T.C.

SELÇUK ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

ULUSLARARASI İLİŞKİLER ANA BİLİM DALI

ULUSAL VE ULUSLARARASI GÜVENLİĞİN BİLEŞENİ OLARAK SİBER GÜVENLİK: IRAK ÖRNEĞİ

Ali Mohammed Idan

DOKTORA TEZİ

Danışman

Prof. Dr. Nezir AKYEŞİLMEN

KONYA- 2020

ÖNSÖZ

Siber güvenlik konusu, modern zamanların en önemli konularından biridir. Çağımızda modern kitle iletişim araçlarının yaygın olarak kullanımı, hayatımızda yeni bir çığır açmıştır. Dijital dünyaya doğru hızlı bir şekilde yelken açtığımız bu dönemde yeni kuşağın yaşam alanını sanal âlem oluşturmuştur.

Siber Güvenlik konusu her zaman ilgimi çekmiştir. Tezimin konusunun **Ulusal ve Uluslararası Güvenliğin Bileşeni Olarak Siber Güvenlik: (Irak Örneği)** olması, beni fazlasıyla memnun etmiş ve büyük bir istek ve sevinçle bu çalışmamı yapmama neden olmuştur.

Bu doktora çalışmamda katkısı olan, ilham veren, vakit ayıran, destek veren herkese teşekkürlerimi sunmayı bir borç bilirim. Öncelikle kıymetli vakitlerinden feragat ederek, tezin bilimselliği konusunda gerekli yönlendirmeleri yapan, babacan şekilde destek veren ve ilgilenen, yorum ve değerlendirmeleriyle yol gösteren saygıdeğer danışman hocam Prof. Dr. Nezir AKYEŞİLMEN'e canı gönülden teşekkürlerimi sunarım. Ayrıca Selçuk Üniversitesi'ne kaydımı yaptırdığım günden bu yana benimle dostane bir şekilde ilgilenen, desteklerini esirgemeyen, kardeşçe tutumlarıyla her zaman yanımda duran tüm Uluslararası İlişkiler bölümü hocalarıma teşekkürlerimi ve en derin saygılarımı arz ederim.

Öte yandan bu araştırmamın ortaya çıkmasında yardım ve desteklerini her zaman yanımda bulduğum tüm dostlarıma teşekkürlerimi bir borç bilirim. Kuşkusuz emeklerini hiçbir zaman inkâr edemeyeceğim başta anneme, kardeşlerime ve ailemin tüm üyelerine destekleri için minnettarım.

ALI MOHAMMED IDAN

KONYA-2

ÖZET

Günümüzde bilginin temel olduğu açık dijital ortamdaki işlemlerde karşılıklı güven ve emniyet duygusunun sağlanması için veri ve bilgi güvenliğinin oluşturulmasını gerektiren kaygılar, elektronik devletin kurulmasına meydan okuyan bir güvenlik endişesi haline gelmiştir.

Siber uzayın, barışın doğasını etkileyen bir risk unsuru olarak güçlenmesi ve istenmeyen siber saldırılar, uluslararası güvenlik gündeminde her geçen gün daha fazla ilgi görmeye başlamıştır. Çünkü siber güvenliğin sağlanması, ülkelerin gücüne güç katarken, ihmal edilmesi durumunda ise siyasi ve askeri hedefler açısından güç dengelerinin değişmesine neden olmuştur.

Bu tez çalışması, veri analizi ve tarihsel yöntemleri esas alarak, ülkelerin ulusal güvenlik sistemleri içindeki siber güvenliğin konumunu açıklığa kavuşturmayı amaçlamaktadır. Milli güvenlik politikası ve stratejileri çerçevesinde esas alınan hedefin; istikrarı sürdürmek adına ulusun ve ulusal değerlerin güvenliğini sağlama noktasından hareketle, siber uzayın anılan kavramla ilişkisini inceleyerek bahsedilen politikanın boyutları ortaya konacaktır.

Çalışmamız, gerçekçi, liberal ve yapılandırmacı teoriler ve Kopenhag Okulu yaklaşımları gibi ulusal güvenlik kavramıyla bağlantılı olan uluslararası ilişkilerin en önemli teorileri üzerine odaklanmaktadır. Ayrıca siber tehditlerin incelenmesinin uluslararası ilişkiler ve ulusal güvenlik üzerindeki etkileri bağlamında anılan teorilerin muhtemel veya ilan edilen yaklaşımları ele alınacaktır. Bilgi teknolojisinin gelişiminden faydalanan terör gruplarının sosyal medya mecralarını nasıl kullandığına değinmektedir. Son bölümde, bir model olarak Irak'taki siber güvenlik ile çeşitli ülke ve kuruluşların siber güvenlik sistemine nüfuz edilmesine olanak sağlayan özel durumlar göz önünde bulundurularak araştırılmıştır. Irak'ta ve diğer tüm ülkelerde ulusal güvenlik sisteminin ayrılmaz bir parçası olan siber güvenliğin artan önemi ve muhtemel sonuçları açıklanmıştır.

ABSTRACT

Cyber conflicts has become today “a ghost that threatens the world and a security concern that challenges the establishment of electronic government, which requires securing data and information, to instill confidence and security in transactions in the open digital environment that we live in today, and that information is one of its most important pillars and components.”Therefore, cyber attacks began to receive increased attention on the international security agenda,, In an attempt to counter its escalation and role in influencing the peaceful nature of cyberspace. This is because the uses of cybersecurity changed the balance of power in many countries that were relying only on traditional power to achieve their political and military goals

Therefore, the aim of the thesis was to clarify the position of cybersecurity within the national security systems of countries by relying on the data analysis method as well as the historical approach to clarify that the primary goal National security policy and strategies was and remains to achieve and maintain national interests and ensure the security of the nation and its values. In a nutshell, this thesis clarifies the concept of national security and its dimensions and levels. The Nationalist took a large part of it. The study dealt with the issue of electronic terrorism and how terrorist organizations use social media and its various applications. And how to benefit from the development of information technology.

In the last part, cybersecurity in Iraq was reviewed as a model in view of the special situations this country is going through that enabled various parties, organizations and some countries to penetrate the cybersecurity system. As an integral part of the national security system in Iraq and in all other countries, it showed how the political, military and economic importance of the institutions specialized in managing cyber security is increasing.

İÇİNDEKİLER

KISALTMALAR

age. : Adı geçen eser

agm. : Adı geçen makale

agt. : Adı geçen tez

C. : Cilt

AB : Avrupa Birliği

ABD : Amerika Birleşik Devletleri

Çev. : Çeviren

BM : Birleşmiş Milletler

md. : Madde/ Maddesi/Maddeleri

MGK : Milli Güvenlik Kurulu

NATO : North Atlantic Treaty Organization (Kuzey Atlantik Antlaşması Örgütü)

p. : Page: Yabancı kaynaklar için Sayfa.

s. : Sayfa

S. : Sayı

ts. : Tarihsiz

vd. : ve diğerleri/ve devamı

BİT : Bilgi ve iletişim teknolojisi

ŞEKİLLER LİSTESİ

GİRİŞ

Bilgi teknolojisinin gelişimi, sanal âlem olarak adlandırılan bir ortamda sosyal, siyasal, ekonomik vb. alanlarda etkisini göstererek, yaşamın tüm eksenlerini kapsayan bir devrim yaratmıştır. Güvenlik ve askeri çalışmalar gibi hassas bilgilerin elektronik alanda bilinçli-bilinçsiz yayınlanması, olumsuz kullanımın ortaya çıktığı en önemli alanlardan biri haline gelmesine neden olmuştur. Bu durum, modern teknolojiyi, savaş yöntemlerini, elektronik suçları ve elektronik savaşları birbirine katmıştır. Teknolojinin kötüye kullanımı, bir anda elektronik ortamda sanal orduların ve bir takım özel grupların ortaya çıkmasını doğurmuştur. Ardından birçok ülkede istikrarsızlığa, siyasi krizlere ve orduların yapısını değiştirmeye yönelik müdahaleleri de beraberinde getirmiştir.

Birçok ülkede Siber Güvenlik, ulusal güvenliğin en önemli unsurlarından biri haline gelmiştir. Çünkü uluslararası sistemin en önemli aktörleri olan ülkeler, bilgi teknolojisini siyasi- ekonomik ve hatta sosyal yapılarını geliştirmede kullanmıştır. Böylece ulusal güvenliğin en önemli unsuru olan "Siber güvenlik", uluslararası aktörlerin uluslararası sistemdeki ilişkilerinin istikrarı için en gözde aracı haline gelmiştir.

Siber alan diye adlandırılan sanal âlem, bilgisayar sistemlerine, internet ağlarına ve çok geniş veri ve bilgi hazinesine dayanmaktadır. Zira bilgisayar, telefon ve diğer iletişim araçları sayesinde çok kolay bir şekilde coğrafik sınırları aşan bağlantılar kurulabilmektedir.

Siber güvenlik, elektronik bilgi ve iletişim sistemlerinin kötüye kullanılmasını önlemekte kullanılan bir kavramdır. Ayrıca bilgi teknoloji sistemleri, çalışmaların varlığını ve sürekliliğini koruma, elektronik alanlardaki bireysel ve kurumsal veriler gibi çeşitli risklerin korunmasını sağlamakta kullanılan tüm teknik ve idari araçları da kapsamaktadır. Artık son zamanlarda bütün devletlerce, geleceğin savaşları olarak öngörülen, toplu yıkım ve tahribatların en önemli nedeni olan "siber saldırılar" ile baş etmek için tedbirler almaya başlandığı dikkat çekicidir. Bu durum, bu tür dijital savaşlar ile karşılaşıp yüzleşmede gelişmiş ülkelerin taktik ve stratejilerinin bir par-

çası haline gelmiştir. Ayrıca bu savaşlara karşı koymak da birçok devletin savunma stratejilerinin ayrılmaz bir parçası haline gelmiştir. Nitekim birçok ülke, sanal alandaki bilgilerin güvenliğini sağlamak adına, kapsamlı bir ulusal strateji geliştirmeye başlamıştır.

