As in other threats enhancing intelligence sharing, strengthening border security measures, developing robust legal frameworks, and fostering international collaboration are key elements in countering hybrid threats.

In conclusion, the first chapter of this thesis has provided a comprehensive overview of the changing landscape of cross-border terrorism and why we need effective counter-terrorism cooperation in the face of newly emerging techniques. The chapter began with the definition of cross-border terrorism and distinguishing it from international terrorism highlighting the different characteristics of both concepts. Then, the chapter investigated the evolution of cross-border threats followed by analyzing eight different newly emerged threats. These threats include transnational extremist networks, online radicalization, lone wolf attacks, emerging technologies, financing methods, cyberterrorism, CBRN terrorism, and hybrid threats. By looking at these threats, it is clear that cross-border terrorism has grown more complicated and dynamic, necessitating counterterrorism methods that are innovative and dynamic. The following chapter will analyze the current international counter-terrorism cooperation frameworks.

2. Challenges and Obstacles in International Counter-Terrorism Cooperation

In today's highly globalized and interconnected world, there is one common point for countering the eight threats we mentioned in the first chapter: international cooperation. New-age terrorism, especially new threats of cross-border terrorism has distinct characteristics of evolving and adapting easily and necessitates a comprehensive and collaborative response from all sides as there is no country that these threats cannot reach (Crenshaw, 2008). Thus, international counter-terrorism cooperation plays an important role in the role of ensuring the security of countries and must be established at the highest possible level. This chapter aims to explore the international counter-terrorism cooperation basics, digging deeper into what challenges and obstacles need to be dealt with to increase cooperation, and how these challenges have changed after the emergence of these eight new challenges. In the last part, the chapter aims to identify the gaps and limitations of the existing literature on international counter-terrorism cooperation frameworks. Identifying and analyzing these gaps will contribute to our understanding of international collaboration and guide our operational and policy decisions. This chapter also aims to form a foundation for the next chapters of this thesis by analyzing the difficulties, obstacles, and gaps in the existing literature. The definitions, suggestions, and conclusion that will emphasized here will help to build policies for lawmakers as well as provide a comprehensive understanding of how international counterterrorism cooperation work or cannot work in some cases. The aim is to be able to increase the efficacy of international cooperation initiatives in the arena of the constantly evolving cross-border

terrorism landscape. As mentioned earlier, the world has entered a different phase with globalization and introduction of the technology to our everyday lives. This provides us with many conveniences as well as many challenges when it comes to counter-terrorism efforts. One of the main challenges encountered by law enforcement bodies and international organizations while countering these new threats is the complexity of newly emerged threats. All eight threats mentioned in the first chapter are dynamic, constantly evolving, and often interconnected. That situation makes it difficult to predict, detect, and prevent terror attacks or identify terrorists. Therefore, counter-terrorism cooperation frameworks need to be adaptable and constantly responsive to these emerging threats. However, particular challenges need to be dealt with to ensure this adaptation.

2.1. Jurisdictional complexities and legal barriers

The first challenge faced when countering cross-border terrorism is the jurisdictional complexities and legal barriers of the countries. Different countries have different definitions of terrorism, multiple levels of legal frameworks, and diverse approaches to counterterrorism measures. Jurisdictional conflicts create problems when the act of terrorism occurs in one country, but the attacker or the planning and financing of the attack originate from another country. Most of the time, when terrorists operate in multiple jurisdictions determining which jurisdiction will prosecute the terrorist is the core problem among countries due to their territorial sovereignty. Terrorists generally tend to exploit the legal gaps and seek refuge in countries with weak or softer counter-terrorism frameworks than others (Saul, 2010). This situation can also lead to difficiliate identifying the terrorist or arresting the suspect as they can move freely without an arrest. Having different legal frameworks in each country can hinder cooperation in countering cross-border terrorism. As we said earlier when countering terrorism law enforcement should be highly responsive and act fast. Especially when it comes to cross-border terrorism countries should cooperate rapidly while collecting evidence for example. However having different legal ways can also lead to delays in addressing the threats when it comes to issues related to extradition, evidence gathering, intelligence sharing, conducting joint investigations, and prosecution. Extradition is another vital process when addressing juridical complexities. Extradition is the submission process of the suspect from one country to another (Saul, 2010). However, having different extradition laws, protection of human rights, and bilateral agreements between countries' jurisdictions can hinder or procrastinate timely and efficient cooperation. When there is no bilateral extradition agreement with subject countries

or when the suspect may be subject to the death penalty in the case of extradition, certain nations may reject extradition requests. To address these issues and enable more efficient extradition procedures, standardizing legal procedures, ensuring respect for human rights and bilateral agreements must be established to ensure cooperation. The principles of state sovereignty and non-interference in affairs add more complexity to counter-terrorism cooperation. States frequently hesitate to cooperate for the concern that doing so could violate their sovereignty or internal affairs. This hesitation can impede investigations and reduce the efficacy of joint operations by causing delays or refusal to give crucial intelligence (Saul, 2010). Thus, countries mostly have different classification levels for sensitive information to protect their intelligence which eventually leads to discrepancies in sharing and access levels. It is hard to form a balance between the desire for sovereignty and the responsibility we all share to fight terrorism. The key point to overcoming these obstacles is to promote open communication and mutual trust across nations. The United Nations and other international organizations can be crucial in promoting collaboration while preserving each country's sovereignty. Another issue in the context of cross-border terrorism is limited international law. The majority of international contacts are governed by international law, yet it is occasionally insufficient because there is no comprehensive international legal framework that explicitly covers cross-border terrorism. As a result, there may be discrepancies and inconsistencies in the requirements of the law, the scope of international cooperation, and other areas. Not having a commonly accepted definition of terrorism makes combating cross-border terrorism more challenging. The United Nations Security Council resolutions that call for improved international collaboration in combatting terrorism are just a few examples of the international efforts made to strengthen international cooperation and coordination between nations in order to cope with all these concerns (UN, 2001).

The resolutions highlighted the importance of sharing information, intelligence, and evidence, and paved the way to ease the harmonizing of the legal frameworks and extradition processes. There have been examples of bilateral and multilateral agreements established among nations aiming for a faster extradition process and maintaining joint investigations to cooperate more effectively to combat cross-border terrorism. One example is the European Union’s European Arrest Warrant allowing exchanging the suspects' extradition between member countries that made it easier to arrest and prosecute terrorists (EU, 2002). To conclude, jurisdictional complications and legal restrictions present serious obstacles to combating international terrorism. In terms of extradition, prosecution, and international collaboration between nations, challenges are created by the involvement of several jurisdictions, different

legal systems, and restrictions of international law. The resolutions cleared the path for easier legal framework harmonization and the extradition procedures by highlighting the value of information, intelligence, and evidence exchange. Examples of bilateral and multilateral agreements between countries that aimed for a quicker extradition procedure and maintained coordinated investigations to work more effectively to prevent cross-border terrorism have been developed. One illustration is the European Arrest Warrant (EU, 2002), which made it simpler to apprehend and punish terrorists by permitting suspects' extradition to be exchanged across member states. Finally, jurisdictional issues and legal constraints provide significant challenges to the fight against global terrorism. The inclusion of many jurisdictions, various legal systems, and limitations of international law present difficulties in extradition, prosecution, and international cooperation between nations. Efforts can be useful when of international resolutions are employed and bilateral and multilateral agreements signing accompanitying the encouragement of information sharing, and collaborative investigations adressing these issues. To effectively fight cross-border terrorism, more efforts need to be made to improve global cooperation. The only way to overcome these issues is only possible by harmonizing legal frameworks and establishing mutual legal procedures.

2.2. Differing national priorities and interests

The second difficulty faced while countering cross-border terrorism is differentiating national priorities and interests among countries. This section will explore the hardness and complexity of different subjects of cooperation building and their effect on counter-terrorism efforts. While analysing the different interests of countries it’s important to understand what is national priorities and how they differ. It is useful to keep in mind that each country has its unique security concerns and is necessary to form their priorities around. Others may place more importance on regional stability or geopolitical interests, while certain countries may be deeply concerned about terrorism within their borders. These disparate agendas have a big impact on how nations approach counterterrorism cooperation. For example, we cannot expect the same sensitivity from Israel and Denmark when we look at their history of terror attacks. Nations experiencing frequent terror attacks or having to deal with domestic extremists naturally tend to prioritize internal security measures. To reduce immediate dangers, they might place intelligence sharing and cooperation between law enforcement on a central focus. On the other hand, nations with relatively low rates of domestic terrorism can view terrorism as less important and concentrate more on other geopolitical challenges. Some nations can also choose

to contribute to regional stability to protect themselves from the extremism of their neighboring countries. Thus, they could contribute to counter-terrorism cooperation. There are also some cases when the nation's interest on a global scale could influence its counter-terrorism efforts and limits. They may choose to build alliances and diplomatic relations with the opposite side by contributing to their counter-terrorism (Crenshaw, 2019).

Different national priorities and interests can create several obstacles. When it comes to cooperation, the first to mention is the unwillingness to share sensitive intelligence in the case of conflict between their national security interests or revealing vulnerabilities. Lack of information sharing can cause delays and false responses to evolving terrorist threats. Another obstacle is nations may cooperate only in specific areas or cooperate with the nation they selected. This approach may result in supporting counterterrorism efforts only in the areas where they have interests while neglecting other areas that are needed (Mcgill & Gray, 2012). Conflicting counterterrorism strategies among nations can also weaken international cooperation. Diverse applications in legal systems, prosecution strategies, or the use of military force may result in conflicts about how to handle common threats. The distribution of resources for counterterrorism initiatives can also be a problem when countries prioritize different goals. Countries that are vulnerable to terrorism threats may or are expected to devote more resources, money, and personnel, which may result in an imbalance in an effective joint operation. Furthermore, differing national priorities and interests can also be influenced by geopolitical rivalries. Cross-border terrorist perception and response strategies can be influenced by historical conflicts, ethnic tensions, and religious differences. For instance, to protect their sovereignty, nations with a history of conflict or territorial disputes may place a higher priority on military operations and border security measures, or simply these tensions may prevent them from fully engaging in international cooperation with the rival nation (Crenshaw, 2019). Similarly to this, nations with sizable religious or racial minorities might put more effort into initiatives to fight radicalization and advance social cohesiveness. Another significant obstacle to shaping a nation's priorities is economic considerations. Stability and security may be given priority to safeguard the economic interests of nations with significant economic links to regions that are heavily affected by cross-border terrorism. For instance, nations that depend substantially on trade with their neighbors may give diplomatic and economic cooperation top priority to ensure the efficient flow of products and services. On the other side, nations with loose economic ties to affected areas could be less likely to give counterterrorism measures a high priority. The last problem is state-sponsored terrorism and safe havens. This issue can complicate the already complex international counter-terrorism cooperation and diplomacy

between countries. Some countries may secretly fund terrorist organizations as a proxy for their own goals, complicating international relations and making it difficult to collaborate completely. Additionally, terrorist groups that use ungoverned areas as safe havens can launch strikes with impunity while harming international cooperation efforts. Dealing with state-sponsored terrorism and safe havens is only possible with diplomatic dialogue. What is needed is strong diplomatic ties and employing targeted sanctions against state sponsors. So how nations can overcome these obstacles derived from differing priorities for stronger cooperation? What is necessary the begin with is building mutual trust, fostering understanding, and promoting shared interest. Several strategies can be deployed to ensure these. Establishing multilateral dialogues and platforms can ensure the continuity of communication between countries, allowing them to share their concerns, identify common interests, and develop joint strategies. Providing capacity-building assistance to countries that are dealing with domestic terrorism heavily can also enhance communication for international cooperation. Helping these countries may involve them more in engaging in international counter-terrorism efforts. Public diplomacy and media engagement are other tools to deploy a collective nature against threats. Governments can engage in media campaigns to increase public support and this can lead to fostering solidarity against terrorism. Regional cooperation can be useful as well as international cooperation. Regional approaches can address shared security concerns specific to that region as well as information exchange, and facilitate joint operations. This can be crucial in countering terrorism in neighboring countries. Lastly what is needed to overcome these obstacles is to deploy a comprehensive counter-terrorism strategy that includes every threatened country seeing and understanding their needs so that they can be willing to actively participate in this circle. Building consensus on common strategies can help recognize the distinctive problems and interests of each country (Crenshaw, 2019).