Yaşadığımız çağda bilgi güvenliği, genel anlamda toplumun ve devletin tüm kurum ve kuruluşlarını kapsayacak şekilde korunup gözetilmesi hayati derecede önemlidir. Bundan dolayı artık birçok ülke, teknolojideki hızlı değişimin ulusal güvenlik bakımından kolay olmayan tehditlerle karşı karşıya kaldığını anlamaya başlamıştır. Bu nedenle, ulusal güvenliği korumak için "Siber Güvenlik" başlığı altında bilgi güvenliğinin sağlanması ve önemli adımların atılması gerekmektedir. Bu meyanda toplumsal ve kurumsal bilgi sistemlerini ve iletişim araçlarını korumak amacıyla, yasadışı internet kullanımıyla mücadele başta olmak üzere geniş çaplı yasal ve teknik araçlara gerek duymaktadır. Siber saldırılarını önlemek, hesaplara ait şifre hırsızlarının önüne geçmek ve devlet ile özel bilgi sistemleri arasında yasadışı gelişmelerin etkisini azaltmak için bir takım güvenlik duvarları oluşturmak çok önemli bir konudur. Kamu güvenliğinin sağlanması, siyasi, ticari, askeri ve ekonomik verilerin korunmasıyla mümkün olur. Ayrıca alınacak tedbirlerin artırılmasıyla beraber veri sistemlerinin güvence altına alınması da siber güvenlik için önem arz etmektedir. Bu nedenle ivedi olarak bu konuda ulusal kurum ve kuruluşların oluşturulması gerekmektedir.

Siber alan somut değil, sanal bir alandır. İletişim araçları ile internet ve veri tabanları bu alanı kullanmaktadır. Her türlü veri ve bilgiye ulaşma olanağı olduğundan, bu alanın casusluk hırsızlık ve sızıntılardan korunması zorunlu olmaktadır. Ulusal temelde siber güvenlik kurumlarının kurulması ile birlikte siber ortamda iletişim ve bilişim alanında bir nevi güvenlik kordonu oluşmuştur. Bu gelişmelere bağlı olarak, bireysel ve toplumsal hak ve hürriyetlerin garanti altına alınmasıyla, özel ve kamu sektörüne ait bilgilerin kirli eller tarafından casusluk ve korsanlıkla elde edilmesine karşı mücadele ederek, hareket sahasını daraltmak ve bu tehditler için farkındalık oluşturarak tepki vermek gibi önemli kazanımlar elde edilmiştir.

1. Araştırmanın Önemi:

Araştırmamız, siber güvenlikle ilgili çalışmalara özel bir katkı sunmayı hedeflemeketedir. Uluslararası ilişkiler bazında özel bir konuma sahip olan siber güvenlik, siyasi, ekonomik ve sosyal alanlar ile uluslararası ilişkileri etkileme rolünün bir sonucu olarak ortaya çıkmaktadır. Bu araştırma önemini; uluslararası sistemdeki tüm aktörlerin veri ve bilgilerinin korunması, saldırı ve tehditlerin önlenmesi, birey ve toplumun güvence içerisinde yaşaması konusunda hayati önem taşıyan siber güvenlik tedbirlerine odaklanmasından almaktadır. Teknolojik ilerlemelerin uluslararası ilişkilerde nüfuz kavramını değiştirmesinden sonra, askeri güç bakımından zayıf olan ülkeler, özellikle yeni iktidar modellerine (yumuşak güç) yönelmesiyle, maliyet açısından fazla külfet gerektirmeyen bilgi teknolojisi imkânına sahip olma gayreti içerisine girmiştir. Ancak bu gelişmeler, önlem alınması gereken bir takım sorunları da beraberinde getirmiştir.

Bu çalışmamız, güven oluşturma, elektronik tehditleri önleme, caydırma ve siber hamlelerin zorluklarıyla başa çıkma konusunda önemli bir bakış açısı kazandırmayı amaçlamaktadır. Aynı şekilde dijital tehditlerden kaynaklanan sorunlara çözüm bulmak için, gelişmiş teknolojik programlara ve yasal mevzuata dayalı esnek kuralların düzenlenmesini öngören, köklü bir vizyona dayanmaktadır. Ayrıca siber uzayın günlük yaşamı etkileyerek hızla daha geniş kitlelere ulaşması nedeniyle, konunun ulusal ve uluslararası ilişkiler perspektifinde değerlendirilmesi gerektiği tespitini ortaya koymaktadır. Bu noktada hükümetin uygulamalarından uluslararası ilişkilere kadar, önemli adımların atılması gerektiği vurgulanmaktadır.

Avrupa ülkelerideki çeşitli kurum ve kuruluşlarında ortaya çıkan elektronik tehditlerle mücadele konusunda bir dizi zorluğun ortaya çıkmasında, bireylerin bilgi ve iletişim teknolojilerine bağımlı olmasının rolü ortaya çıkmıştır. Bu nedenle bu tehditlerin önlenebilmesi ve bunlarla mücadelede kesin sonuç alınabilmesi için toplumun her bireyinin bizzat katılımı üzerinde önemli çalışmalar yapılmıştır.

İnternet sunucu şirketleri, kötüye kullanımı önleyen bir çerçeve dâhilinde hizmet sunması ve güvenli kullanıma hâkim olma sorumluluğu taşımalıdır. Bu bağlam-

da sorun, teknolojiyi araç edinen vatandaşın interneti kullanmasında değil, aksine gerekli önlemelerin alınarak vatandaşın özgürlük alanını güvence altına alma noktasında ortaya çıkan ihmallerdedir. Bilgi iletişim teknolojisinden yararlanan kamu kurum ve kuruluşları ile özel sektöre bağlı kuruluşlar, işlemlerini vatandaşın lehine çevirmelidirler. Sağlık, Güvenlik, Ticari ve Finansal Kuruluşlar gibi alanlarda gerçekleşmesi muhtemel tehlikelerden vatandaşın hak ve özgürlüklerinin güvence altına alınması gerekmektedir.

2. Araştırmanın Amacı:

Güvenlik çalışmaları, özellikle hızlı değişim ile karakterize edilen çağımızda, büyük önem arz etmesinden dolayı birçok araştırmacının ilgisini çekmektedir. Siber güvenliğin, nispeten yeni bir kavram olarak karşımıza çıkması ve henüz belirsiz niteliklere sahip olması, bu kavramın uluslararası ilişkiler üzerindeki etkisini ve Irak gibi gelişmekte olan ülkelerde siber tehditlerin siyasi istikrarsızlık üzerindeki tesirini açıklamak, araştırmanın en önemli hedefleri arasında olmuştur.

Ayrıca siber güvenliğin, ulusal ve uluslararası sistem ile aktörler üzerindeki etkileri ve bunların iç ve dış politikaya yansımaları irdelenmiştir.

Siyasal, ekonomik ve sosyal alanlarda siber uzayın olumsuz kullanımından kaynaklanan risklerin azaltılması, sosyal ve politik sorunlara çözüm bulunmasına katkı sunmak, araştırmanın üzerinde durduğu konular arasında ele alınmıştır. Özellikle Irak gibi gelişmekte olan ülkelerde, siber uzayın rolünün açıklığa kavuşturulması ve halkın bilinç düzeyinin yükseltilmesi aynı meyanda işlenmiştir.

3. Araştırma Varsayımları:

1-Siber uzayın etkisiyle yeni "güvenlik" kavramlarında önemli değişiklikler meydana gelmiştir. Bunlar; siber güç, siber çatışma ve siber savaş kavramlarıdır. Devletler, bireyler ve diğer rasyonel aktörler, ne zaman ve neden çatışmaya girdiklerine ilişkin kazanç ve kayıp hesaplamaları kullandıklarına göre, eğer kayıplar kazançlardan daha büyükse, devletler ve siber uzaydaki diğer aktörler rakipleriyle yüzleşmek için saldırgan adımlar atmaktan caydırılabilecek midir?

2-Siber güvenlik, ulusal güvenliğin en önemli unsurlarından ve sektörlerinden biri ise siber tehditlerin ciddiyetindeki bir artış, doğrudan ulusal güvenliğe yönelik tehdit yüzdesinde de bir artışa neden olur mu?

3-Siber uzayda ülkeler arasında artan koordinasyon ve işbirliği, tehdit risklerini azaltacaktır. Etkili bir şekilde siber tehditlere karşı topluca karşı durulması, siber uzayın güvenliğini bozmaya çalışan güçlere yönelik bir caydırıcılık oluşturabilir mi?

4-Teknolojik olarak gelişmiş ülkelerin çoğu, hukuki alanlarda yüzleşmek için büyük çabalar sarf etmiştir. Ancak siber teknolojisiyle saldıran güçlerin teknolojik ilerlemedeki güçlerinden aldıkları rehavetle siber uzayın güvenlik sistemindeki herhangi bir boşluğu istismar etmeleri nedeniyle küresel boyutta korkunç tehlikelere neden olabilmektedirler. Bu aktörler küresel anlamda güvenli bir siber ortam oluşturamayacaklar mı?

5-Devletler, ulusal çıkarlarını korumak için rasyonel kararlar alan önemli mekanizmalardır. Bu nedenle her devletin, siber uzay teknikleriyle saldıran bir devletin oluşturduğu tehditle yüzleşmesini zorlayacak yeterli güç yeteneklerine sahip olması, gerektiğinde bu yetenekleri kullanmaya her zaman hazırlıklı olması gerekmektedir.

4. Araştırmanın Sınırları:

Araştırmanın zamansal ve mekânsal sınırları geniş tutulmuştur. Nitekim Siber Güvenlik konusu, fiziksel olarak değil, sanal olarak ortaya çıkmış en hassas konulardandır. Bugün dünya bazında internet kullanıcılarının sayısı 4,7 milyar kullanıcıyı aşmıştır. Bu oran, dünya nüfusunun yaklaşık % 60'ını oluşturmaktadır. Böyle devasa bir ağa sahip siber alandaki güvenlik çalışması, ulusal ve ulusalararası güvenlik için önem arz etmektedir.

Dünya çapındaki networkler ve iletişim ağları birbirine bağlı olarak dünyanın çeşitli bölgelerine yayılma özelliğine sahiptir. Devlet egemenliğinin ötesinde siber uzayın genişlemesi, paralel olarak mekânsal sınırların ötesine geçilerek veri ve bilgi aktarılmaya çalışılmaktadır.

İnternet sağlayıcı şirketlerin kesintisiz ve kaliteli bir hizmet sunabilmesi, bilgi teknolojisinde güvenli bir ortamın oluşturulmasına bağlıdır. Siber saldırılarıyla gerçekleştirilen tehditlerin önlenmesinin ekonomik maliyeti, Ulusal güvenliğin tesis eilmesi kadar öneme sahip değildir. Bu nedenle ulusal güvenlikle ilgili hassasiyetler, ekonomik çıkarların üzerinde tutulmalıdır. Araştırmanın zamansal sınırları, 1980'lere ve öncesine dayanmaktadır. Bu süreç internet ağlarının geliştirilmesini sağlayan modern teknolojinin gelişimiyle bağlantılıdır. 1988'de ilk mobil virüse rastlanmış ve saldırıları bu güne kadar devam etmiştir. Gün geçtikçe gelişen teknolojik silahların esas alınması ve bunları kontrol etme maliyeti artmaktadır. Dünya çapında 130'dan fazla ülke,(Cohen 1988) ulusal güvenlik ekipleri içinde siber savaş için bölümler tahsis ettiğini açıklamıştır. Bahsedilen birimler, siber suç, siber sahtekârlık ve siber risklerin çeşitli yönleriyle mücadelede geleneksel güvenlik çabalarına katkıda bulunmaktadır.