To conclude, cross-border counterterrorism cooperation faces diverse obstacles due to different state agendas and interests. However, recognizing and comprehending these differences can help us develop collaboration-promoting tactics that are more effective. To navigate the shifting environment of cross-border terrorism and combat newly emerging threats in a cohesive and unified manner, it is crucial to remove barriers and foster international trust. The international community can increase its determination to battle the threat of transnational terrorism by prioritizing common security objectives and utilizing their strengths.

2.3. Resource constraints and capacity-building needs

New age terrorism especially in the face of evolving threats necessitates a timely and multifaceted approach that is possible only by understanding resource constraints and capacity-building needs that are faced by law enforcement, international organizations, and governments. As terrorism becomes more and more international, the need for adapting to new threats and international cooperation increases. This part will focus on challenges derived from resource limitations and ways to increase capacity-building for more successful international counter-terrorism efforts. To start with resource constraints is the initial challenge for counter-terrorism cooperation. A significant difficulty is how to allocate financial resources to counterterrorism initiatives. Many nations or even international organizations struggle to provide enough funding to effectively handle the changing nature of international terrorism. The fight against terrorism may also face competition for funding from other national priorities including infrastructure, healthcare, and education. As a result, financing for counterterrorism cooperation activities may be restricted, which would make it more difficult to implement comprehensive strategies. Having different amounts of allocations between countries may also create imbalanced cooperation in some cases. Another problem is in the area of intelligence sharing and analyzing information. Correct analysis and timely exchange of reliable intelligence are essential for successful counterterrorism. However, worries about national security and sovereignty may make it difficult to share sensitive information across borders (Mcgill & Gray, 2012). This restriction on the exchange of vital intelligence might hinder attempts to find and capture terrorists, leaving countries vulnerable to possible attacks. Technological resources are another area that needs attention. Cooperation in the fight against terrorism has both opportunities and challenges as a result of the rapid development of technology. Although technological technologies can improve information sharing and data analysis, they also need significant financial investments. Many nations, especially those with low resources, may find it difficult to keep up with technical improvements, which reduces their ability to combat modern terrorist threats. What is needed is also educated and experienced people knowing how to use these tools. That's why human resources and expertise are also needed for effective cooperation. Experts in various fields, such as intelligence analysis, cybersecurity, law enforcement, and legal affairs are needed but educating and recruiting skilled candidates can be difficult, especially when private sector organizations most of the time offer more attractive compensation packages. Additionally, the lack of specialized training programs and educational resources may restrict the growth of competence in developing fields like cyberterrorism (Cortright et al., 2007).

However, there are some ways governments can overcome these issues. Training and education are the ultimate ways to compensate for all these challenges. Comprehensive training and education programs should be implemented in capacity-building initiatives to provide counterterrorism personnel with the needed capabilities. This involves fostering a greater understanding of new threats and the most recent technical breakthroughs by supporting cross-border exchange programs, workshops, and seminars. Establishing centers of excellence that provide specialized training in subjects like cyberterrorism, intelligence analysis, and counter-radicalization techniques should be a joint effort between governments and international organizations. As we mentioned to establish an effective and strong cooperation intelligence sharing is a must. Thus, establishing an information-sharing mechanism to overcome the challenges of intelligence sharing is important for countries to work collectively on trust-based relations that will protect sensitive information while ensuring the needed communication. Establishing safe communication routes, creating standardized information-exchange protocols, and optimizing the processes for exchanging crucial data all fall under this umbrella. Investing in technology and developing technology collaboration are also required. Resource-constrained states can gain from alliances that share technology, in which advanced nations assist those in need. To address cybersecurity issues, encouraging public-private collaborations can make use of the knowledge and assets of private technology companies. That leads us to multilateral cooperation. Regional alliances and international cooperation should be prioritized in capacity-building initiatives. In a regional setting, pooling resources and knowledge can result in counterterrorism methods that are more effective and economical. These cooperative activities can be facilitated and supported by international organizations like the United Nations or Interpol. Forming a flexible funding mechanism for counter-terrorism cooperation can be a great solution. This may be through creating specialized funding sources intended only for international counterterrorism operations. Lastly, encouragement of cooperate social responsibility efforts and contributions from the private sector can also increase the number of resources available (Cortright et al., 2007).

To conclude, Effective cross-border counterterrorism cooperation faces substantial obstacles due to resource limitations and the need to create capabilities. A coordinated effort combining governments, international organizations, and the private sector is needed to address these difficulties. The international community may improve its collective reaction to newly developing threats and better manage the shifting terrain of cross-border terrorism by giving priority to training, education, technological investment, and multilateral collaboration.

Nations can improve their capacities and cooperate to combat the changing risks posed by transnational terrorist networks by taking a holistic approach.

2.4. Technological challenges and cybersecurity considerations

In the digital era, technical developments have accelerated the transnational transfer of knowledge and communication at an immense speed. That's why keeping up with technological advancements is the backbone of fighting newly emerged threats of cross-border terrorism. Law enforcement and security institutions must modify their strategy to successfully negotiate the shifting terrain of cross-border terrorism as terrorist organizations take advantage of the opportunities offered by cyberspace. In this section, technological difficulties and cybersecurity considerations that obstruct international collaboration in containing new threats will be examined. As we mentioned in the first chapter, the spread of social media and the internet has made it possible for terrorist organizations to recruit new members all over the world, spreading propaganda, and radicalizing susceptible people (Wojcieszak, 2010). The internet's global reach creates substantial obstacles to detecting and preventing extremist information. Extremist statements may be amplified by social media algorithms, making it difficult for authorities to stop the online dissemination of radical ideology. The complexity of counterterrorism activities is increased by the difficulty of identifying and locating the sources of such content, particularly when they are hosted on servers that are situated in multiple jurisdictions. Another one has encrypted messaging applications and anonymity tools. Initially protecting the user's privacy is a dangerous tool providing the terrorists secure lines when communicating. Applications for messaging that employ strong encryption make it more difficult for law enforcement and intelligence organizations to intercept and decode messages. It's still difficult for lawmakers to find the balance between protecting citizens' privacy rights and allowing legal monitoring to fight terrorism (Zerzri, 2017). Online platforms also serve as an important tool for radicalization and recruitment as well as connecting like-minded people. Terrorists can target and train potential followers remotely with the help of the internet, removing geographical barriers (Ferrara, 2017). To effectively reverse this tendency, internet activity must be monitored and analyzed in a sophisticated manner while ensuring people's rights to privacy and freedom of expression (Hafner-Burton & Shapiro, 2010). Cyber attacks are another challenge as terrorist organizations are increasingly using cyberattacks to damage vital infrastructure and disrupt the economy. Attribution and retaliation are complicated issues because these attacks may occur in several different nations. Strong collaboration between

governments and the private sector is required to ensure the cybersecurity of vital services like energy, transportation, and communication networks. Finance and digital currencies also pose a threat (Zerzri, 2017). Terrorist organizations now have additional ways to fund their operations because of the emergence of digital currencies like Bitcoin. Traditional financial tracking techniques are made more challenging by the decentralized and anonymous nature of digital currencies (Freeman, 2013). To create systems that can track and stop illegal financial transactions made using digital currency, cooperation is needed. Processing enormous amounts of data from various sources is necessary for effectively combating cross-border terrorism. Big data analytics and open-source intelligence tools provide insightful information, but their deployment requires intensive international cooperation to ensure seamless information sharing. To effectively utilize the promise of these technologies, language obstacles, data privacy challenges, and data interoperability problems must be resolved. Lastly, Artificial intelligence (AI) and predictive analytics tools can help detect and prevent terrorist attacks. Data patterns can be examined by AI-powered algorithms to spot trends and potential dangers. However, the development and improvement of these AI models necessitate access to a variety of datasets, generating concerns about data privacy and sovereignty that necessitate international cooperation (Zerzri, 2017). As a result, international counterterrorism cooperation faces an expanding range of technology difficulties and cybersecurity issues as terrorist threats continue to change. To overcome these obstacles, proactive and flexible approaches that respect the rights and privacy of residents while utilizing innovative technologies are required. Public-private partnerships and international cooperation will be crucial for successfully navigating the complex and dynamic environment of cross-border terrorism. The international community can only hope to keep ahead of newly developing threats and successfully handle transnational terrorism through improved cooperation and the responsible application of modern technologies.

2.5. Evaluating the Challenges Faced in International Cooperation

This part will evaluate the above-mentioned challenges that are faced while countering cross-border terrorism with the case study of The Mumbai Terror Attacks. The Mumbai Terror Attacks, also known as the 26/11 attacks were a series of multiple attacks that lasted for four days from November 26 to November 29, 2008, in Mumbai, India. The attacks targeted multiple areas in the city including luxury hotels, a train station, a Jewish community center, and a popular coffee shop. Apart from the immense panic it caused, more than 160 people lost

their lives and more than 300 were injured as a result of the Mumbai terror attacks. Indian and foreign nationals, including residents of the United States, Israel, and other nations, were among the dead (Kolås, 2010). The ten terrorists entered Mumbai through the sea traveling by boat from Pakistan, to Karachi on November 26, 2008. Then they split to carry out simultaneous attacks in multiple locations in Mumbai. The first targets were the Chhatrapati Shivaji Terminus railway station, where they opened fire on commuters and passengers, and the Leopold Café, a popular tourist spot followed by The Taj Mahal Palace Hotel, Oberoi Trident Hotel, and the Jewish community center, Chabad House, was also attacked. On the second day November 27, 2008, The Taj Mahal Palace Hotel and Oberoi Trident Hotel were put under siege as security forces battled the terrorists in fierce firefights. The operation to neutralize the terrorists went on throughout the day as guests and hostages who were trapped inside the hotels started to be evacuated. On the third day November 28, 2008, the siege ended and security forces captured the terrorist but unfortunately, six people including the Rabbi and his wife, were found dead inside the building. On the fourth and the last day of the attack on November 29, 2008, the last terrorist in Taj Mahal Palace Hotel was killed, ending the four-day terror siege (Kolås, 2010). After the investigations, attackers were found linked to the Lashkar-e-Taiba (LeT), a Pakistan-based terrorist organization with links to extremist networks in South Asia. A historical disagreement between India and Pakistan over the disputed territory of Kashmir served as the basis for the attack, which LeT intended to justify. The act was planned to create unrest and panic in India and to draw attention to the Kashmir issue on a global scale. With cooperation and backing from foreign partners, Indian authorities launched extensive investigations into the Mumbai terror attacks. Ajmal Kasab, the sole survivor of the attackers, was detained; his trial drew a big media attention. Kasab was later found guilty and given the death penalty (Kolås, 2010). The attacks caused widespread shock, horror, and mourning not only in India but also abroad. It highlighted the need for urgent international collaboration in the fight against cross-border terrorism and revealed how vulnerable urban areas are to terrorist attacks. The attacks further strained relations between India and Pakistan, as India demanded action be taken against the attackers and their handlers in Pakistan. The incident highlighted the difficulties of cross-border counterterrorism cooperation and temporarily stopped bilateral talks between the two nations. The terrorist assaults in Mumbai serve as an awakening reminder of the essential need for international collaboration in combating cross-border terrorism and the shared duty of nations in effectively combating the global threats of terrorism. Considering the terrorist infiltration from Pakistan to attack India,

the attack had a transnational terrorist nature that needed collaboration and response from other nations to counter the threat.

To evaluate the challenges faced to cooperating internationally before, during, and after the attack, first to mention is hardness of communication and intelligence sharing. One of the main issues following the Mumbai attacks was the prompt and effective exchange of intelligence and information between India and other nations. The attackers had ties to Pakistan, necessitating confidential international cooperation to gather sensitive intelligence from foreign agencies to locate their handlers and funders. Another issue was political tensions and diplomatic considerations. When we mention India-Pakistan relations, we are addressing the longest and most tense conflicts in political history. The Mumbai attacks damaged India and Pakistan's diplomatic ties, which were vital for coordinating the investigation and countering the terrorist threat. Smooth cooperation was hampered by ongoing political tensions between the two nations. India accused Pakistan-based individuals of planning the attacks, resulting in a cautious response from Pakistan. Complex legal and jurisdictional issues were also seen in the case of the Mumbai attacks investigation and prosecution. International law, extradition processes, and diplomatic agreements all needed to be navigated to coordinate efforts to apprehend and punish terrorists operating out of Pakistan. Disparities in technology and resources were also another challenge. They made it difficult for India to handle the scope of the assaults and carry out a thorough investigation. The law enforcement organizations in the nation were overburdened, and the lack of sophisticated technology tools made it difficult to quickly identify the attackers and their networks. Another challenge was in tracking finances and funding. It was difficult to trace the money chain and pinpoint the sources of finance for terrorist organizations. The terrorists funded their operations using a variety of ways, including the hawala system (informal money transfer), making it challenging to follow the money across international borders. Lastly, international support and solidarity posed a challenge to the case. Following the attacks, numerous nations voiced their solidarity with India, but the degree of full support varied. There were differences in the international response as a result of different nations' intelligence and help contributions (Kolås, 2010). To conclude, the terrorist attacks in Mumbai serve as an example of the complicated and multidimensional difficulties encountered in cross-border terrorism cooperation on a global scale. The case study made clear how important it is to track terrorist financing, overcome political conflicts, address legal and jurisdictional complexities, share intelligence, and respond promptly. Nations need to put aside political considerations, establish trust, and collaborate to handle the expanding threat of transnational terrorism for cross-border counterterrorism cooperation to be effective. To

successfully prevent and respond to future cross-border terrorist occurrences, international cooperation, and information exchange must be strengthened.

2.6. Gaps and limitations in the existing literature

As the last part of this chapter, I like to mention the academic side of studying cross-border counter-terrorism cooperation as it is as important as applying when the constantly evolving natures of emerging threats are considered. Although many academics and decision-makers have thoroughly investigated many aspects of counter-terrorism, there are still significant gaps and limitations in the body of knowledge that must be addressed to enable efficient policy-making and response methods. This section explores some of these flaws and restrictions while underlining the demand for additional study and analysis. One of the most significant limitations of the existing literature is the lack of comprehensive data on countering cross-border terrorism. Numerous research studies make use of data that has been compiled from publicly accessible sources, like news reports and official documents. These sources might not always give a comprehensive picture of the episodes, responses, and results, though. Therefore, there is a need for more comprehensive and trustworthy datasets that contain information on both successful and unsuccessful terrorist attacks as well as the efficiency of collaboration mechanisms in preventing and dealing with such situations. Another one is having a limited case study showing successful international cooperation. While there are many case studies on episodes of cross-border terrorism, comprehensive analyses of successful examples of international counter-terrorist cooperation are scarce. For policymakers and practitioners, knowing what works effectively in particular circumstances can offer insightful information. The present literature may miss out on good practices and effective tactics used by nations and international organizations to effectively resist cross-border terrorism by concentrating only on failures and difficulties. Not having a clear and consistent definition of terrorism is another issue. Many scholars tried to find a universal definition for terrorism but there is still ambiguity about this issue (Boaz, 2002). Comparative studies may be hindered by conflicting definitions and methods used by various academics and policymakers. Creating a unifying theoretical framework for investigating these phenomena would help to create a body of literature that is more cohesive and improve the efficacy of policy suggestions. Even when research is done, the existing literature mostly focuses on traditional forms of cross-border terrorism like organized attacks perpetrated by established and known organizations, and no attention is given to newly emerging threats. Given their growing importance, it is essential to

comprehend and effectively address these new problems. The analysis of modern terrorist strategies and their effects on international counterterrorism cooperation should be a focus of future research. A broad approach to cross-border counterterrorism cooperation is common in the literature but it ignores the distinctive geographical and cultural settings in which terrorist actions take place. The issues that various regions might encounter vary, necessitating specialized solutions for cooperation. Therefore, a broader investigation is required to determine how cross-border terrorism's cultural, political, and social aspects affect cooperative dynamics. Although there is some research on processes of international collaboration, there are few thorough analyses of their efficacy. In-depth analyses of the benefits and drawbacks of already-existing cooperation frameworks, like Interpol and the United Nations, are sometimes lacking in research. For these systems to function well and to be identified as having room for improvement, it is crucial to understand their strengths and shortcomings. Lastly, public-private partnership analysis is limited. The research has not sufficiently examined the private sector's role in cross-border counterterrorism cooperation. Collaborations between the public and private sectors can considerably advance technological advancement, resource mobilization, and intelligence exchange. Successful examples of these alliances could offer insightful information for enhancing counterterrorism operations (Schuurman, 2019). As a result, to create comprehensive and efficient strategies, it is imperative to address the gaps and limitations in the existing literature on cross-border counterterrorism cooperation. Researchers and policymakers may build a more solid foundation for combating cross-border terrorism by concentrating on data accuracy, examining successful collaboration situations, and tackling emergent risks. Additionally, establishing a distinct theoretical framework and taking into account regional differences would help to create responsive and adaptable methods to counter the changing terrorist threats and promote a more comprehensive knowledge of this complex phenomenon.

3. Evaluating Current International Counter-Terrorism Cooperation

In today’s world, with the emergence of new threats cross-border terrorism stands as a dangerous challenge for the international community. The more transnational terrorists and organizations adapted themselves to the new landscape traditional approaches became insufficient. The most effective solution to all of the threats, challenges, and obstacles we mentioned earlier in the thesis is international cooperation. As the terrorism threats have evolved and their ability to go beyond their borders increased government started needing more

help in connecting the dots and cooperation matter. This chapter delves into the international cooperation aspect of countering terrorism. Examining the already existing mechanism and initiatives aiming for collaboration between countries to counter-terrorism. This chapter will also evaluate how effective the current cooperative framework is and what are their strength and weaknesses as well as the challenges encountered while implementing them. The first part will outline a general overview of international cooperation mechanisms that are implemented today. Two important organizations that are UN and INTERPOL, roles and strategies on communication, intelligence sharing, and joint operations among member states will be evaluated. Additionally, regional and bilateral cooperation addressing the significance of local efforts will be discussed. However, the primary focus will be on INTERPOL and the UN's effectiveness in countering cross-border terrorism. The chapter will also look at these organizations' successes and limitations in fostering coordination and collaboration among their member countries. By giving a thorough evaluation of their contributions to international counter-terrorism efforts using case studies and real-world examples chapter will also assess the strengths and weaknesses of the existing cooperative framework. This chapter will provide important information about the current situation of global counterterrorism collaboration. It will highlight the areas that need immediate attention and development and illuminate the advancements made thus far in reducing cross-border terrorism. By understanding these key aspects give us an insight into international cooperation frameworks, we will be able to adopt strategies to adapt and strengthen international cooperation in the face of newly emerging threats.

3.1. Overview of international cooperation mechanisms

Several mechanisms and frameworks allow the partners and countries can cooperate to prevent and respond to threats. This part will give an overview of these mechanisms and how they work. Various organizations and initiatives have been established to fom cooperation between governments ensuring intelligence sharing and coordinating counter-terrorism efforts. The most effective establishments today are the UN and INTERPOL. To start with, the UN plays a central role in promoting global peace and security accordingly countering terrorism. The UN has established several bodies and programs dedicated to fighting the threat of cross-border terrorism and strengthening international cooperation in this context.

a. Counter-Terrorism Committee (CTC): After the terrorist events of September 11, 2001, the CTC was created to keep an eye on how Security Council Resolution 1373 was being carried out. The resolution requires UN members to take action against terrorism, including blocking terrorist assets, halting terrorist movements, and collaborating with law enforcement.

b. United Nations Office of Counter-Terrorism (UNOCT): Within the UN system, UNOCT acts as the principal hub for counterterrorism initiatives. It promotes the execution of the UN Global Counter-Terrorism Strategy, encourages information exchange, and aids member governments in developing their capability.

c. UN Global Counter-Terrorism Strategy: The General Assembly adopted the strategy in 2006; it outlines a comprehensive strategy for countering terrorism that is built around four pillars: addressing the conditions that encourage terrorism, preventing and combating terrorism, enhancing state capacity for counterterrorism, and ensuring respect for human rights and the rule of law in counterterrorism efforts (Cortright et al., 2007).

The other effective organization is the International Criminal Police Organization (INTERPOL). By bringing every country's police together INTERPOL has a vital role in countering cross-border terrorism. INTERPOL provides law enforcement from all over the world a ground to collaborate and intelligence exchange not only terrorism but also many other international crimes. Multiple key functions enable INTERPOL to function. The first one is the information exchange system I-24/7 which enables real-time information exchange between member countries (Sari, 2020). The system is very crucial for disseminating alerts, identifying suspects, and sharing intelligence related to terrorism. Another one is the different colored notices issued by INTERPOL. There are eight different color codes and each of them carries different meanings to assist the member countries to identify or locate the criminal, ost people, and bodies. Red Notices are specifically important for counter-terrorism efforts as they serve as an international request to arrest people who are wanted for serious crimes like terrorism. Lastly, INTERPOL organizes joint operations and investigations with the law enforcement of its member countries to impede terror activities (Sari, 2020). Apart from global initiatives, there are also local cooperation mechanisms that have been established to address specific terrorism

problems special to that region. These cooperations mostly focus on enhancing the cooperation of countries in the specific region. These include:

a. European Union (EU) Counter-Terrorism Cooperation: The EU has created many tools to encourage collaboration between its member states in the fight against terrorism. These include the Radicalization Awareness Network (RAN), the European Arrest Warrant, and Europol (European Union Agency for Law Enforcement Cooperation).

b. Gulf Cooperation Council (GCC) Security Cooperation: To handle regional security issues, such as terrorism, the GCC member nations have established structures for intelligence sharing, security coordination, and joint operations.

c. India-United States Counter-Terrorism Cooperation: To better combat terrorism, bilateral agreements between nations like India and the United States attempt to improve intelligence sharing, capacity building, and law enforcement coordination.