5. Araştırma problem:

Elektronik-sanal mecralar, artan teknoloji kullanımına bağlı olarak küresel sistemin genel yapısında ve doğasını şekillendirmede büyük bir rol oynamaya başlamıştır. Elektronik alan, güç kavramının geleneksel ve önemli biçimi sayılan sert güç olgusu ile sınırlı olduğu algısının zayıflamasına zemin hazırlamış, sanal veya elektronik güç denen yeni bir türün oluşmasını sağlamıştır. Bahsedilen yeni güç türü, teknoloji bilgisine sahip herkesçe ulaşabilir bir nitelikte olmuş, farklı amaçlarla, çeşitli çıkarlar doğrultusunda yönlendirilmiştir. İlgili gücün olumlu ve barışçı kullanımı yanında terörist gruplar tarafından saldırı ve sızma gibi kötü hedeflere alet edildiği de gözlemlenmiştir. Küresel oyuncular dışındaki aktörlerin casusluk ve bilgi kaçırmak için ondan faydalandığına rastlanmıştır. Bu noktadan hareketle değişik işlemlere sanal dünya çerçevesindeki bilişim teknolojisinin hakim olmasıyla birlikte siber güvenliğin değeri yükselmiştir. Uluslararası ilişkiler ve benzeri disiplinlerde uluslararası güvenlik ve strateji bağlamında akademik çalışmalar yürüten araştırmacılar, siber meselelere gittikçe daha fazla eğilmektedir. Dijital aygıtların, sanal mecraların milli ve küresel seviyede küresel hükümet, egemenlik, ulusal güvenlik vb. başlıklar etrafında emniyet durumlarına ve sorunlarına tesirini incelemektedir.

Bu konuda çeşitli sorular ve problemler ortaya konmaktadır:

güvenlik kavramı sürekli bir değişim içerisine girmiştir. Günümüzde, her alandaki değişimin hızlı bir şekilde artması ve özellikle yirminci yüzyılda küreselleşme, bilim ve teknoloji alanındaki gelişmeler, akademi literatüründe yer alan diğer kavramlarda olduğu gibi, güvenlik kavramı tanımında da değişime yol açmıştır.Siber alandaki teknolojinin ulusal güvenlik kavramı üzerindeki etkisi nedir? Siber alandaki teknolojinin güç kavramına etkisi nedir?

altyapılarını geliştirerek ve yüksek düzeyde teknolojik ilerleme kaydederek yoluyla Ülkeler siber güvenlik alanında üstünlük elde etmek için mücadele ediyor , siber uzayda teknolojinin güç kavramı üzerindeki etkisi nedir?

21. yüzyılda teknolojik gelişmeler sonucunda güvenlik parametreleri değişmiş; kara, deniz, hava ve uzay yanında beşinci bir alan ortaya çıkmıştır Devletin bölgesel sınırlarını aşıyor. Bu alan siber uzay (cyber space) alanı olarak ifade edilmektedir. Siber alanda kullanılan teknolojilerin devlet egemenliğine etkisi nedir?

Siber güvenliğin Bağıl kavram olduğunu bilirsek, mevcut küresel gelişme ışığında geri siber uzay kullanımında geride kalan Irak gibi ülkelerin geleceği ne olacak?

Bir devletin vatandaşları, toprakları veya kurumlarının kullanıldığı bir siber saldırıda uluslararası hukuki sorumluluğu nedir?

Terörist yapıların siber alandaki hedeflere yönelik saldırılarda kullandığı uygulamalar ve araçlar nelerdir?

6. Araştırmanın Metodu:

Siber güvenlik, çağımızın yeni ve hızla gelişen bir konusu olduğundan, bu çalışmamızı ortaya koyarken bi r araya getirerek istifade ettiğimiz veri ve bilgiler; ya bir takım resmi belge ve istatistikleri içeren temel kaynaklar ya da yürürlükte olan kanun maddeleri veya web sitelerinde yer alan yayınlanmış makalelerden yararlanılmıştır. Bir olayla ilgili durum incelemesi yaparken karşılaştırmalı yaklaşımla ortaya

koymaya çalışılmıştır. Siber güvenlik olaylarının izlenmesi ve saldırılara karşı alınacak önlemlere değinirken Almanya, İngiltere ve Amerika Birleşik Devletleri gibi ülkelerdeki örneklerine işaret edilmiştir. Bunun yanı sıra Irak bilgi suçları yasası ile Türkiye Cumhuriyeti'nin yasaları arasında basit bir karşılaştırma yaparak, Irak'ın bu konuda Türkiye gibi dost bir komşu ülkenin uygulamalarından yararlanabileceğine işaret edilmiştir.

Araştırmamız genel anlamda siber güvenlik ve özelde Irak'ta siber güvenlikle bağlantılı olduğundan, güvenlik durumuna daha iyi uyan ve bunu açıklayan bir güvenlik metodu teorisi yaklaşımını kullanma ihtiyacı doğmuştur. Bu nedenle, "geniş güvenlik" yaklaşımı olarak adlandırılan metodun izlenmesi uygun görülmüştür. Nitekim sektörler arası analiz olarak adlandırılan bu metot, tarihte ilk defa 1993 yılında Barry Buzan, Charles Jones ve Richard Little tarafından hazırlanan "Kaosun Mantığı: Yeni Gerçekçilikten, Yapısal Gerçekçiliğe" (The logic of Anarchy: Neorealism to Structural Realism) kitabın yayımlanmasına kadar giden bir analiz metodudur ve uluslararası sistemin faaliyet alanlarına bölünmesine göre analiz etme yöntemidir.

Bu metoda göre her alan (sektör) ulusal güvenliğe özel bir ışık tutmaktadır. Ulusal güvenlik kavramının beş alanı; siyasi sektör, ekonomik sektör, askeri sektör, çevre sektörü, toplumsal sektör olarak ayrılmıştır. Araştırmamızda ulusal güvenliğin boyutları incelenirken bu metodun izlenmesi uygun görülmüştür.

Ayrıca, daha fazla uluslararası ilişkiler teorileri geliştirilmesine, realist, liberal, yapılandırıcı ve Kopenhag Okulu'ndaki araştırma hedeflerini de kapsayan uygun teorik çalışmaların ortaya konulmasına ihtiyaç duyulmuştur.

Araştırma; yerel sistem analizi, bölgesel sistem analizi ve uluslararası sistem analizi olmak üzere üç analiz seviyesinden oluşmuştur. Bu sistem ve teorilerin her birinin siber güvenlik alanındaki rolü açıklığa kavuşturulmuştur. Bununla beraber genel olarak uluslararası güvenliği etkileyen diğer devlet dışı aktörlerin rolü de incelenerek bilişim teknolojisinin gelişmesinden yararlanan terör örgütlerinin tehlikesine dikkatler çekilmiştir.

BİRİNCİ BÖLÜM

1. ULUSAL VE ULUSLARARASI GÜVENLİK BAĞLAMINDA SİBER GÜVENLİĞİN TANIMI, ÖZELLİKLERİ VE BOYUTLARI

Uluslararası sistem, toplumların şahit olduğu değişimlerle uyumlu şekilde farklı evreler aracılığıyla gelişmektedir. Belirli zaman dilimlerinde uluslararası ilişkilerin farklı biçimleri dünya siyasetine hükmetmiştir. Ortaçağ dini düşüncenin egemenliğine tanıklık etmiş, arından aklın egemenliğine dayanan aydınlanma çağı gelmiştir. Akabinde milliyetçiliğin egemenliğine tanık olan XIX ve XX. yy evreleri görülmüştür. Bu durum üçüncü bin yıllık dilime yani 2000'lere dek sürmüş, iki denge unsuru üzerinde yükselen bilim ve teknoloji düşüncesi bahsedilen zamana hâkim olmuştur. Bilim ve teknoloji çağında bir taraftan insanlığın yararına dijital ilerlemeler sağlanırken diğer taraftan onun yıkılmasına neden olacak güçte benzersiz silahlar üretilmeye başlanmış ve günümüz dünyası, tarihin seyrini değiştirecek bir olaya, sanayi devrimine şahit olmuştur (Al-Zubaidi 2015).

Ayrıca modern dönemde yeni bir tür devrime, veri ve bilgiye dayalı teknoloji devrimine tanıklık edilmektedir. Asrımız, hiçbir devlet, şirket ve bireyin stratejik açıdan bilgiden soyutlanamayacağı sanal bilgi çağıdır. Teknoloji devriminin kazanımları olumlu yönde insanlığın hizmetine kullanıldığı gibi olumsuz yönde de bazı devletlerin ekonomilerine zarar verecek biçimde kullanılmakta, devletlerin ulusal güvenliğini tehdit eden en büyük faktör olma yolunda ilerlemektedir (Dutta and Bilbao-Osorio 2012).

1.1. Ulusal güvenlik Tanımı ve Boyutları:

Genel anlamı ile güvenlik, insanlığın ömrü ile ilişkili olup emniyet barış ve huzur içinde bulunmayı ifade eden kadim bir kavramdır. İnsan içgüdüsel olarak öncelikle yeme, içme, giyinme ve barınma ihtiyacını karşılamaya çalışır. Sonrasında ise kendi güvenliğini sağlamaya odaklanır. Faaliyetlerini ve işlerini rahatlıkla yapabilmesi için kendisini tamamıyla güven içinde hissetmesi gerekir. Bu nedenle insanlar aile, kabile gibi sistematik gruplara kendilerini dâhil ederek, her birey için ortak nite-

likteki bütüncül güvenliklerini temin etmeye uğraşmışlardır. Semavi dinler de güvenliğin önemini vurgulamıştır. Kur'an-ı Kerim'de Bakara ve Kureyş surelerinde görüldüğü gibi birçok ayette güvenlik kavramı zikredilmiştir. Kureyş suresinde şöyle buyrulur:

"Kureyş'e kolaylaştırıldığı, evet, kış ve yaz seyahatleri onlara kolaylaştırıldığı için onlar, kendilerini açlıktan doyuran ve her çeşit korkudan emin kılan şu evin Rabbine kulluk etsinler." (Kureyş,1-4).

"Hani İbrahim, "Rabbim! Bu şehri güvenli bir şehir kıl. Halkından Allah'a ve ahiret gününe iman edenleri her türlü ürünle rızıklandır." demişti. Allah da, "İnkâr edeni bile az bir süre, (bu geçici kısa hayatta) rızıklandırır; sonra onu cehennem azabına girmek zorunda bırakırım. Ne kötü varılacak yerdir orası! demişti." (Bakara, 126).