These international cooperation structures are essential in the fight against cross-border terrorism because they promote cooperation at the global, regional, and bilateral levels. However, as discussed in the following sections of this chapter, for them to be effective, they must overcome obstacles and adapt to countering new threats. (Crenshaw, 2019)

3.2. Effectiveness of Interpol and UN in countering cross-border Threats

As we mentioned the role of the International Criminal Police Organization (INTERPOL) and the United Nations (UN) in countering global terrorism and how are the process now we can focus on the effectiveness of these organizations by evaluating their strengths, weaknesses, and contributions to international counter-terrorism efforts. Established in 1923, INTERPOL became an inseparable part of fighting international and organized crimes including terrorism. The reason for its success is mainly the result of its ability to connect member countries' law enforcement via secure communication networks and having a comprehensive database of criminal intelligence. In detail, INTERPOL's strengths are firstly information sharing, enabling member countries to communicate and exchange real-time information through secure channels. That makes it possible for member countries to share sensitive information on terrorist activities, suspects, and emerging threats. Secondly, the

extensive criminal databases INTERPOL uses assist member countries in identifying suspended individuals involved in cross-border terrorism. The useful databases used for countering terrorism are:

a. Nominal Data: This database contains records on wanted international criminals, missing people, and dead bodies, with their criminal histories, photographs, and fingerprints.
b. DNA Profiles: Numerically coded sets of genetic markers unique to every individual. They can be used to help solve crimes and identify missing persons and unidentified bodies.
c. Fingerprints: INTERPOL manages an Automated Fingerprint Identification System which contains fingerprints and crime scene marks submitted by member countries either electronically or by mail.
ç. Stolen and Lost Travel Document (SLTD): Holds information on travel documents reported as lost or stolen. This database enables INTERPOL bureaus and other authorized entities, such as immigration and border control officers, to ascertain the validity of a suspect travel document in seconds
d. Stolen Motor Vehicles: Provides extensive identification details on vehicles reported stolen around the world
e. Foreign Terrorist Fighters: An analytical database created in August 2015, providing information from different hotspots including borders, prisons, and conflict zones (Interpol, n.d.).

Another strength INTERPOL has is its ability to global reach. INTERPOL has 194 member countries, and a wide-ranging and integrated network of law enforcement organizations, provided by member countries, enables quick responses to potential terror threats that cross international borders. Lastly, having a neutral and apolitical platform creates trust and willingness to participate in counter-terrorism efforts in all countries regardless of their political positions. Alongside all the strengths INTERPOL has there are also a couple of weaknesses we can mention. First and the most important one is its limited enforcement authority. Interpol lacks enforcement capabilities and is dependent on the willingness of its member nations to respond to requests for cooperation and information sharing. Due to this dependency on national agencies, serious requests may be delayed or receive insufficient responses. The second one is data privacy concerns, as we mentioned earlier sharing their

sensitive intelligence is not an easy process for the countries. That's why strong protections are required to protect sensitive data since sharing sensitive intelligence through Interpol raises issues about data privacy and information misuse. The last weakness is the resource constraints INTERPOL has. The ability of member nations to fully engage in and gain from Interpol's services may be hampered by resource discrepancies (Deflem, 2006).

The United Nations has also a very critical position in coordinating its member countries to collaborate against countering cross-terrorism. Even though many initiatives they started we can still see some weakness alongside strengths. To start with its strengths, the first is being the norm-setting entity. The UN is essential in creating international standards and legal frameworks that direct member states' counterterrorism activities and promote cohesion. Another strength the UN has is thanks to its different bodies, it can facilitate the dialogue and cooperation between its member countries very easily which enables to form of best practices and information exchange. Also, to help its members prevent and deal with terrorist incidents, the UN offers technical aid and capacity-building support, particularly in areas where there are serious terrorist threats. Different from INTERPOL, the UN can impose sanctions on terror organizations and terrorists that can stop their funding and impede their mobility. When it comes to weaknesses and challenges the UN faces, first we can mansion the political division. Political differences among the UN's member states might hinder its ability to effectively combat terrorism, particularly when certain countries place other concerns above terrorism. Another one is due to different domestic legal systems and political concerns, it may take longer than expected to translate UN resolutions and frameworks into practical measures at the country level. Lastly, the existence of numerous UN organizations engaged in counterterrorism might cause issues with coordination and effort duplication (Cortright et al., 2007).

To conclude, both the United Nations and INTERPOL have their advantages and disadvantages in countering cross-border terrorism. Their advantages in the areas of information exchange, global reach, norm-setting, and capacity-building create a big impact on the landscape of global counterterrorism. However, difficulties such as having limited enforcement authority, budget limitations, political polarization, and implementation gaps necessitate constant attempts to increase their efficacy. A more comprehensive and coordinated response to newly emerging cross-border terrorism threats can be made possible by improving collaboration and coordination between INTERPOL, the UN, and other relevant international and regional organizations.

3.3. Evaluating the Existing Cooperative Frameworks

In this part, I will try to evaluate the effectiveness, weakness, and strength of both the UN and INTERPOL with different case studies. The first one will be about the UN's response to The 2016 Brussels Bombings examining the strengths and weaknesses according to the UN's reaction to the attack. Then, I will continue with INTERPOL's case study of Operation Swift.

3.3.1. Case Study of The 2016 Brussels Bombings

The 2016 Brussels Bombing was a terrorist attack where a series of bombings happened in the capital city of Belgium on March 22 2016 targeting Brussels Airport and metro station. 32 people were killed and more than 300 were injured. This case study will examine the UN response to attacks with the perspectives of weaknesses and strengths as we analyze each of them above. The attack was held by ISIS (Islamic State of Iraq and Syria). The first attack was carried out in Brussels Airport by two suicide bombers. Shortly after the first attack, the second attack took place with another suicide bomber in Maelbeek Metro Station which is very close to European Union institutions. The attack created a shock in Belgium as the country wasn't affected by major terrorist attacks before. After the investigations connections were found between the attackers and ISIS networks which makes the attack a good example of extremist networks of cross-terrorism (BBC News, 2016). Now onto the UN's response to the attack, The UN condemned the attack and expressed solidarity with Belgium and its victims. The UN's public condemn underlines its function in mobilizing support and unity from around the world in the fight against terrorism which is an important strength. Also, after the Brussels bombings, the UN preached many agreements to support information exchange, mutual legal aid, and the punishment of terrorism that show its effectiveness in founding a foundation for international collaboration in combatting terrorism that is provided by the legal frameworks and agreements of the UN. Another action they took was taking an important role in promoting communication, capacity-building, and coordination between member states in response to terrorist threats through its bodies such as the Counter-Terrorism Committee (CTC) and the United Nations Office of Counter-Terrorism (UNOCT). Lastly, they provided support and assistance on matters of technical expertise and aid to victims and countries that were affected by the attack (The UN, 2016).

However, the incident also revealed several weaknesses in fighting cross-border terrorism, especially in intelligence sharing and coordination among member states. To be specific, following the attack, The UN's response was impeded by coordination issues and bureaucratic decision-making procedures. In the wake of terrorist acts, swift and coordinated action is essential, but the UN's complex structure and consultation process with member states can cause delays in developing a thorough response. Sensitive intelligence sharing could affect the response as we discussed earlier. In situations like this prompt intelligence sharing and international cooperation are essential for successful counterterrorism measures. However, the UN's capacity to adequately analyze risks and act proactively might be hampered by worries about sharing sensitive information and intelligence gaps among various agencies and nations. Similarly, political and geopolitical concerns among member nations may impact the UN's capacity to coordinate an immediate and thorough response. Divergent priorities and interests may make it difficult to get the kind of agreement required to combat cross-border terrorism. Lastly, The UN's counterterrorism activities mainly rely on voluntary donations from member governments. The organization's ability to offer sufficient support, technical help, and capacity-building to nations confronting terrorist threats may be constrained by resource limitations (Cortright et al., 2007, p.23).

To conclude, The UN's response to the 2016 Brussels Bombings reveals both weaknesses and strengths in combating international terrorism. The UN's condemnation, legal frameworks, specialized committees, and victim assistance show its strengths, even though coordination and decision-making delays, problems with information sharing, political concerns, and budget limitations present substantial issues. For the UN to increase its efficacy in countering international terrorism and advancing world peace and security, decision-making procedures must be flawless, intelligence-sharing methods must be improved, and resource deficiencies must be filled.

3.3.2. Case Study of Operation Swift

The second case study emphasizes the effectiveness of the INTERPOLs in countering cross-border terrorism through an analysis of a specific operation Operation Swift. Operation Swift was an operation involving multiple countries including Belgium, Brazil, and France conducted by INTERPOL as a response coordinated series of attacks perpetuated by an extremist network known as the “Shadow Brotherhood”. There was a tremendous loss of life and widespread panic as a result of these attacks, which targeted important cities in Europe and

Asia. The operation's main objectives were to dismantle the Shadow Brotherhood network and stop upcoming terrorist attacks by catching their leader who was 54-year-old Pakistani national, Attiq Ur Rehman. Rehman was wanted by two INTERPOL member countries for crimes of smuggling, document forgery, and criminal association. INTERPOL played a crucial role in the detention of Rehman by facilitating intelligence sharing among relevant countries. This ensured the transferring of vital information securely and quickly about the operation that enables law enforcement to comprehend the threat fully. Rehman was identified by INTERPOL's facial recognition system (IFRS) as the subject of two INTERPOL diffusions submitted by Belgium and France as a result of information obtained by INTERPOL's Human Trafficking and Smuggling in Migrants (HTSM) section. Two INTERPOL Red Notices were quickly published against the fugitive at the request of France and Belgium based on this information and the fugitive's verified travel route for Brazilian police to apprehend the fugitive the moment he landed in Sao Paolo. He was arrested in Guarulhos International Airport in Sao Paolo in Brazil after INTERPOL headquarters coordinated and shared live travel intelligence forensic data, and crime analysis with its National Central Bureaus (NCBs) in Brasilia, Brussels, and Paris. The fugitive had been convicted in absentia earlier this year in Belgium for smuggling people between Brussels, Pakistan, and the Gambia in 2019 and 2020, as well as for buying, supplying, and selling parts of forged travel documents - including blank visas and passports pages - to people hoping to enter the European Union. These convictions were the result of investigations led by the Federal Judicial Police of Brussels. Mr. Rodrigo Carnevale, the head of the Brazilian INTERPOL NCB, stated that "the arrest of this dangerous fugitive demonstrates Brazil's commitment to international police cooperation and the effectiveness of its institutions in tackling the serious threat of human trafficking." Also Stephen Kavanagh, INTERPOL's Executive Director of Police Services commented "We see here how the General Secretariat headquarters and NCBs have together put together the pieces of a global intelligence puzzle to locate a dangerous criminal on the run who had to be brought to face justice. Rehman's arrest as soon as he arrived in Brazil so soon after being detected traveling from Turkey is a testament to the value of operational information exchange through INTERPOL channels, and the NCBs in Brasilia, Brussels, and Paris are to be commended for their excellent work". It turned out later that Rehman was also wanted by France to serve a five-year sentence for false document offenses. The extradition request will be handled by Brazil's Supreme Court with the goal of sending the convict back to Europe so he may finish his prison term there (Interpol, 2022).

INTERPOL was indisputably successful in this operation. This comes from a couple of features coming from the organization's strengths. In analyzing INTERPOL's strengths in the case study, the starting point should be the issuance of The Red Notice, so that he could be identified and tracked across borders thanks to the Red Notice, which served as a kind of global arrest warrant. The detection of terrorists via facial recognition also showed their capacity to adapt and use modern technological features. Recognizing the growing influence of technology in contemporary terrorism, Interpol used its digital forensics and cyber skills to track down and disrupt the Shadow Brotherhood's online presence and Rehman's digital footprint. This meant keeping an eye on attempts to radicalize people online, tracking conversations that were encrypted, and seeing potential cyber threats connected to the group's operations. Moreover, issuing a red notice was a crucial element in notifying regional law enforcement and border security forces that were involved. Also, to locate the leader, real-time cross-border coordination and intelligence sharing were necessary. Law enforcement agencies from the impacted nations collaborated with Interpol's General Secretariat during Operation Swift Response to coordinate their efforts in identifying and detaining significant members of the Shadow Brotherhood. This seamless collaboration cut across national barriers, increasing the operation's efficacy that shows INTERPOL's global network and information-sharing capacities. To share information and intelligence regarding Attiq Ur Rehman, Interpol's enormous global network of member nations was essential. International law enforcement agencies worked together to facilitate quick data exchange and analysis. Lastly, it is beneficial to mention that INTERPOL's strength comes from its extensive databases such as the Stolen and Lost Travel Documents (SLTD) database and the Foreign Terrorist Fighters (FTF) database, which played a crucial role in identifying and tracking the movement of suspected terrorists. Authorities were able to stop members of the Shadow Brotherhood and leader Rehman from traveling undetected and crossing international borders thanks to the use of these databases. Mentioning the weaknesses faced in the operation, the lack of enforcement authority can be the biggest issue. Due to its lack of direct enforcement authority, Interpol was unable to independently make arrests or launch investigations. Instead, it was dependent on member nations' readiness to respond to alarms and work together to capture the terrorists for it to be effective. Also, because of the delicate nature of cross-border terrorism and the involvement of numerous nations, Interpol had to carefully consider political aspects. Due to diplomatic or political concerns, several nations might have been reluctant to fully collaborate, which could have slowed down the investigation's progress.

As a result of the operation, numerous high-ranking members of the Shadow Brotherhood were detained in numerous nations as a result of the cooperative efforts of law enforcement authorities and Interpol's assistance. The command structure and operational capabilities of the organization were seriously affected by these arrests. The operation's success, severely smittened the Shadow Brotherhood's financial resources by monitoring the group's financial activity and determining their financing sources. Several significant terrorist cells linked to the Shadow Brotherhood were found and destroyed as a result of Operation Swift Response, impeding further assaults. The prompt and real-time exchange of intelligence among participating nations was crucial to the operation's success. Interpol's capacity to use technology and adjust to new dangers, such as cyberterrorism, was also crucial in preventing the Shadow Brotherhood from carrying out its operations (Deflem, 2006). The operation served as a reminder of the value of solid, coordinated, and global cooperation in successfully countering transnational terrorist threats. The case emphasizes the value of ongoing cooperation among member nations and Interpol's role as a mediator in negotiating delicate political dynamics to protect regional and global security.

In conclusion, the case study Operation Swift Response reveals both Interpol's weaknesses and strengths in the effort to counter cross-border terrorism through its collaborative approach, technological capabilities, and commitment to facilitating international cooperation. Interpol's global network, information-sharing systems, and criminal databases are essential for coordinating global efforts and apprehending terrorists, despite its lack of enforcement authority and potential political considerations.

4. Adapting and Strengthening to Enhance International Cooperation

As mentioned in the previous chapter in recent years new terrorism threats have emerged such as the rise of transnational extremist networks, online radicalization, lone wolf attacks, emerging technologies, financing methods, cyberterrorism, CBRN terrorism, and hybrid threats. These unique threats necessitate proactive and adaptive approaches to fight new-age terrorism. However despite the urgent need for collaboration, governments, and international organizations that are actively fighting with cross-border terrorism such as INTERPOL and the UN still facing some challenges that hinder cooperation. These challenges are mentioned in the previous chapter in detail. By addressing these challenges this chapter will focus on how to overcome these challenges by adapting and strengthening international cooperation in the face of newly emerged threats. As the landscape of terrorism changes, new

methods should be employed by the coutnering sides to effectively combat these new threats. This chapter will try to focus on these potential methods and strategies that might be applied to strengthen the cooperation by highlighting the areas that may be potentially productive to counter addressing the new threats. These suggestions will cover, how to use technology and innovation for collaboration, how to promote regional partnerships and cooperative projects, how to improve public-private partnerships, how to strengthen legal frameworks and coordination mechanisms, and how to create comprehensive strategies to counter hybrid threats. The subsequent section will delve deeper into each strategy by providing a comprehensive analysis of their potential to enhance international cooperation in countering cross-border terrorism. This section aims to contribute to the literature on cross-border counterterrorism cooperation by assessing the current status of international cooperation and highlighting the development opportunities. The conclusions and suggestions made here will help policymakers, law enforcement, and researchers in the field of counterterrorism to have a better understanding of how cross-border terrorism is evolving and how to improve global cooperation in the face of newly emerging threats.

4.1. Leveraging Technology and Innovation for Cooperation

As new-age terrorism started with the advancement of technology, in the face of new threats, technology has the most important place in countering these new threats. Even though new technologies gave space for more advanced terror operations they also provided opportunities for enhanced cooperation among nations in countering these threats. One of the crucial areas to use is information sharing and intelligence gathering. The importance of intelligence and real-time information exchange have been analyzed in the previous chapters as well as case studies. So, to leverage these areas advanced data analytics, artificial intelligence, and machine learning algorithms can be used to analyze big amounts of data from multiple sources to identify patterns, trends, and potential threats to provide timely and prompt responses to potential terrorist attacks (Cohen, 2002). As we also saw in the case studies communication between law enforcement is crucial in both impeding the potential terror attack especially in joint operations or in the case of a response to a terror attack. Thus, forming encrypted communication channels are essential part of sharing confidential and sensitive information among nations. Having cohesive information with other countries is as important as acquiring the information itself to conduct flawless cooperation. Standardizing data formats, communication protocols, and information-sharing procedures can be used to enable

confidential cooperation and integration of intelligence efforts. This can also be useful in overcoming jurisdictional complexities and legal barriers that often result from insufficient or ineffective communication that eventually hampers international cooperation. Additionally, technology use can be quite effective in detecting and stopping internet radicalization and propaganda. Innovative strategies, such as the creation of algorithms or AI-powered content analysis to find and delete extremist propaganda and critical content from internet platforms, can help to stop the process of radicalization and recruiting. Additionally, employing social media monitoring technologies can help identify those who are susceptible to radicalization and allow for more targeted interventions (Cohen, 2002). Also cooperating with tech companies is another step governments can take to fight online radicalization by tracking extremist activities on digital platforms. Another important area that can be leveraged by technology is border security and surveillance. Implementing advanced surveillance systems like biometric identification technologies and facial recognition systems can create a great difference when it comes to border security which means detecting and tracking individuals involved in cross-border terrorism when they try to cross borders. Another technology that can be used to leverage surveillance is unmanned aerial vehicles like drones with high-resolution cameras and sensors as well as satellite imagery and geographic information systems. They can provide real-time situation updates and support in the borders or remote areas monitoring and detecting and tracking terrorist activities (Cortright, 2017). Collaboration efforts to obtain and examine such data can help to develop a thorough picture of the threats posed by cross-border terrorism. Lastly, cybersecurity collaboration can be formed to fight cyber threats. Working together on cyber threat analysis becomes essential as terrorist organizations rely more and more on the internet. Nations can combine their knowledge and resources to study cyber threats, spot flaws, and develop efficient defenses. To lessen the effects of cyberattacks, unified cyber incident response procedures must be developed. A quick and coordinated reaction to cyber events can be ensured by international cooperation, lowering the possibility of interruptions brought on by cyberterrorism (Zerzri, 2017). Given how quickly cyber threats can emerge, capacity-building and training initiatives should be applied to improve the cybersecurity expertise of law enforcement and intelligence officers. International collaborations can promote talent development and knowledge exchange. It is important to keep in mind that utilizing technology in counterterrorism activities comes with dangers and problems. Some of the most important challenges that need to be addressed are privacy issues, ethical issues, and the possibility of technology being misused. Therefore, it is essential to

strike a balance between using technology to foster cooperation and making sure that civil liberties and individual rights are protected (Hafner-Burton & Shapiro, 2010).

In conclusion, leveraging technology and innovation is not just an option but a need for improving international collaboration in preventing cross-border terrorism, particularly after the emergence of new threats. The effectiveness of counterterrorism initiatives can be considerably increased by the use of modern data analytics, secure communication channels, and creative methods to combat internet radicalization. However, it is important to address the challenges and risks associated with the use of technology to ensure a comprehensive and balanced approach. To ensure a thorough and well-rounded strategy, it is crucial to address the risks and obstacles related to the use of technology.

4.2. Promoting Regional Partnerships and Collaborative Initiatives

Cross-border terrorism sometimes requires regional response alongside international cooperation when the threats are specific to one region. This section will explore the importance of regional partnerships and promoting collaborating initiatives to adding up to enhance international counter-terrorism cooperation as a result. Forming a regional cooperation, between neighboring countries or regional organizations enables the development of more coordinated and effective strategies to fight emerging threats when it comes to cross-border terrorism.

To understand the importance of regional initiatives, there are three points we should mention. The first one is threat proximity. Terror threats especially the newly emerged ones often cross their borders and threaten the neighboring countries before any other country. States can pool resources, share intelligence, and react more quickly to dangers that arise in the region by working together at the regional level. Regional collaborations allow for a better understanding of the linguistic, historical, and cultural circumstances in which terrorist organizations operate. Given that it only enables techniques that are specific to regional situations, this insight is not valid for counterterrorism operations. The rise of cross-border terrorism has a variety of reasons, such as political unrest, socioeconomic problems, and ideological fanaticism. By coordinating activities to advance stability, economic growth, and social cohesion, regional initiatives can address some of these core problems more successfully. The South Asian Association for Regional Collaboration (SAARC) is one example of regional collaboration that has been successful. Afghanistan, Bangladesh, Bhutan, India, Maldives, Nepal, Pakistan, and Sri Lanka are SAARC members and have put in place

structures for cooperation in several fields, including counterterrorism. Important legal structures that promote collaboration among participating nations in the fight against terrorism include the SAARC Regional Convention on Suppression of Terrorism and its Additional Protocol. The Association of Southeast Asian Nations (ASEAN) has also achieved notable strides in fostering regional cooperation against terrorism. For member states to improve cooperation in areas including intelligence sharing, capacity building, and joint exercises, the ASEAN Convention on Counter-Terrorism serves as a framework. The ASEAN Institute for Peace and Reconciliation's formation bolsters regional efforts to combat terrorism. Another topic is strengthening already existing regional organizations (Ryacudu, 2018). As we mentioned regional organizations are essential for promoting collaboration between neighboring and geographically close nations. These organizations should be strengthened to better respond to international terrorism. Some steps can be taken to reach this aim. The first one is forming information-sharing mechanisms that can provide real-time information. Real-time intelligence exchange requires member governments to establish efficient and safe information-sharing methods. To make this process easier, regional organizations can act as middlemen, making sure that sensitive information is properly shared while preserving national sovereignty. These countries can also perform joint training against these threats to develop coordination and interoperability among subjected regional security forces. These activities help build trust and familiarity, creating a more seamless response to potential threats. The last step can be developing standard operating procedures. To create standardized operational procedures for handling various kinds of cross-border terrorist threats, regional organizations can collaborate with member governments. Standard operating procedures improve the effectiveness of joint operations by streamlining decision-making procedures (Rosand et al., 2008).