İkinci Dünya Savaşı'ndan sonra uluslararası güç seviyelerinin farklılaşmasının ardından, yeni askeri ve siyasi koşulların doğması sonucunda güvenlik çalışmalarına odaklanma sürecine girilmiştir. Kuvvetler arasındaki dengeler, bloklaşmalar ve eksenlerdeki farklılıklar, bu koşullar ile örtüşen ulusal güvenlik çalışmalarının çoğalmasına yol açmıştır (Tarboshi 2010). Yeni tekniklerle binlerce masum insanın katledilmesine sebep olan savaşlardan alınan dersler, iç ve dış güvenlik konularına ilgiyi artırmış, ayrıca uluslararası ilişkilerde ideale ulaşma arzusu da güvenlik çalışmalarının yaygınlaşmasını sağlamıştır. Bu dönemde bazı çevrelerce dünya savaşlarının korkunç sahnelerine yeniden şahit olunmaması için dünya çapında barış ve güvenliğin sağlanması zorunlu hale gelmiş ve bunun yolları ve araçları araştırılmıştır. Yeni nesil ileri teknoloji silahların üretilmesine paralel olarak çeşitli ülkeler tarafından güvenlik çalışmalarıyla ilgili teoriler geliştirilmiştir (Mohammed 2017).

1.1.1. Ulusal Güvenlik Kavramının Tarihsel Gelişimi

Ulusal güvenlik kavramı, 1648 yılında imzalan Vestfalya Antlaşması'ndan sonra doğan ulusal/milli devlet olgusu ile bağlantılıdır. Devletlerin sınırları, temel ve dayanakları bu antlaşma ile belirlenmiş, devlet varlığının en önemli dayanağı olarak ulusal güvenlik üzerinde durulmuştur (Al-Zubaidi 2015) .

Thomas Hobbes, 1651 yılında insanlığın yalnızlık, yoksulluk ve vahşetten kaçarak toplumsal bir düzen yaratmaya doğru yöneldiğini söylerken ulusal güvenliğe değinmektedir. Hobbes'e göre insanın saldırgan iç güdüsü, kendisini güvensiz hissetmesine yol açmaktadır. İnsanın güvenlik arayışı, onu devletin temsil ettiği toplumsal ve siyasi bir düzeni bulmaya itmiştir (Hobbes 2010).

Hobbes'a göre, devletler, uluslararası ilişkilerde aktörler olarak, iktidar için kendi aralarında sürekli bir çatışma halinde görünürler. Birleşmiş Milletler, Avrupa Birliği, sivil toplum örgütleri gibi yapıların gerçek aktörler olmaması bu çatışmadan yoksun olmalarıdır. Devletin esas rolü kendini diğer devletlerden korumaktır. Bir devletin çıkarlarını düşmanlarından koruma gücüne sahip olması, "ulusal güvenlik" kavramını açıklamaktadır. Bu bağlamda uluslararası ilişkilerde gerçekçiliğin çatışma ve güç mücadelesi çevresinde şekillendiği anlaşılmaktadır (Tshtoush 2012).

Emmanuel Kant, 1795 tarihinde yayınlanan "Kalıcı Barış" adlı makalesinde şöyle demektedir: "Felsefeci, ulusal devletler ve hâkim ulusal becerilerin yerini aydınlanmış bir dünya düzeninin alacağını öngörüyorum. Nitekim küresel bir çerçeve içinde ulusal güvenliğin olması ve ulus devletler açısından uluslararası hukukun üstünlüğü altında özgün çıkarlarının elde edilmesi, öncelikli hedef olarak ulusal devletin daha büyük bir organizasyona (uluslararası sisteme) katılımı söz konusudur." Bu şekilde rasyonel bir vizyonu ve misyonu bulunan genel bir sistem, uluslararası bağlamda, ülkelerin ulusal güvenliğini de sağlayacaktır (Kant 1984).

Terim olarak ulusal güvenlik kavramı, II. Dünya Savaşı'ndan sonraki ABD tarihi ile yakından ilişkilidir. 1947 yılında ABD kongresi ilk ulusal güvenlik yasasını geçirmiştir. Yasa geleneksel anlamda devletin dış düşmanlarına karşı ekonomik, askeri, siyasi ve diplomatik araçlar ile korunmasını amaçlamıştır. Ancak bahsedilen kanun, son zamanlarda, insan güvenliği yaklaşımını da kapsayacak şekilde genişletilmiştir. Gelişim düzeyi, her türlü potansiyel tehdit ve güvensizlik halini, sorumlu aktörleri de kapsayacak şekilde emniyetle bağlantılı olarak değerlendirilmiştir. Bu kavram uygulama ve kavramsal biçimi bakımından Batı toplumlarının biriken deneyimlerini temel almıştır (BİRDİŞLİ 2011).

Kavram, ABD'nin Sovyetler Birliğini kuşatmak şeklinde özetlenebilecek tek bir hedef için stratejik ulusal güvenliğe odaklanarak geliştirdiği sloganlar çerçevesinde Soğuk Savaş döneminde tam olarak netleşmiştir. Ancak Sovyetler Birliği'nin dağılması ve çökmesi ile beraber Amerikalılar yeni siyasi durumlara uygun bir yönelim ve arayışlara başlamıştır. Amerika dünya siyasetine hâkim tek güçlü kutup olarak ortaya çıkmış, ekonomide kapitalist sistemin başarısı ve askeri alandaki geleneksel güvenlik tehditleri ile risk konularının ulusal güvenlik rotalarının belirlemesinde yeni bir döneme geçilmiş, tehdit unsurları yeniden değerlendirilmiştir. (Teivāns-Treinovskis and Jefimovs 2012).

Yenidünya düzeninde ABD için uygun olan ulusal güvenlik modeline dair ABD'li politikacılar çeşitli alanlarda farklı tehditler saptamışlardır: Bütçe ve dış ticaret açığı, küresel ekonomik sorunlar ve çevresel bozulma, bunlardan bir kaçıdır.

Ulusal güvenlik ifadesi, II. Dünya Savaşı'ndan sonra genel bir kapsamda kullanılmıştır. Deniz Kuvvetleri Sekreteri James Forrestal, Amerikan Senatosu'ndaki bir oturumda şu sözleri söylemiştir: "Ulusal güvenlik meselesi sadece ordu ve donanma meselesi değildir. Savaş için toplam gücümüzü hesaba katmalıyız. Madenlerimiz, sanayimiz, insan gücümüz, yenilenebilir gücümüz ile sıradan sivil hayatı kapsayan her türlü aktivelerimizi de hesaplamalıyız" (Rosso 1995).

Ulusal güvenlik sözcüğü 1945 yılında açıklanmaya ihtiyaç duyulan bir kavram iken, 1947'den itibaren geniş çerçevede kullanılmıştır. ABD Ulusal Güvenlik Konseyi'nin temelini oluşturan kanunun, giriş kısmında ulusal güvenlik kavramının tanımlanmaması ise dikkat çekicidir. 1947'deki bu yasada ilgili kavram, "Konseyin görevi başkana tavsiyelerde bulunmaktır" ifadesi ile değişik şekillerde yorumlanacak biçimde açık uçlu bırakılmıştır. Ulusal güvenlik kavramı sadece askeri alan ile sınırlandırılmamış, yerel, yabancı ve askeri bütün politikalar ile alakalı bütün durumları kapsayacak şekilde yorumlanmıştır.

İngiliz bilim adamı Barry Buzan, "Ulusal Güvenlik" kavramının nispeten kapalı ve kuramsal açıdan net bir şekilde tanımlanamayan bir terim olduğunu ifade etmektedir. Ancak siyasi açıdan güçlü bir değeri bulunan bir kavram olarak kalmasının

doğru olacağını ileri sürmekte ve şöyle demektedir; "Sınırları tam olarak belirlenmeyen bir ulusal güvenlik kavramının siyasi ve askeri alanda korunmasının çok daha fazla önemi vardır. Tanımdaki belirsizlik de ulusal güvenlik gerekçesi ile İçişleri'nin yetki alanındaki pek çok konuya müdahale etme ve nüfuzunu kullanma hakkı vermektedir" (Buzan, 2008).

Ulusal güvenlik için, evrensel düzeyde kabul gören belirli bir tanımdan bahsetmek pek mümkün değildir. Zira ulus devlet kavramı ve devlet dinamikleri hakkında da net bir tanım bulunmamaktadır (Malec 2003).

Ulusal güvenlik kavramı ile ilgili onlarca tanım mevcuttur. Bu tanımlar aracılığıyla kavramın anlaşılması için genel bir çerçeve sunulmasına rağmen hala anlamdaki kapalılık giderilmemiştir. Ulusal güvenlik öncelikle en basit şekliyle askeri tehditlerden kurtulmak ve bağımsız siyasi karar vermek olarak görülmüştür. Ancak daha sonra kapsam genişlemiş, çağın ihtiyaçlarını göz önünde bulundurularak askeri güvenlik dışında ekonomi, siber alan ve denizler gibi alanlar da ona eklenerek son şekli verilmiştir (Maier 1990).

Amerikan gazeteci ve siyaset adamı Walter Lippman, ulusal güvenlik kavramını tanımlayan ilk isim olarak kabul edilmektedir. 1943 yılında Lippman bu kavramı, savaş açısından net bir tanımla şu şekilde açıklamıştır: "Ulusun savaştan kaçınmak için yasal kararlarından fedakarlık yapmaya mecbur kalmaması ve saldırı karşısında meşru kararlarını koruyabilmesi, onun güvende olduğunu gösterir" (Lippmann 1987). Arnold Wolves (1952) ise ulusal güvenlik kavramını, her ülkenin kazanılmış değerleriyle, belirli bir halk tarafından benimsenen olgularla ve onlara karşı tehditlerle ilişkilendirerek şöyle söylemektedir: "Gizemli bir simge, farklı insanlara farklı şeyleri çağrıştırmaktadır. Ulusal güvenlik nesnel anlamda kazanılmış değerlere karşı herhangi bir tehdidin olmamasını, ayrıca yine bu değerlere karşı saldırının olmamasından emin olunmasını ifade etmektedir" (Wolfers 1952).

Robert McNamara'ın görüşü ise şöyledir: "Güvenlik kalkınmadır. Kalkınma olmadan güvenlik olmaz. Bugün kalkınmayan bir devlet kolaylıkla güven içinde yaşayamaz" (McNamara 1968) .

1977- 1981 yılları arasında Carter idaresinde ABD Savunma Bakanı olarak görev yapan Harold Brown, ulusal güvenlik kavramını genişleterek ona çevresel ve ekonomik güvenlik gibi unsurlar eklemiştir: "Ulusal Güvenlik, ülke topraklarında somut bir şekilde güveni sağlayabilme gücüdür. Makul şartlar dâhilinde dünyanın geri kalan ülkeleri ile ekonomik ilişkilerin, doğanın, kurumların kollanması ve dış baskılara karşı yönetim erkinin ve sınırlara olan hâkimiyetin korunması demektir" (Watson 2002).