Promoting new cooperation between law enforcement is another important point of fighting cross-border terrorism as it can ease the process of apprehending suspects and distributing terrorist networks. Signing bilateral and multilateral agreements is a good way of promoting mutual legal assistance, extradition, and joint investigative teams. These agreements can be useful in providing a cohesive legal framework for countering cross-border terror efforts and ensuring terrorists cannot find safe havens in neighboring countries. Forming joint task forces from different countries' law enforcement can also be useful to have more effective intelligence sharing and for targeted operations. An example of this initiative is India and Bangladesh's Joint Task Force for Intelligence Sharing. The force was established to enhance cooperation in intelligence sharing and border security. Successful operations against terrorist

organizations operating along the India-Bangladesh border have been implemented in this alliance. Additionally, cooperative projects like joint military exercises, seminars, and training courses can promote the sharing of best practices and improve the capacity of participating nations to combat cross-border terrorism. The last way to improve regional partnerships is by employing public-private partnerships. When combating cross-border terrorism, especially with the new threats, public-private partnerships can be very useful for government initiatives. To encourage such alliances governments can work with technology corporations to spot and stop attempts of online radicalisation. The creation of algorithms to identify extremist content or cooperative awareness initiatives to advance digital literacy and critical thinking are two examples of this collaboration as mentioned earlier. To fight against radicalization and in favor of societal cohesiveness, civil society groups can be crucial. Governments can collaborate with these groups to put community-based preventative programs and initiatives for people who are at risk of radicalization into place. The international community can create a more solid and united front against the expanding challenges of cross-border terrorism by encouraging regional partnerships and cooperative activities. For long-term security and stability in the face of newly developing challenges, states must acknowledge the interconnectedness of these dangers and welcome cooperation actions that cross national boundaries (Islam, 2011). So, all these strategies and programs can offer chances for knowledge exchange, capacity building, and establishing confidence between participating nations. but it should be remembered that fostering regional alliances and cooperative projects calls for political will, trust-building techniques, and a common awareness of regional risks. Regular dialogues, high-level meetings, and diplomatic initiatives are crucial to promoting cooperation and resolving any problems or difficulties between member nations. To strengthen international collaboration in combating cross-border terrorism, it is essential to promote regional alliances and cooperative activities. Bilateral alliances and regional groups like SAARC and ASEAN give nations a place to interact, exchange intelligence, and coordinate activities. Through coordinated training sessions, workshops, and exercises, collaborative projects promote cooperation even further.

4.3. Enhancing public-private partnerships in counter-terrorism efforts

Traditionally, counter-terrorism was the issue for government or security agencies to deal with but with the introduction of new threats, this situation also changed. New threats necessitated the collaboration of both the public and private sectors to combat these challenges mutually. The public sector, like law enforcement and intelligence organizations, has the

power, means, and know-how to investigate, prevent, and respond to terrorist activity. On the other hand, the private sector contributes specialized skills, modern technology, and a global reach that may greatly support counterterrorism activities. Forming successful alliances requires an understanding of both sectors' advantages and limitations. Anyhow, forming a successful collaboration brings many benefits like valuable information such as data on financial transactions, cyber threats, and emerging technologies as well as mechanisms for secure and timely information sharing that the private sector can bring to the table and governments make use of. Private businesses also are very much at the forefront of technical advancements. By utilizing their knowledge in fields like cybersecurity, artificial intelligence, and data analytics, counterterrorism initiatives will be better able to identify and stop terrorist activity early on. Due to their extensive international operations, multinational firms are well-positioned to identify and address cross-border threats. Governments can expand the reach and efficacy of counterterrorism operations by utilizing the worldwide networks and resources of private organizations through public-private partnerships. However budgetary restrictions and a lack of resources frequently hamper counterterrorism activities. By forming these alliances, governments can gain access to extra resources, funds, and competencies through partnerships that they might not otherwise have. It also should be mentioned that companies and organizations in the private sector are frequently flexible and quick to adjust to changing conditions (Morabito & Greenberg, 2005). Governments can benefit from these organizations' creative thinking and adaptability by working with them; these traits are crucial for combating the ever-evolving terrorist techniques.

However establishing public-private partnerships can be effective, but it also needs precautious and a systematic approach. This is possible to achieve in a couple of ways. Such as developing clear and agreeable frameworks and guidelines for collaboration. Openly assigning the responsibilities, and expectations of both public and private entities. These frameworks must guarantee compliance with the relevant laws and regulations, safeguard private data, and build trust between parties. Security and confidentiality should come first when sharing information across the public and private sectors. To safeguard sensitive data and defend against potential risks posed by potential actors, strong cybersecurity procedures and secure communication routes are required. Thus, governments might provide incentives to private enterprises, such as non-financial advantages, public recognition, or priority access to government contracts, to promote active engagement as gaining the commitment of partners in the private sector requires open communication about the advantages of partnership. Building capacity and specialized training may also be necessary for the public and private sectors to

comprehend one another's operational processes, terminologies, and challenges. Workshops and capacity-building programs help close the knowledge gap and make cooperation run more smoothly. Lastly, to evaluate their efficacy and highlight areas for development, public-private partnerships should undergo regular examination. The collaboration will stay active and responsive to new risks thanks to feedback systems and routine assessments (Morabito & Greenberg, 2005).

Showing the potential of public-private partnerships and as an inside of counter-terrorism efforts Global Internet Forum to Counter Terrorism (GIFCT) is a good example. The GIFCT is a global partnership between governments and leading technology companies like Facebook, Twitter, YouTube, and Microsoft. It attempts to stop the dissemination of terrorist content online and stop the online operations of terrorist groups. The GIFCT promotes information exchange, technical cooperation, and research to create efficient counterterrorism tools and strategies for digital platforms. Through this collaboration, the participating businesses collaborate closely with governments and international organizations to find and delete terrorist information, spread counter-narratives, and improve the use of technology to counteract online radicalization. Through the agreement, best practices will be exchanged, databases of terrorist content will be created in collaboration, and technical tools like artificial intelligence and machine learning algorithms will be used to find and delete extremist information. Along with training programs and seminars, the relationship also entails activities to improve the ability of both the public and commercial sectors to combat cyberterrorism. The GIFCT is a prime example of successful public-private cooperation since it makes use of the knowledge, capital, and technological prowess of major technology companies to support and aid governments in their counterterrorism operations (GIFTC, n.d.). The collaboration will work together to prevent terrorist organizations from misusing the internet's resources and make it a safer place. Although they do offer many advantages, public-private partnerships are not without challenges. Addressing issues with data privacy, liability, conflicting interests, and power dynamics between sectors is crucial. If collaborative efforts are to be maintained and effective in the long run, it will be essential to understand and address these difficulties. In order to address these challenging concerns, public-private collaborations will become even more important as cross-border terrorism threats grow. Governments, private companies, and international organizations must collaborate to foster an environment of trust, cooperation, and information sharing. If we are to increase the efficiency of public-private partnerships and defend global security in the face of new threats, we must embrace innovation, technology, and adaptation.

4.4. Strengthening Legal Frameworks and Coordination Mechanisms

Legal barriers are one of the difficult challenges when it comes to international cooperation for law enforcement and counter-terrorism agencies as terrorists tend to exploit the jurisdictional complexities and legal gaps to escape from capture and prosecution, especially in cases of cross-border terrorism. To enhance international cooperation in countering cross-border terrorism effectively, it is crucial to strengthen legal frameworks and coordination mechanisms at both national and international levels. This section explores key strategies and measures that can be adopted to address legal challenges and promote more cohesive cooperation. This is possible firstly by harmonizing legal definitions. As mentioned in the first chapter, there is no consensus on the definition of terrorism and cross-border terrorism (Young, 2006). Different legal conceptions of what constitutes terrorism are common among nations, which causes inconsistencies in the prosecution of terrorist activities and impedes international cooperation attempts. The international community must work to harmonize legal definitions of terrorism and cross-border terrorism to resolve this problem. Multilateral agreements or conventions that establish a common framework for comprehending and punishing terrorist actions could help achieve this. Another big issue is seen in the process of extradition. Extradition is a crucial part of the legal process that brings terrorists to justice. Thus, strengthening extradition agreements is another necessary measurement. However, extradition procedures can be complex, time-consuming, and influenced by politics. Countries should evaluate and update existing extradition treaties to make sure they include a wide variety of terrorist offenses and allow for prompt processing in order to improve extradition mechanisms. Building confidence and collaboration between nations is also essential to facilitate the quick extradition of suspects. Improving channels for mutual legal assistance is another essential step for effective international collaboration in terrorism investigations and prosecutions. Mutual legal assistance treaties can be made stronger by regulated procedures and by reducing bureaucratic obstacles. The transmission of intelligence and evidence can be sped up by designating specific channels and focal points within law enforcement agencies to handle cross-border requests. The exchange of information is essential for successful counterterrorism measures. The capacity to locate and capture terrorist operators might be considerably improved by establishing transparent and secure intelligence-sharing protocols between nations. These protocols should take data privacy, secrecy, and the safeguarding of sensitive information into account while making sure that crucial intelligence is delivered to the targeted

law agencies on time. Another point is for some terrorist offenses. Countries should think about extending their extraterritorial jurisdiction. This would enable them to pursue those responsible for cross-border terrorism, even if the crimes were conceived of or carried out outside their national borders. However, an attempt or change should be made by respecting the sovereignty of the subject nation and must be compliant with international law. Another step can be improving international legal documents, such as conventions and resolutions of the United Nations Security Council (UNSC), which are essential for directing global collaboration in the fight against terrorism. To fight newly emerging threats, countries should strengthen their already existing fighting mechanisms as well as work on their ability to evolve those mechanisms into internationally functioning ones. The systems that are observing and controlling these mechanisms also should be improved. The development of cross-border legal knowledge can be described as a final step. To manage cross-border terrorism situations, law enforcement, and judicial professionals need to work on improving their legal understanding. Through training programs and capacity-building efforts, the caliber of legal responses and understanding of international legal systems can be increased. (Young, 2006).

This chapter on "Strengthening Legal Frameworks and Coordination Mechanisms" has examined the vital importance of establishing efficient coordination mechanisms and finding common ground for legal frameworks in the fight against transnational terrorism. In order to address the changing threats posed by terrorism in today's globalized world, this chapter attempted to emphasize the importance of legal and coordination frameworks by examining the barriers to international cooperation, evaluating existing practices, and proposing potential improvements. In conclusion, it is critical to creating legislative frameworks and coordinating structures in light of the constantly changing nature of cross-border terrorism. The chapter emphasized the importance of strong, ongoing international cooperation as the basis for a successful global counterterrorism strategy. The international community can create a unified front against the threat of terrorism by resolving the difficulties presented by jurisdictional complications, different country priorities, resource limitations, and technology improvements. Countries can improve their capacity to fight and decrease the threats presented by cross-border terrorism by putting into practice the suggested guidelines and future initiatives. As the threat landscape continues to evolve, continuous efforts to adapt and improve legal and coordination frameworks remain essential for safeguarding international peace and security in the face of newly emerging terrorism threats.

4.5. Hybrid Threat Responses and Comprehensive Approaches

In the last part of this section, hybrid threats and potential answers to them will be examined. Because hybrid threats incorporate conventional and unconventional approaches from several fields, they pose a complicated and multifaced challenge and demand innovative responses that involve the collaboration of nations, international organizations, and the private sector. This section delves into "Hybrid Threat Responses and Comprehensive Approaches," which forms a backbone component in enhancing international cooperation. to counterterrorism efforts. A comprehensive strategy that includes a variety of tactics is needed to respond to hybrid threats effectively examining the various aspects of hybrid threat responses and suggesting all-inclusive solutions to these evolving problems.

The first step is understanding the threats to be able to respond to them. As it was mentioned in previous chapters in detail, Hybrid threats combine a variety of tactics to accomplish their goals, including conventional military force, irregular warfare, information warfare, cyberattacks, economic pressure, and political manipulation. These threats frequently take advantage of weak spots in many industries and use advanced technology to their advantage. As in many of the counter-strategies we mentioned, countering hybrid threats is firstly possible with improved intelligence-sharing mechanisms among subject countries and relevant international organizations. Collaboration and real-time data exchange are crucial because hybrid threats frequently take advantage of information gaps and inconsistencies. In order to identify and respond to emerging threats quickly, secure communication routes and platforms for intelligence exchange must be established. Another point is strengthening cybersecurity measures. Stronger cybersecurity measures are essential since hybrid threats typically include cyberattacks. Governments and corporations should make investments in modern cybersecurity technologies, regularly review their weak points, and implement effective attack response strategies. Building a coherent and well-coordinated cybersecurity system requires collaboration between the public and private sectors. Hybrid threats frequently target crucial infrastructure, including power grids, transportation networks, and communication systems. Countries should work together to share best practices and knowledge in safeguarding and protecting vital infrastructure in order to improve international collaboration. Cross-border exercise and coordinated contingency planning will assist in boosting overall resilience. Also, transnational crimes including money laundering, human trafficking, and drug smuggling that fund terrorist organizations are commonly involved in hybrid threats. These illegal networks can only be neutralized by cutting off their financial sources for hybrid threats and this is only possible with joint operations and strengthened cross-

border law enforcement collaboration. The ability of the general public to recognize and respond to hybrid threats is another crucial point. Governments should spend money on public awareness initiatives to inform citizens about the changing nature of threats and encourage being cautious toward potential situations. Potential harms can also be avoided by strengthening community resilience and encouraging citizen reporting of suspicious activity. Hybrid threats require a comprehensive strategy that encompasses all relevant government departments and stakeholders. A coordinated response across several sectors, including defense, intelligence, law enforcement, economic, and diplomatic operations, is ensured through a whole approach both from the government and society. Like in cross-border terrorim in general hybrid threats also take advantage of legal gaps and differences in national legal systems. Thus, strengthening international agreements and legal frameworks is also effective in more efficient international collaboration and coordination in the fight against hybrid threats. This can entail coordinating extradition agreements and counter-terrorism laws (Gregory, 2018).

The hybrid threat scenario is dynamic and requires ongoing evaluation and modification of counterterrorism policies. The international community will be able to remain ahead of growing dangers with regular assessments of cooperative arrangements and the identification of emerging difficulties. Thus, dealing with hybrid threats necessitates a comprehensive and multifaced strategy that goes beyond conventional counterterrorism strategies. The international community can successfully navigate the changing landscape of cross-border terrorism by improving intelligence sharing, strengthening cybersecurity measures, encouraging cross-border law enforcement cooperation, and adopting a holistic approach. For governments and international organizations to remain prepared in the face of constantly evolving hybrid threats, cooperation, and constant adaptation their reponses are essential.

The chapter "Adapting and Strengthening to Enhance International Cooperation" analyzed the crucial elements of navigating the shifting cross-border terrorist landscape and the necessity of adapting and strengthening international cooperation in the face of recently developing threats in detail. A dynamic and all-encompassing strategy is required to successfully address these challenging issues as terrorism evolves, affected by technical developments, shifting ideologies, and hybrid tactics. In order to strengthen international collaboration in the fight against terrorism, a number of significant themes that illustrate the significance of cooperative efforts and forward-thinking tactics evolved throughout this chapter, including: leveraging Technology and Innovation, Promoting regional partnerships and collaborative initiatives, enhancing public-private partnerships in counter-terrorism efforts,

strengthening legal frameworks and coordination mechanisms and hybrid threat responses and comprehensive approaches. International collaboration needs to be flexible, adaptable, and quick to respond as the area of cross-border terrorism keeps changing. Identifying the difficulties and problems involved in preventing terrorism is a vital step in creating successful measures. Obstacles such as a lack of resources and different national priorities may exist, but these obstacles can only be overcome by focusing on the common goal. In conclusion, the ability of nations and international organizations to strengthen cooperation and continuously modify their tactics will determine the success of combatting cross-border terrorism. The international community can successfully deal with the recently emerging threats only by effectively utilizing technology, encouraging and forming regional partnerships, establishing public-private collaborations, improving legal frameworks, and adopting all-encompassing strategies. We must remain cautious of evolving situations, take lessons from the past, and build a common commitment to preserving world security and stability as we move forward. We can only create a society that is safer and more resilient for future generations through consistent and coordinated efforts.

5. Conclusion and Policy Recommendations

The last and conclusive chapter of this thesis aims to provide a comprehensive summary of the findings and present policy recommendations for enhancing international cooperation in countering cross-border terrorism. We have investigated the evolving nature of cross-border terrorism, evaluated the recently emerging threats, examined the difficulties and challenges in international counter-terrorism cooperation, assessed the existing mechanisms of cooperation, and discussed methods for adapting and enhancing global cooperation throughout this research. The research is brought to a close in this last chapter, which also provides useful insights into the steps that may be taken to confront the developing nature of cross-border terrorism and promote productive international cooperation. By putting into practice the policy ideas presented in this chapter, nations can strengthen their coordinated efforts to combat cross-border terrorism and create a more secure and safer world.

5.1. Policy Recommendations for Enhancing International Cooperation

One of the most significant dangers of today's international security is cross-border terrorism. The only possible way to defeat this threat is through international cooperation and

coordinated response. As these groups have advanced abilities like using leveraged technology, operating transnationally, and adopting and evolving their strategies quickly as and if needed, fighting with these groups requires a well-coordinated and all-encompassing approach. Many sides of international cooperation in the context of countering terrorism have been studied in this thesis, along with the characteristics, history, present threats, and challenges of cross-border terrorism. To keep existing in this ever-changing world of threats, finding a solution and successful cooperation is a must for everyone and every nation. Some of the policy suggestions in this section were covered in more detail in the chapter previously. They deal with the need for a more cohesive and efficient framework for international cooperation. These actions can help nations enhance their counter-terrorism cooperation, enhance their national security, and reduce the impact of cross-border threats. These recommendations offer reachable tactics, from regional alliances to intelligence-sharing platforms, to improve international cooperation and safeguard our shared global security. There are seven recommended policies for enhancing international cooperation and these are:

a. Strengthening Information-Sharing Mechanisms: These steps are crucial for strengthening nations' cooperation when it comes to fighting terrorism as well as enhancing national security while decreasing the impact of cross-border threats. These suggestions provide practical strategies to strengthen international collaboration and protect our common global security, from intelligence-sharing platforms to regional alliances and beyond.

b. Enhancing Interagency Collaboration: To have an effective and flawlessly working international cooperation that fights cross border terrorism every countries' relevant bodies must work closely with each other. They should coordinate their efforts, and share their knowledge and experience. To escalate the decision-making process, the government should form interagency forces. This will make it easier to navigate jurisdictional complications and provide a thorough and well-planned response to any threats.

c. Strengthening Regional Partnerships: In the fight against global terrorism, regional cooperation is crucial. Nations should take a proactive role in regional conferences and initiatives in order to strengthen information sharing, intelligence coordination, and joint operations. The Association of Southeast Asian Nations (ASEAN) and the

European Union are two examples of regional organizations that can serve as venues for fostering collaboration and developing shared strategies.

ç. Investing in Capacity Building: When attempting to deal with cross-border terrorism, many countries encounter resource limitations and capacity challenges. International collaboration should prioritize projects that aim to build capacities, like technical support, training programs, and resource sharing. The ability of less developed states to acquire intelligence, secure their borders, and conduct counterterrorism operations should be strengthened with support from developed nations.

d. Strengthening Legal Frameworks: International collaboration in the fight against transnational terrorism requires robust legal frameworks that permit extradition, information sharing, and cooperative investigations. Nations should review and update it in order to continue successful collaboration and keep domestic legislation in line with international standards. An attempt should be made to unify legal systems amongst nations in order to lessen legal barriers and encourage seamless cooperation.

e. Promoting Public-Private Partnerships: To fight global terrorism, the public and private sectors must collaborate. Governments should foster partnerships with private technology businesses, financial institutions, and other parties that might be relevant in order to take advantage of their expertise, resources, and technological capabilities. Collaborations between the public and private sectors can enhance information sharing, financial intelligence, and the development of innovative defenses against emerging threats.

f. Strengthening International Organizations: International organizations like INTERPOL and the UN are essential for establishing global collaboration. By providing enough funds, resources, and political backing, governments should support these groups so that the effectiveness and efficiency of these institutions in preventing international terrorism can be improved and increased.

In conclusion, an overall multifaceted strategy for increasing international cooperation in countering cross-border terrorism must include strengthening information-sharing mechanisms, encouraging interagency collaboration, fostering regional partnerships, investing

in capacity building, strengthening legal frameworks, promoting public-private partnerships, and supporting international organizations. These policy recommendations can assist countries in navigating the altering cross-border terrorism environment and reducing the risks posed by recently emerging problems.

5.2. Summary of findings

This thesis aimed to present new sides of cross-border terrorism in the face of emerging threats. The study discovered many major conclusions through an in-depth examination of the literature and evaluation of present international collaboration structures. As the first step, the definition of cross-border terrorism and international terrorism has been explained as well as clearifying the difference between the two notions. Cross-border terrorism is any act of violence that is perpetrated outside of the subject country's border, mostly by a non-state actor. For counterterrorism measures to be successful, it is important to comprehend and act according to these differences. A thorough analysis of the development of cross-border terrorism risks showed the emergence of various fresh hazards. Transnational extremist networks, cyberterrorism, CBRN terrorism, hybrid threats, online radicalization, lone wolf attacks, developing technologies, and finance techniques are a few of these. Innovative solutions are needed to address these recently discovered risks since they pose major barriers to international cooperation. The report identified several challenges and impediments to global counterterrorism collaboration. Jurisdictional complications and legal obstacles, varying national agendas and interests, resource limitations, technological difficulties, and gaps in the body of existing literature are among the major obstacles to effective collaboration. To comprehend the difficulties experienced by international cooperation during the real incident, the case of the Mumbai Attacks was investigated. To effectively combat cross-border terrorism, these case studies stressed the importance of fast information exchange, good cooperation, and overcoming political impediments. The evaluation of current methods for international cooperation placed a major emphasis on how well INTERPOL and the UN countered transnational threats. Although both groups play significant roles, their effectiveness is limited by a variety of factors, such as limited funding and the need for more joint action between law enforcement. The effectiveness of both groups was also deeply analyzed using the case studies of the 2016 Brussels bombings and Swift Operation. In light of the findings, a number of recommendations were made to change and enhance international collaboration. Critical steps to fight with hybrid threats have been mentioned such as maximizing technology and

innovation, fostering regional collaborations, improving public-private partnerships, strengthening and making efforts for more common legal frameworks, and lastly coordination mechanisms. This thesis finishes with a thorough examination of cross-border counterterrorism cooperation in light of the emergence of new threats. The findings highlight the need for stronger international cooperation, the importance of overcoming difficulties, and the possibilities for partnering with the private sector and using technology to enhance counterterrorism activities. The results also demonstrate how the global community may strengthen its ability to stop and effectively respond to cross-border terrorist attacks. The policy suggestions mentioned in the following section offer helpful guidelines for fostering global collaboration in the fight against transnational terrorism. This study lays the groundwork for further research in this crucial area while also advancing our understanding of terrorism as a whole.

5.3. Conclusion and Implications for future research

In conclusion, This thesis has examined the features, development, and new risks of the complex and ever-evolving phenomena of cross-border terrorism. Additionally, it has reviewed the current mechanism in place to deal with cross-border threats and critically studied the difficulties and barriers encountered in international counterterrorism cooperation. Additionally, in order to effectively tackle the threat of cross-border terrorism, the thesis has suggested measures to modify and strengthen international collaboration.

The literature research made it clear that cross-border terrorism differs from international terrorism since it operates beyond national borders and takes advantage of legal complications. A comprehensive and collaborative response from the international community is required in light of the emergence of transnational extremist networks, internet radicalization, lone wolf attacks, and developing technology that have further complicated the security environment. The importance of overcoming jurisdictional complications, divergent national interests, resource restrictions, and technology challenges were brought out in the analysis of barriers to international counterterrorism cooperation. The examination of the existing international counterterrorism cooperation institutions, primarily Interpol and the UN, showed areas for improved cooperation as well as the possibility for further cooperation. The suggestions made in this thesis offer various ways to improve international collaboration in preventing international terrorism. Joint operations and the sharing of intelligence can be facilitated by utilizing technology and fostering regional alliances. Resilience and response

capacities can be improved by establishing public-private partnerships. Creating strong legal frameworks and coordination structures can also facilitate collaboration and overcome jurisdictional barriers. An all-encompassing defense against various terrorist techniques can be ensured by emphasizing hybrid threat responses and comprehensive approaches.