Harvard Üniversitesi Tarih Profesörü Charles Mayer, 1990'da ulusal otorite bağlamında ulusal güvenliği şu şekilde tanımlamıştır: "Ulusal Güvenliğin en iyi tanımı; belirli bir toplumun kamuoyunun faydalanabilmesi için, gerekli gördüğü şeylerde kendi kaderini tayin, özerklik, refah ve huzur gibi iç ve dış koşulları kontrol edebilme kabiliyetidir (Maier 1990).

"National Security: Imperatives and Challenges" kitabının yazarı Prabhakaran Paleri'ye göre ulusal güvenlik şu şekilde tanımlanabilir: "Ulusal güvenlik bir ülkenin ölçülebilir anlamda çok boyutlu tehditlere karşı koyabilme kapasitesini, açık bir şekilde halkının güvenliği için kullanması aracılığıyla herhangi bir zaman diliminde ulusal bir devlet olarak varlığını sürdürebilmesidir. Yönetim aracılığıyla devletin politika araçlarını dengeleyerek hesaplayarak, deneyimleyerek sağlayabilmesi, ayrıca dış değişimler aracılığıyla küresel güvenliğini karşılayabilmesidir (Paleri, 2009: 460).

Ulusal güvenlik kavramının en çok kabul göreni ve en yaygın olan tanımı şöyledir: Devletin ve milletin her türlü iç ve dış tehlike ile krizlerden korunmasıdır. Bunun sağlanabilmesi için, askeri, güvenlik, siyasi, ekonomik, diplomatik, çevresel vb. kapasitelerin kullanılmasını gerekli kılar.

Henry Kissinger ise ulusal güvenliği, "toplumun var olma hakkını savunma iradesi göstermesidir" şeklinde tanımlar (Kissinger 1969).

Uluslararası sistemin küreselleşmesi ve modern zamanda çeşitli teknolojik, siyasi ve ekonomik alanlarda büyük gelişmeler görülmesi neticesinde geleneksel ekonomik ve siyasi kavramlar değişmiştir. Değişimin yansıdığı önemli alanlardan biri de

içeriği, doğası ve kullanım kapsamıyla ulusal güvenlik kavramıdır. Bu kavram artık içerik, sadelik ve kapsam genişliği bakımından eski anlamını korumamaktadır (Drent, et al. 2014a).

Aşırılık, terör ve vekâletle savaş sistemlerinin yayılması gibi çeşitli siyasi durumları içeren dünya sistemindeki değişimlere, ulusal güvenlik paralel olarak kapsamlı ve çok boyutlu bir kavram haline gelmiştir. Organize suçlar, terörizm, çevresel bozulma, doğal kaynaklar üzerindeki çatışmalar, kontrolsüz göçmen akını, yasadışı göç, yoksulluk ve insanlık için bir tehdit haline gelen açlık gibi belirli bir bölgesel ve hatta sınır ötesi çerçevede problemler belirmiştir. Dolayısıyla bazı araştırmacılara göre, güvenlik kavramının farklı seviyelerde genişletilmesi zorunlu olarak görülmüştür (Iglesias 2011).

Ulusal güvenliğin temel kavramları bölgesellik ve askeri savunma ile sınırlı değildir. Son beş yıl içerisinde mevcut küresel ekonomik krizin etkisiyle giderek karmaşıklaşan uluslararası çerçeve güvenlik sorunlarının sadece dâhili/kişisel veya sivil- askeri olarak taksim edilemeyeceğini ortaya çıkarmıştır. Bu nedenle günümüz dünyasında güvenlik kavramı birden çok özelliğe sahip bir nitelik almıştır. En önemli özellikler aşağıdaki gibi tanımlanabilir:

1. Kapsayıcılık: Güvenlik olgusu, sadece belirli ülkelerin veya grupların güvenliklerine zarar verilip verilmemesi ile sınırlı kalmamıştır, genel olarak küresel güvenliği içerecek şekilde kapsamlı ve sınır ötesi bir yapı kazanmıştır.

2. Devamlı Gelişim: Güvenlik tehditlerine karşı kullanılan araçların ve çeşitliliğinin artması, bu tehlikelerin gelişim boyutunu göstermektedir.

3. Etki Alanları ve Öneminin Artması: Belirli güvenlik tehditleri bazı ülkelerin özellikle ekonomik, siyasi ve askeri yönlerini tehlikeye atmakta ve onların geleceğini kontrol etmektedir.

4. Güvenlik tehditlerinden etkilenen birden çok alan vardır: Ulusal güvenlik bugün artık her insana farklı şeyleri ifade ettiği için sadece askeri alan ile sınırlı

değildir. Örneğin bilgi teknolojisi güvenliği, enerji güvenliği, çevre güvenliği ve hatta sağlık ve gıda güvenliği gibi alanlar bu çerçevede değerlendirilebilmektedir.

1.1.2. Ulusal Güvenlik Seviyeleri:

Ulusal güvenliğin sağlanması için şu üç düzeyin gerçekleşmesi ve birlikte sağlanması gerekmektedir:

1. Düzey: Dâhili Düzey:

Soğuk Savaş döneminde ortaya çıkan ulusal güvenlik kavramı; "devletin güvenlik ve savunmaya dair bütün meseleleri kontrol eden devletin dâhili/ iç ve milli unsurları" şeklinde açıklanmaktaydı. Askeri, ekonomik ve siyasi programlar da bu unsurlar içerisinde değerlendirilmektedir. Bu doğrultuda ulusal güvenliğe, bireysel güvenlik (Individual Security) de denilmekte ve böylelikle devletin en önemli sorumluluklarından olduğu vurgulanmaktadır. Bireyin toplum yapısında, vatandaşın ülkesinin sınırları içinde ya da dışında, kendi hayatını ve varlığını herhangi bir tehdit olmaksızın güven ve istikrar içinde hissetmesidir. Devletin iç güvenliğinin politik, sosyal ve ekonomik düzeylerde sağlanması hedeflenmektedir. Emniyetli ve istikrarlı bir hayat elde etmek için ülkeye yönelik dış tehditler önlenmeli, devletin sınırları ile siyasi yükümlülükleri dâhilinde düzen sağlanmalıdır. Ayrıca birbirine bağlı kurumlar arasında karşılıklı dayanışmayı oluşturmak amacıyla iç ve dış güvenlik arasında zorunlu ve karşılıklı ilişkiye ihtiyaç vardır (Timonen and Nikander 2017).

11 Eylül 2001 olaylarının ardından, Avrupalılar artık savaşları büyük bir tehdit olarak görmemeye başlamıştır. Uzun süren barış ve istikrardan sonra Avrupa'da devletlerarasında silahlı mücadeleler daha az belirgin hale gelmiştir. Hollanda nüfusunun % 60'ından azı, yasadışı göç, terör eylemleri, salgın hastalıklar, çevre kirliliği, uyuşturucu ve siber güvenlik suçları, gibi iç güvenlik tehditlerinin artması nedeniyle ulusal güvenliğin öncelikli olarak önemsenmesini istemiştir. Bu nedenle Savunma Bakanlığı'nın ulusal görevlere daha fazla odaklanması gerektiğini, silahlı kuvvetlerinin ülke dışına konuşlandırması konusunda ise isteksiz oldukları ortya çıkmıştır. (Drent, et al. 2014b).

Belirli bir sistem dâhilinde yerel güvenlik (Local Security) adında yeni bir kavram ortaya çıkmakmıştır. Bir devletin öncelikleri içinde belirli bir sahayı kapsayan yerel güvenliğin bir alt başlığı olarak "kişisel güvenlik" (Regime Security) şeklinde adlandırılan bir birim oluşturulmuştur. Bu birim; mevcut iktidarın anayasal meşruiyetini koruması ve durumu muhafaza ederek milli otoritede yeralan yönetici kadronun varlığını korumak için rejimin sağlaması gereken özel güvenlik alanıdır. Bu anlam dâhilinde güvenliği sağlama sorumluluğu silahlı kuvvetler, iç güvenlik güçleri ve yardımcı organları ile sağlanmaktadır. Buna dayanarak da bu kurumlar güvenlik kavramının tanımı çerçevesinde ulusal güvenliği etkileyen bütün tehditlere karşı her türlü güç ve şiddet kullanma hakları meşru görülmüştür (Beasley 2009).

2. Düzey: Bölgesel Güvenlik:

Uluslararası siyasi arenada 1945 yılından sonra başlayan ve özellikle de 1990 sonrası çokça kullanılan, "bölgesel iş birliği" kavramının öne çıktığını görmekteyiz. İkinci Dünya Savaşı ve Soğuk Savaşın bitmesi ile sömürgeciliğin son bulmasının ardından, dünyanın her yerinde bölgesel örgütlenmelerin ve çok taraflı faaliyetlerin geliştiğini söyleyebiliriz. Bugün Avrupa Birliği (AB), Kuzey Atlantik Paktı (NATO), Amerikan Devletleri Örgütü (OAS), (Bailes and Cottey 1992) vb. yapılar bu çeşit örgütlenmelerdir. Bu örgütler, bir devletin içinde bulunduğu uluslararası ilişkileri ilgilendiren ve bölgesel ülkelerle coğrafi, dini veya ulusal bağlantıları içeren bir nevi güvenlik merkezleridir. Bu ilişkiler, genel anlamda çıkar ilişkisine dayalı, ekonomik ve politik etkileşimlerdir. Birçok ülke özellikle ekonomi ve güvenlik alanlarında bölgesel bütünleşmeyi sağlamak için çalışmaktadır. Avrupa entegrasyonu (European integration) bu amaçla kurulmuş önemli organizasyonlardan biridir (LOMBAERDE and SÖDERBAUM 2013).

Bu düzeyin altında güvenlik (Sub-Regional Security) olarak isimlendirilen güvenlik çeşidi yer almaktadır. Bu ise belirli sayıdaki devletlerin, ortak çıkarları doğrultusunda belirlenen güvenlik gereksinimlerinin güvence altına alınmasıyla ilgilidir. Bu çerçevede bir gurup ülkenin, belirli bir zamanda belirli tehlikelere karşı belirli tedbirler alarak ortak savunma ve beraber hareket etme işbirliğidir. NATO, Körfez İşbir-

liği Konseyi ve Mağrip Birliği bu duruma örnek olarak gösterilebilir (Buzan, et al. 2003).