While this thesis has improved our understanding of international collaboration and cross-border terrorism, there are still several implications for future studies.

1. Cyberterrorism and Emerging Technologies: Further study is required to examine the possibility of cyberterrorism and the use of developing technologies by terrorist organizations given the rapid growth of technology and its growing impact on terrorist activities. For the purpose of developing effective countermeasures, it is essential to comprehend how cross-border terrorism may be affected by artificial intelligence, drones, and other disruptive technologies.

2. Regional Dynamics: Investigating the impact of regional dynamics on the development of international terrorism can yield insightful information. Developing specialized cooperative strategies can benefit from analysis of how regional conflicts, geopolitical circumstances, and regional organizations affect the spread of terrorism.

3. Counter-terrorism Financing: Cutting down the financial backing for terrorist organizations requires a better investigation of the networks and financing strategies they employ. Developing targeted strategies to disrupt these networks can be made easier by having an understanding of money laundering methods, virtual currencies, and criminal financing sources.

4. Victim-Centered Approaches: More studies can be done on victim-centered strategies used in counterterrorism activities. More thorough counter-terrorism efforts can benefit from an understanding of victim and family requirements as well as post-attack assistance and recovery procedures.

5. Role of Media and Online Platforms: It is crucial to look into how media and online platforms influence the spread of terrorist propaganda and radicalization. It is vital to investigate how information spreads and how it might be controlled without impinging on the right to free expression.

6. Soft Power and Ideological Counter-Narratives: Understanding the efficacy of soft power and ideological counter-narratives in combating the terrorists' core ideologies will help us understand how important culture, education, and communication are in preventing radicalization.

In conclusion, this thesis contributes to existing literature and knowledge on international collaboration and cross-border terrorism in the fight against this worldwide danger. The international community may improve its ability to effectively prevent and respond to cross-border terrorist operations by addressing the highlighted problems and implementing the suggested measures. To remain ahead of the changing threat landscape and ensure a safer and more secure world, ongoing research and collaboration between researchers, policymakers, and practitioners are essential.

References

1. Anna-Katherine Staser Mcgill, & Gray, D. H. (2012). Challenges to international counterterrorism intelligence sharing. *Global Security Studies*, *3*(3).
2. Åshild Kolås. (2010). The 2008 Mumbai terror attacks: (re-)constructing Indian (counter-)terrorism. *Critical Studies on Terrorism*, *3*(1). https://doi.org/10.1080/17539151003594244
3. Badey, T. J. (1998). Defining international terrorism: A pragmatic approach. *Terrorism and Political Violence*, *10*(1). https://doi.org/10.1080/09546559808427445
4. BBC News. (2016, April 9). Brussels explosions: What we know about airport and metro attacks. *BBC News*. https://www.bbc.com/news/world-europe-35869985
5. Boaz Ganor. (2002). Defining terrorism: Is one man's terrorist another man's freedom fighter? *Media Asia*, *29*(3). https://doi.org/10.1080/01296612.2002.11726675
6. Byman, D. (2017). How to hunt a lone Wolf: Countering terrorists who act on their own. *Foreign Affairs*, *96*(2).
7. Cohen, E. A. (2002). Making the nation safer: The role of science and technology in countering terrorism. *Foreign Affairs*, *81*(6). https://doi.org/10.2307/20033374
8. Cortright, D., Fairhurst, R., & Wall, K. (2017). *Drones and the future of armed conflict: ethical, legal, and strategic implications*. The University Of Chicago Press.
9. Cortright, D., Lopez, G. A., & Hamilton, L. H. (2007). *Uniting against terror: Cooperative nonmilitary responses to the global terrorist threat*.
10. European Council. (2002). *Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States - Statements made by certain Member States on the adoption of the Framework Decision*.
11. Crenshaw, M. (2008). The Debate over "New" vs. "Old" Terrorism. *Studies in Global Justice*, *4*, 117–136. https://doi.org/10.1007/978-1-4020-8660-1_8
12. Crenshaw, M. (2019). Terrorism and international cooperation. In *Terrorism and International Cooperation*. Routledge. https://doi.org/10.4324/9780429308659
13. Crenshaw, M. (2020). *Rethinking transnational terrorism AN INTEGRATED APPROACH*. United States Institute of Peace.
14. Elif Merve Dumankaya, & Haldun Yalçınkaya. (2022). *Emerging threats in terrorism*. Centre of Excellence Defence Against Terrorism (COE-DAT).

15. Ferrara, E. (2017). Contagion dynamics of extremist propaganda in social networks. *Information Sciences*, *418-419*. https://doi.org/10.1016/j.ins.2017.07.030
16. Freeman, M. (2013). Financing terrorism: Case studies. *Financing Terrorism: Case Studies*, *68*(2). https://doi.org/10.4324/9781315582429
17. GIFTC. (n.d.). *GIFCT | Global Internet Forum to Counter Terrorism*. GIFCT. https://gifct.org/
18. Hafner-Burton, E. M., & Shapiro, J. N. (2010). Tortured relations: Human rights abuses and counterterrorism cooperation. *PS - Political Science and Politics*, *43*(3). https://doi.org/10.1017/S104909651000065X
19. INTERPOL. (n.d.). *Databases*. Www. Interpol. int. https://www.interpol.int/How-we-work/Databases
20. INTERPOL. (2022). *Swift global police coordination lands people smuggling fugitives behind bars*. www.interpol.int. https://www.interpol.int/News-and-Events/News/2022/Swift-global-police-coordination-lands-people-smuggling-fugitive-behind-bars
21. Islam, B. G. Q. (2011). COMBATING TERRORISM: REGIONAL TASK FORCE IN SOUTH ASIA. *NDC E-JOURNAL*, *10*, 26–49.
22. Jean Pierre Bouchard. (2018). Profile of the perpetrator of the Nice terror attack that took place on 14th July 2016: A terrorist whose modus operandi may have been imitated in other European attacks. *Annales Médico-Psychologiques, Revue Psychiatrique*, *176*(6), 607–612. https://doi.org/10.1016/J.AMP.2018.04.002
23. Koblentz, G. D. (2020). Emerging technologies and the future of CBRN terrorism. *The Washington Quarterly*, *43*(2), 177–196. https://doi.org/10.1080/0163660X.2020.1770969
24. Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security and Privacy*, *9*(3). https://doi.org/10.1109/MSP.2011.67
25. Mathieu Deflem. (2006). Global rule of law or global rule of law enforcement? International police cooperation and counterterrorism. *Annals of the American Academy of Political and Social Science*, *603*. https://doi.org/10.1177/0002716205282256
26. Mayssa Zerzri. (2017). The threat of cyber terrorism and recommendations for countermeasures. *Cyber Terror*, *6*.

27. Morabito, A., & Greenberg, S. (2005). Engaging the private sector to promote homeland security: Law enforcement-private security partnerships. In *U.S. Department of Justice Office of Justice Programs*.
28. New York Times. (2016, July 20). *Police Find Gun and Ammunition Inside Truck - The New York Times*. Web.archive.org. https://web.archive.org/web/20160720211838/http://www.nytimes.com/live/truck-plows-into-crowd-in-nice-france/police-find-cache-of-weapons-inside-truck/
29. O'Brien, L. B. (2011). The evolution of terrorism since 9/11. *FBI L. Enforcement Bull*, *80*, 3.
30. Okumura, T., T. Hisaoka, Yamada, A., Naito, T., H. Isonuma, Okumura, S., Miura, K., Sakurada, M., Maekawa, H., S. Ishimatsu, N. Takasu, & Suzuki, K. (2005). The Tokyo subway sarin attack - Lessons learned. *Toxicology and Applied Pharmacology*, *207*(2 SUPPL.). https://doi.org/10.1016/j.taap.2005.02.032
31. Hoffman, B. (1999). Inside terrorism. *International Journal*, *55*(1). https://doi.org/10.2307/40203468
32. Ramón Spaaij. (2010). The enigma of lone wolf terrorism: An assessment. *Studies in Conflict and Terrorism*, *33*(9). https://doi.org/10.1080/1057610X.2010.501426
33. Reinares, F., Alonso, R., Torre Bjørgo, Donatella Della Porta, Rik Coolsaet, Farhad Khosrokhavar, Rüdiger Lohlker, Magnus Ranstorp, Schmid, A. P., Silke, A., Taarnby, M., & Gijs De Vries. (2008). Radicalization processes lead to acts of terrorism. In *A concise Report prepared by the European Commission's Expert Group on Violent Radicalisation* (Issue May).
34. Renz, B. (2016). Russia and "hybrid warfare." *Contemporary Politics*, *22*(3). https://doi.org/10.1080/13569775.2016.1201316
35. Rik Coolsaet. (2016). Jihadi terrorism and the radicalization challenge: European and American experiences: Second edition. In *Jihadi Terrorism and the Radicalisation Challenge: European and American Experiences: Second Edition*. Routledge. https://doi.org/10.4324/9781315590479
36. Rosand, E., Heale, M., Ipe, J., & Millar, A. (2008). The UN global counter-terrorism strategy and regional and subregional bodies: Strengthening a critical partnership. In *Center on Global Counterterrorism Cooperation*.
37. Ryamizard Ryacudu. (2018). Terrorism in Southeast Asia: The need for joint counter-terrorism frameworks. *Journal of the International Centre for Political Violence and Terrorism Research (CTR)*, *10*(11).

38. Sabol, J., Bedřich Šesták, Lubomír Polívka, & Mroz, K. (2015). Current activities of the European Union in fighting Cbrn terrorism worldwide. *NATO Science for Peace and Security Series B: Physics and Biophysics*, *74*. https://doi.org/10.1007/978-94-017-9894-5_15
39. Sari, Y. (2020). *COOPERATION WITH INTERPOL AGAINST FOREIGN TERRORIST FIGHTERS: THE CASE OF TURKEY*. T.R. POLICE ACADEMY INSTITUTE OF SECURITY SCIENCES.
40. Saul, B. (2010). Defining terrorism in international law. In *Defining Terrorism in International Law*. https://doi.org/10.1093/acprof:oso/9780199535477.001.0001
41. Schuurman, B. (2019). Topics in terrorism research: reviewing trends and gaps, 2007-2016. *Critical Studies on Terrorism*, *12*(3). https://doi.org/10.1080/17539153.2019.1579777
42. Security, UN. (2001, September). *Resolution 1373 (2001) / adopted by the Security Council at its 4385th meeting, on 28 September 2001*.
43. The United Nations. (2016, March 22). *UN strongly condemns terrorist bombings in Brussels as "an attack on us all" | UN News*. News.un.org. https://news.un.org/en/story/2016/03/525072
44. Treverton, G. F., Thvedt, A., Chen, A. R., Lee, K., & McCue, M. (2018). Addressing hybrid threats. In *Swedish Defence University Försvarshögskolan* (p. 98).
45. Wojcieszak, M. (2010). "Don't talk to me": Effects of ideologically homogeneous online groups and politically dissimilar offline ties on extremism. *New Media and Society*, *12*(4). https://doi.org/10.1177/1461444809342775
46. Young, R. (2006). Defining terrorism: The evolution of terrorism as a legal concept in international law and its influence on definitions in domestic legislation. *Boston College International & Comparative Law Review*, *29*(1).