3. Düzey: Uluslararası (Küresel) Güvenlik:

"Uluslararası toplum" tek başına bir toplum değil, çoğul bir yapı ve birliktelik-tir. Dünya üzerindeki toplumların tamamını ilgilendirmesinden dolayı bu kavram, uluslararası güvenlik olarak isimlendirilmiştir. Bu düzey, küresel anlamda devletlerin hareketleri ile ilgilidir. Soğuk Savaş sonrasında gelişen, Birleşmiş Milletler dâhilinde bir fikri yapının ortaya çıkmasıyla hayat bulmuştur. Bu akımın düşüncesi,"Dünyanın güveliği herkesin işidir" fikriyle açıklanabilir. Kendi güvenliğiniz, başkalarının güvenliğinin tehlikede olması pahasına elde edilemez. Zira güvenlikten yoksun yönler potansiyel tehlikedir. Güvenlik, ancak ortak çaba sonucu gerçekleşebilir (Booth 1999).

Bu birliktelik, bizlerin çeşitli devletlerden oluşan bir dünyada yaşadığımız, esas güvenlik kaynakları ve emniyet tehditlerinin devletlerarası düzlemde görülen korku, karşılıklı şüphe ve çatışmadan kaynaklandığı, dolayısıyla da hayatta kalmak için sürekli mücadele etmemiz gerektiği varsayımına dayanmaktadır. Ulusal güvenlik sorunu da birbirine zarar verebilecek silahlı bağımsız devletlerden ve karmaşık dünya düzeninden kaynaklanmaktadır. Ulusal güvenlik politikaları caydırıcılığı olan silahlı ulusal güçler meydana getirerek devletlerin sürdürebilirliğini sağlamaya yöneliktir (Jackson-Preece 2011). Ulusal güvenliğe dair bahsedilen model, "tüm devletler güvende olmadan, hiçbir devlet güvende değildir" noktasından temellendirilmektedir. Ayrıca Soğuk Savaşın başlangıcından itibaren "Dünya tektir veya hiçtir" sloganının savunulması yoluyla küresel bir birliğin önemli ön koşulları belirlenmektedir. İlgili yaklaşım, uluslararası ilişkilerde idealizm teorisine en yakın fikirleri içermektedir. Uluslararası hukuk ilkelerinin uygulanması yoluyla çatışmaların ortadan kaldırılması girişimi, uluslararası mahkemelere yönelme, güven oluşturma ve küresel yönetim sisteminde düzen oluşturma amacı ile kitlesel tedbirler almayı da kapsamaktadır. Dolayısıyla dünyayı güven içinde tutmak ve sürekliliğini korumak için desteklenmesi gereken yegâne fikir "Dünya tektir veya hiçtir" ilkesi olmalıdır (Heurlin, et al. 2006).

“Bölgesel çıkarlar” üzerine tesis edilen ilişkiler, ulusal ve küresel güvenliği oluşturmaktadır. Teknolojik devrim, henüz iletişim ve ekonomik anlanda dünyanın birbirine bağlanacağı ve evrensel güvenlik problemlerinin doğuşuna imkân veren bir seviyeye ulaşmamıştı. Bundan dolayı ulusal güvenlik kavramı ile henüz başlangıçta bütün dünyadaki tehditleri azaltma veya engelleme hedeflenmemiştir (Intriligator and Coulomb 2008 .

Bazı araştırmacılar ulusal güvenliği, BM’nin kuruluş anlaşmasına atıflta bulunarak, “Kolektif güvenlik” “Collective Security” olarak adlandırmaktadır. Bu salt bir ulusal sorumluluk olarak değil, bölgesel veya kitlesel bir sorumluluk olarak değerlendirmektedirler. Çünkü güvenlik sorunları, durum ve ilişkileri bozarak mevcut barış halini değiştirmeyi hedeflemektedir. Bahsedilen tehdit girişimine karşı bir baskı gücü oluşturulması ve uluslararası temel önlemlerin uygulanmasıyla güvenlik gerçekleşebilecektir. Bu durum, ortak güvenlik çıkarlarını korumak için ülke gruplarının kurulması ve üye ülkeler arasında uzun vadeli resmi bir taahhüt inşa edilmesi sonucunu doğurmuştur. “Kolektif güvenlik” kavramı, askeri savunma açısından coğrafi sınırları olsa dahi, güvenlik için geniş olanaklar sağlamaktadır (Aleksovski, et al. 2014).

Kolektif güvenlik, genellikle Milletler Cemiyeti ve Birleşmiş Milletler gibi uluslararası kurumlar tarafından yönetilen, sıklıkla uluslararası hukuk, uluslararası yardım ve yönetişim kavramlarıyla desteklenen bölgesel ve küresel bir kavram olarak görülmektedir. Güçlü devletler, kolektif güvenlikte küresel ve bölgesel bir rol üstlenmektedir. Bu devletler, küresel tehlikelere karşı mücadelede birlikte hareket etme konusunda, özellikle de askeri ve ekonomik kullanımında kendilerini yetkili görmektedirler. Küresel güvenlik veya kolektif güvenlik, insanlığın karşı karşıya olduğu tehlikeler karşısında uluslararası iş birliği, kolektif eylem ve karşılıklı çıkar ilişkileri göz önünde bulundurularak sağlanmaktadır. Örneğin, küresel ısınma ve dünyayı tehdit eden kuraklık sorunu, böyle bir uluslararası işbirliğini zorunlu hale getirmektedir. Çünkü uluslararası güvenliğin sağlanabilmesi, Güç Dengesi Sistemi ile Kolektif Güvenlik Sistemi mekanizmalarının çalıştırılmasına bağlıdır (Paulo 2014).

1.1.3. Güç Dengesi Sistemi:

Ülkelerden birinin diğerleri üzerinde tehakküm kurma ve siyasi dengelerine müdahale etme gibi meşru olmayan yollarla baskı kurmasının önüne geçilmesi için, bir askeri güç dengesinin oluşturulması ve bu konuda uluslararası sistemde güvenlik ve istikrar yaratılmasını anlatan bir teoridir. Bir ülkenin askeri açıdan güçlenmesi, o ülkeye çok yönlü bir üstünlük avantajı sağlamaktadır. Diğer açıdan bakıldığında ise güç dengesinin ihlalini de beraberinde getirmektedir. Zira söz konusu ülke, diğer ülkeler nezdinde bir tehdit unsuru olarak algılanabilmektedir. İlgili devletin uluslararası sistem içerisinde barış ve güvenliğin sağlanabilmesi için güç dengesine tabi olması gerekmektedir. Günümüzde dünya ülkelerinin birbirleri arasındaki silahlanma yarışı da güç dengesini sağlama çabasından kaynaklanmaktadır. Bu teoriye göre devletlerin askeri gücünü diğer ülkeler nezdinde kabul edilebilir sınırlar içinde sürdürmeleri, bir tür yazısız anlaşma olarak değerlendirilmektedir (Kaufman, et al. 2007).

Güç dengesi sistemi, 1648 tarihli Vestfalya Anlaşması'ndan sonra ortaya çıkmıştır. Devletlerin birbirlerine karşı kazanımlarını maksimize etme yarışına girmesiyle devam etmiştir. Güç dengesi bir dizi ülke arasında nispeten eşit bir güç dağılımının olduğu bir düzendir. Bu yapıda herhangi bir ülke kendi egemenliğini diğer ülkelere dayatma gücüne sahip değildir (Luard 2016). Güç dengesi iki durumda elde edilebilir. Bunlar:

a) Tehditlere karşı uluslararası düzeyde topluca mücadele edilmesi: Bu hareket tarzı mücadeleyi meşrulaştırmakta ve sistemi zayıflatmak isteyen ülkeler için caydırıcılık teşkil etmektedir. Uluslararası barış ve güvenliği sağlamak için ittifaklar kurma gereğini ortaya çıkarmaktadır. Bununla kapasiteler ölçüsünde aralarında tekabüliyet sağlama ve uluslararası güç dengesinin bozulmasını önlemeye çalışma hedeflenmektedir.

b) Kolektif/ Toplu güvenlik sistemi: Uluslararası örgütler ya da organlara üye olan her devletin bütün üyeleri bu güvenlik şemsiyesi altında sorumluluğunu üstlenecektir (Jerotijević and Palević 2016). Bu sistemde, tüm üyelerin güvenliğinin sağlanması ise belirli bir teşkilata ait devletlerin anlaşması anlamı-

na gelmektedir. Bu sistemle ilişkili bir bireyin güvenliği, tüm üyelerin güvenliğinin bir teminatı olup bir kişiye yönelik tehdit tüm üyelerine yapılmış sayılmaktadır. Kolektif güvenliğin sağlanabilmesi için iş birliği yapılmalıdır. Milletler Cemiyeti ve daha sonra Birleşmiş Milletler çatısı altında savaşları önlemek ve çözmek için ortaya konan çabalar söz konusu iş birliğine bir örnektir.

Kolektif güvenliğin uygulanabilmesi için bir takım hususlar göz ardı edilmemelidir. Örneğin, Birleşmiş Milletler Sözleşmesi gibi tüm taraflarca üzerinde anlaşılan genel güvenlik kuralları bulunması gerekmektedir. Aynı şekilde karar verme ve uygulama yetkisine sahip otoritelerin ya da organların var olması ve böylece çeşitli mekanizmaları işleterek devletleri sorumlu tutma yetkisine sahip olması gerekmektedir. Bir diğer husus da böyle bir uygulamanın işleyişine katkı sunacak ve bir denetim biriminin varlığı kaçınılmazdır. Zira Birleşmiş Milletler Güvenlik Konseyi yürütme ve karar alma merciidir. Birleşmiş Milletler Tüzüğünde, uluslararası barış ve güvenliğin sağlanmasına dair Güvenlik Konseyi kararları vardır. Bunlardan birisi de uluslararası ilişkilerde haksız yere silah tehdidiyle güç kullanılması (nefsi müdafaa dışında) yasağı vardır (Fiki 2018).

1.2. Uluslararası Güvenlik Analizinde Siber Güvenlik ve Teorik Eğilimler:

Sosyal bilimlerin bir parçası olan uluslararası ilişkiler, bir rakip grup içinde fikir ve teori temelinde birçok siyaset ve güvenlik alanının analiz edilmesine ve yorumlanmasına dayanmaktadır. Bahsedilen kuram ve düşünceler, belirli bir olguyu açıklamak amacıyla ortaya atılan problemleri çözmek amacıyla oluşturulmuştur. Güvenlik çalışmaları, uluslararası ilişkilerin en önemli araştırma alanlarından biri olmuştur. İletişim araçlarının, bilgi teknolojisinin ve yeni bir çatışma türü olan siber saldırıların çıkması, uluslararası güvenliğin yeniden analiz edilmesi ve bu tür çatışmalarla ilişkisinin incelenmesi gerekmiştir. Bu konuyla ilgili en önemli teoriler şunlardır:

1.2.1. Realizm Teorisi:

Gerçekçi/ realist teori, Uluslararası ilişkiler alanındaki en önemli teorilerden biridir. Realizm okulu, II. Dünya Savaşı'ndan sonra idealist akıma temel bir tepki olarak ortaya çıkmıştır. Realizm, uluslararası ilişkileri; güç, çıkar, savaş ve çatışma siyaseti üzerinden okumaya ve analiz etmeye yoğunlaşmış ve dünya çapında bu tür olguları çözümlemek ve anlamlandırmak için politik açıklamalar sunmayı amaçlamıştır (Hüseyin Hussein 2016, 2016).

Devlet, uluslararası ilişkilerde tek aktördür ve güvenliğin birincil referans noktasıdır. Uluslararası siyaset, "etik" kavramıyla özdeşleşmiştir. Bu bağlamda Makyavelli, etik kavramını, "gücün ürünü" olarak tanımlamaktadır. Thomas Hobbes ve Jean Bodin de aynı düşünceyi desteklemektedir.

Günümüzde uluslararası sistem anarşik ve devletlerin davranışlarını kontrol edebilen merkezi bir otoriteden yoksundur.

Gerçekçilik iki kavram üzerine kuruludur; güç ve ulusal çıkarlar. Realizmde, bu iki unsurun dış politikanın belirlenmesindeki etkileri incelenmektedir. Realist sava göre devletler, kendilerini savunmak veya diğer ülkeleri etkilemek için, askeri kapasitelerini geliştirerek, rasyonel olarak çaba göstermektedir ki, bu durum da kalıcı bir savaş tehdidi oluşturmaktadır. Aktörler arasındaki güç dengesi, istikrarı sağlama açısından önemlidir. Ancak güç dağılımının, güven eksikliği temeline dayandırılmış olması, endişeleri artıran bir sistemle karşı karşıya olduğumuzu göstermektedir (Waltz 2008).

Realizm ve Siber Güvenlik Teorisi:

Realist teori, uluslararası anarşik sistemde öz güvenliğini sağlamaya çalışan birincil aktör olarak, devletin incelenmesiyle ilgilidir. Bu teori; ülkeler arasındaki güvenlik konularını ve güç dağılımını analiz ederek, ilgili ülkelerin politikalarını açıklamaktadır.

Realizm kuramının siber alandaki rolü, özellikle siber savaşların ortaya çıkmasından sonra devlet ve aktörlerin davranışlarını tahmin etmek, anlamak ve yorumlamak için, sanal âlemdeki olgulara ve kavramlara bu teorinin varsayımlarının uygulanabilme olasılığının anlaşılmasıyla belirlenecektir. Realizm teorisinin, siber uzayda uygulanabilirliğini anlayabilmek için daha ayrıntılı olarak incelememiz gerekecekitir.

Birincisi: Uluslararası Sistem anarşiktir:

Uluslararası sistem, iradesini dayatabilen ve kararlarını uluslararası sistemdeki aktörlere uygulayabilen baskın bir merkezi otoriteye sahip değildir. Bu faktör, yeni realistlerden Kenneth Waltz'ın, "Uluslararası Politika Teorisi" kitabında söylediği gibi, uluslararası sistemdeki aktörler arasında güvensizlik hissine yol açmaktadır. Söz konusu his, devletlerin emniyet önlemleri almalarını sağlayacaktır. Bu araçların ve önlemlerin en önemlileri güç unsurunu artırmaktır. Gücün artması, uluslararası sistemde diğer ülkelerin güvenlik ve istikrarının azalmasına da yol açacaktır. Çünkü bir devletin uluslararası sistemde, güç potansiyeline yükselmesi, diğer ülkeler arasında sahip oldukları güvenlik miktarında bir azalma duygusu yaratacak, onları güvenlik ikilemi olarak bilinen bir sonuca, belki de ülkeler arasında rekabete ve silahlanma yarışına girmeye itecektir (Waltz 2010).

Siber alan, uluslararası sistem kadar anarşiktir. Realist James Adams "Sanal Savunma/Virtual Defence" adlı makalesinde; "internetin, dünya üzerinde farklı koşullarda yaşayan insanların aynı bilgilere erişmesine izin verdiğine değinmekte ve hükümetlerle devlet dışı aktörler arasında eşitlik yarattığına"(Adams 2001) dikkat çekmektedir. Artık yabancı hükümetlerin veya gençlerin bilgisayardaki karmaşık saldırıları nedeniyle hükümet veritabanlarının ve kamu tesislerinin istila edilebileceği bir dünyada yaşanmaktadır. Böylesi atakların ve belirsizliğin varlığı tüm ülkeler için yeni bir güvenlik sorunu yaratmaktadır. Siber güvenlik, ayrıca siber alandaki tehdit ve tehlike kaynaklarının tanımlanması, saldırı ve savunma kapasitelerini saptama gibi bir takım güçlüklere sahiptir. Bu da önemli endişeler oluşturmakta ve güvenlik sistemini çok gergin bir noktaya taşımaktadır (Chauvin 2016).

“Siber alan, merkezi bir hükümete tabi olmayan anarşik bir sistem altında yeni bir uluslararası savaş alanı haline geldiğinden, (Mills 2010)“realist güvenlik” paradigmasına mükemmel bir şekilde uymaktadır. Bu durumda, her ülke tek başına ya da asla güvenemeyecekleri müttefikleriyle ayakta durmakta, gücünü inşa etmeye ve savunmasını geliştirmeye çabalamaktadır. Öte yandan diğer ülkelerin her atılımının, güvenliğe doğrudan bir tehdit oluşturabileceği endişesini de göz ardı etmemektedir.

Siber alanın düzenlenmesi, siber güvenlikle ilgili uluslararası mevzuatın oluşturulmasıyla, devletler tarafından kabul edilen ve Birleşmiş Milletler gibi kuruluşlar tarafından denetlenen yasalar dâhilinde bir küresel işbirliği gerektirmektedir. Aynı şekilde bu ceza adaleti sistemindeki aktörlerin eğitimini de gerektirmektedir.

Adli personele ve kolluk kuvvetlerine, uygun adli bilişim ve soruşturma araçları sağlanarak suç niteliği taşıyan davranışların tanımı yasal çerçeveye oturtulmalıdır. Dijital kanıtların belirli özellikleri göz önüne alınarak usul kurallarının geliştirilmesi önem arz etmektedir. Bu noktadan hareketle siber suç alanında, eğitime önem verilmelidir. Öte yandan dijital kanıt toplama ve cezai kovuşturmanın etkinliğini sağlamada büyük sorunlara neden olan, sistem operatörlerine yönelik bilgi ve donanıma önem verilmelidir. Böylece uluslararası yasalara da uygun şekilde caydırıcı önlemlerin alınması mümkün olacaktır.

Uluslararası işbirliğinin yanı sıra; özel sektör şirketlerin (İnternet servis sağlayıcıları) işbirliği de bu konuda önem arz etmektedir.

Bu önemli tedbirlere rağmen, Siber güvenliğin tam olarak sağlanması yeterli değildir. Ancak bu, yasal yöntemlerle temel hak ve hürriyetlere saygının artırılacağı ve siber suçlara önemli ölçüde etkili bir yanıt verilebileceği göz ardı edilmemelidir.(Nations 2019)

Ancak devletleri ve hükümetlerini yasal kuralları uygulamaya zorlayan bir unsurun olmaması temel problemdir. Bu nedenle, siber uzay karmaşa ve düzensizlikten muzdariptir. Dolayısıyla, realist teorinin varsayımları siber güvenlik uygulamaları için geçerli görünmektedir (Jabbour 2015).

İkincisi: Devlet, Uluslararası İlişkilerde Tek ve Ana Aktördür:

II. Dünya Savaşı'ndan sonra Hans Morgenthau, klasik gerçekçiliğin/realizmin temellerini Uluslar Arası Politika adlı kitabında ortaya koymuştur. Bu eser daha sonraki realist yazıları yönlendiren teorik bir çerçeve haline gelmiştir.

Bu kitap aracılığıyla uluslararası ilişkilerde insan doğasından uzak bir bilimsel teori şekillendirilmek istenmiştir. 1648'de Vestfalya Antlaşması uyarınca ortaya çıkan ulus devletler, uluslararası ilişkilerde birincil ve büyük aktör olduğu ve uluslararası sistemdeki temel analiz birimi olduğu düşünülmekteydi. Devlet, dış dünya ile olan ilişkilerinde, dış politik yönelimlerini uyumlu hale getiren bir varlık olarak görülüyordu. Coğrafik yapı bağlamında kimi ülkeler, diğer ülkelerden daha fazla işgal edilme potansiyeline sahiptir. Bazı ülkeler diğerlerinden daha stratejik konumdadır. Ayrıca coğrafik bölge, iklimi ve araziyi de etkilemekte ve bir ülkenin diğer ülkelerle yüzleşmek için kapasitelerini seferber etme yeteneğini belirlemektedir (Sempa 2015).

Devletin siyasi veya bölgesel sınırlarını tanımayan dijital alan, yerel veya uluslararası aktörlerin, bir devletin egemenliğini kabz etmesine ve bir ülkenin siyasi ve bölgesel sınırlarına nüfuz etmesine imkân tanımıştır. Siber uzayda bu teknolojik gelişmenin devam etmesi, devletin sınırlarını kontrol etme, maddi, kültürel ve ahlaki değerlerini koruma yeteneğini azaltacaktır. Joseph Nye, siber alanla ilgili "güç dengesinin değişimi"(Betz and Stevens 2011)konusunda ele aldığı yazılarında bu sonucu öngörmektedir.

Özellikle internet servis sağlayıcılarının çoğu, yönetimi belirli bir ülkenin politikasına tabi olmayan özel şirketler olduğundan, bireylerin, kuruluşların ve terörist grupların internete erişmesi ve devletin egemenliğini tehdit etmesi mümkündür. Bu durum aynı zamanda devletin siber alanla yakından ilişkili tüm önemli sektörlerini, özellikle de küresel şirketlere açık ve ulaşılabilir hale gelen ekonomi sektörünü koruma yeteneğini zayıflatmaktadır. Ülke ekonomisini ve sosyal dokusunu siber güvenlik riskleriyle karşı karşıya bırakmaktadır. Bu nedenle devletlerin haklarını asgari

düzeyde elde edebileceği yasal ve politik standartlar oluşturulması için, ivedilikle uluslararası iş birliği sağlanmalıdır (Deibert and Crete-Nishihata 2012).

Siber saldırılar nedeniyle, ülkelerin siyasi sınırlarının tehlikede olduğuna dair endişelerin ortaya çıkması sonucu birçok ülkede işgücü sistemlerine elektronik uygulamaların devreye konulması, siber politikalardan büyük ölçüde etkilendiğini göstermiştir. Teknolojik alt yapısı olan ve bütçeleri birçok ülkenin bütçesini aşan şirketler kolayca hareket edebilmektedir. Korsanlık konusunda belki bir işlem ya da kişi yüzünden savaşlar yaşanabilmekte veya önemli tesisler kapatılabilmektedir. Sosyal medya aracılığıyla, sahte hesaplar üzerinden siyasi süreçleri manipüle ederek toplumları kargaşaya sürükleme ve hür iradelerini kontrol etme müdahaleleri son yılların en önemli siber saldırıları olarak ortaya çıkmıştır. 2016 yılında ABD'de gerçekleştirilen başkanlık seçimlerine, Rus bilgisayar korsanlarının gerçekleştirdiği müdahale buna bir örnektir (Persily 2017).

Uluslararası düşman kurum ve kuruluşların siber alanı kullanarak bir devletin egemenliğini tehdit girişimleri, devletin uluslararası ilişkilerin ana aktörü olduğu realist teorinin varsayımlarıyla durdurulabilmesi mümkün olacaktır. Aksine bu alandaki tehditler her geçen gün daha da yoğunlaşacaktır. Aslında çoğu İnternet servis sağlayıcısı, belirli bir ülkenin kontrolü altında olmayan kendi politikalarını takip eden özel şirketlerdir. Ancak kötü niyetli oluşumların ellerinde bir tehdit unsuru olmaması için önemli tedbirlerin alınması kaçınılmazdır (Habermas 2006).

Üçüncüsü: Ülkeler Güvenliklerini Sağlamak İçin Güçlerini Artırmaya Çalışırlar:

Uluslararası anarşik sistem altında ülkeler, sahip oldukları doğal, coğrafi ve demografik varlıklara ek olarak bilimsel ve teknolojik kapasitelerine güvenerek kendi güçlerini desteklemeye ve geliştirmeye çalışacaklardır.

Ayrıca, ülkeler arasındaki ittifaklar devletlerin savunma yeteneğini artırabilir. Realist teori, siber saldırılar bağlamında uluslararası sistemdeki aktörlerin güç dağılımının kapsamını anlamak için kullanılabilir. Ayrıca bu teori, siber gücün katkısının ne kadar olduğunu gösterir. Bu merhaleden sonra belirli sınırlar içinde devletin gele-

neksel gücünü artırması, düşmana zarar verme ve tehdit etme kabiliyetlerini kanıtlama safhası gelmektedir.

ABD ve İsrail, İran'ın nükleer reaktörlerinde çok sayıda santrifüjü yok eden Stuxnet virüsünü geliştirdiğine dair iddialarını buna dayandırabiliriz. Nitekim İran Sanayi Bakanlığı yetkililerinden Mahmoud Leah açıklamasında; "Otuz bin bilgisayara virüs bulaşmıtır" diyerek, bu tür girişimlerin ülkesine karşı yürütülen elektronik savaşın bir parçası olduğunu vurgulamıştır (aljazeera.net. 2010.). İran, bir takım füze sistemlerine virüs saldırısı gerçekleştirmek isteyen bir İsrail casus ağını tutuklamıştır. İranlı bir üst düzey yetkili ise ülkesinin e-savaşa karşı bir internet uzmanları ordusu hazırladığını dile getirmiştir.

Devletler Özgüvenlerini Artırmaya Çalışırlar:

Çoğu ülke, ABD ordusundaki elektronik komuta gibi geleneksel askeri güçlerini desteklemek için özel ekipler ve elektronik ordular kurmuştur. Siberuzay, farklı ortamlarda bir avantaj, üstünlük veya etki yaratarak devletlerin gücünü en üst düzeye çıkarmak için kullanılabilir. Sonuç olarak, politika yapıcıların sadece nükleer tesisler için değil, aynı zamanda diğer kritik altyapılar için ve siber alanda faaliyet gösterme kapasitelerini geliştirme ve kullanma becerisi için, siber güvenlik politikaları oluşturmayı düşünmeleri gerektiğini gösteren "siber strateji" terimi ortaya çıkmıştır.

Bu strateji, ulusal iktidar ve unsurları aracılığıyla hedeflere ulaşılmasını veya desteklenmesini sağlama, diğer operasyonel alanlarla birleştirme ve koordinasyon sağlama imkânı bulmaktadır.

Realist teori, siber tehditlerine karşı iradeyi harekete geçirmesiyle, düşmanı aciz bırakararak ya da tehdit ederek devletin kendi gücünü artırmaya katkıda bulunup bulunmadığını sorgular.

Bununla birlikte, siber gücün geleneksel askeri operasyonlarda alışılmış olduğu gibi hedefleri yok etme yeteneğinden yoksun olduğu da akılda tutulmalıdır. Bu nedenle, siber savaşa girişin düşük maliyetine rağmen, hedeflenen ülkeler için büyük bir tehdit oluşturup oluşturmaması tartışılabilir.

Dördüncüsü: Uluslararası Politikanın Etik İlkesi İle İlişkisi:

Etik, insan davranışları açısından iyi olduğuna inanılmayan veya kötülük olarak algılanan şeylerden kaçınmaya yönelik değerler ve idealler kümesidir. Politika ise insan topluluğuna liderlik etmenin ve yararlı olduğunu düşündüğü kanun ve kurallarla onları yönetme yollarından ya da araçlarından biridir.

Uluslararası ilişkiler; savaş, barış, ticaret, üretim, hak ve hukuk üzerine kurulan karşılıklı bir takım iyi ilişkiler ve çalışmalar olduğundan bu ilişkilerin etik karinesi üzerine kurulması kaçınılmazdır.

Machiavelli, siyaset ve etiğin insani ilke ve ilişkilerin belirli bir tarzını savunarak bir araya gelse dahi aslında çatışma içinde olduklarına inanmaktadır. Machiavelli kitabında "Hükümdar" siyasetin etik kurallara egemen olduğuna inanmakta ve politik amaçlara ulaşmak için her türlü aracın kullanılabileceğini düşünmektedir. Bu konuda şu ünlü tavsiyesini yapmaktadır: "Gaye, aracı meşru kılar." Böylece, özellikle Birleşmiş Milletler ortaya çıktıktan sonra, çoğu insan hakları sözleşmesi ve uluslararası sözleşmenin temeli haline gelen tüm geleneksel politikalar etik sözcüğünü kullanmışlardır (Lamus 2016). Bu nedenle Soğuk Savaş'tan sonra politik ahlaka bakış artmıştır.

Amerika Birleşik Devletleri tarafından yayınlanan değerlerin küresel etkisinin bir sonucu olarak insan hakları konusunda dünya ülkelerinde belirli bir aşamaya gelinmiştir. Günümüzde etik, uluslararası ilişkilerin önemli bir parçası olarak görülmektedir.

Siber güvenlik alanında, büyük güçler, özellikle Amerika Birleşik Devletleri, yumuşak güç kullanımına başvurmuştur. Yumuşak güç, Joseph Nye tarafından ilk kullanılan bir kavramdır. Zorlama olmadan çekme ve kendine katma stratejisidir. Bilgi ve veri teknolojisinin geliştirilmesine dayanan dış politika hedeflerine ulaşma konusunda ikna aracı olarak başvurulmuştur.

Yumuşak güç kullanımının sonuçlarının, askeri güç ve ekonomik baskı araçlarının kullanılmasından daha iyi sonuç alınabildiği kanıtlanmıştır (Nye and Joseph 2008).

Etik ve yumuşak güç terimleri Irak ve Afganistan savaşlarından sonra ABD'nin bir süper güç olarak, bir takım ülkelerin kişisel özgürlükler ve insan hakları ilkelerini umursamadığını ve ahlaki değerleri hiçe saydığını iddia etmesinden sonra sıklıkla kullanmıştır. ABD, söz konusu ülkeleri yeniden kazanma ve özellikle Ortadoğu bölgesinde gerçekleştirdiği savaşlara neden olarak gördüğü terör ve radikalizme karşı etik kuralları çerçevesinde demokrasiyi işletmek için bu kavramlara başvurmuştur.

Bilgi savaşı yeni olmasa da, siber teknoloji daha ekonomik bir silah olarak ortaya çıkmıştır. Düşmanlara ulaşılmada daha hızlı ve tehlikelere anında müdahale imkânı sağlamaktadır. Bununla beraber siber alanda gerçekleştirilen saldırılarda kimlik keşfi çok da kolay olmamaktadır (Melissen 2005).

Uluslararası güç dengesi istikrarı sağlayan bir unsurdur. Günümüzde ortaya çıkan güç dağılımı ise uluslararası sistemin, güvensizliğe dayanan yapısını belirleyen bir faktördür:

Hükümetler siber uzayda rollerini giderek daha fazla vurgulamakta ve kapasitelerini artırmaya çalışmaktadır. Böylelikle devletlerin diğer ülkeler ve uluslararası kuruluşlarla rekabet ederken, aralarındaki orantısız güç dağılımı, bir takım çekişmelere ve iktidar mücadelelerine neden olmaktadır (Zinnes 1967).

Güç dengesi teorisi, uluslararası ilişkilerde kalıcı ve dinamik kavramlardan biridir. "İktidarın dengesi" kavramının ortak başlangıç noktası, devletlerin rasyonel olarak hareket ettikleri temel varsayımdır. Bu yüzden, çatışmaları düzenlemek için daha yüksek bir otoritenin olmadığı kaotik sistemlerde güvenliklerini veya güçlerini en üst düzeye çıkarmaya çalışırlar. Bir kurumda meydana gelen ufak bir dengesizlik, uluslararası sistemdeki aktörlerin ve rakiplerinin artmasına çanak tutmaktadır. Bu durum çoğu zaman ve başka ülkelerin hegemonya olasılığına dair net kaygılar yaratmaktadır. Bu yüzden tüm ülkeler bu tür zafiyetler konusunda ihmalkârlıklarıyla yüzleşmeye hazır olmalıdır (Yılmaz 2008).

Daniel Kuehl, “siber güç”ü operasyon ortamlarında elektronik araçlarla etkili olmayı veya terör olaylarını durdurmak için, siber alanı kullanma kapasitesi olarak tanımlamaktadır.

Bu tanım üzerinden siber bir gücün uluslararası ilişkiler alanında ne kadar etki yaratabileceğinin bilinmesi gerektiği anlaşılmaktadır. Bu olgunun devletler ve uluslararası aktörler arasındaki güçleri yeniden şekillendirme ve dağıtma potansiyelinin var olup olmadığı bir faktör olarak varlığı ne kadar önemliyse, kendi ulusal çıkarlarıyla çelişen düşmanı kontrolün ötesinde eylemler yapmaya zorlamak da maddi güce benzer şekilde zorlama olasılığı değerlendirilmelidir (Kuehl 2009).

Tüm bu konuları anlamak için siber güç’ün unsurlarını incelemek, araç ve kullanım kapsamını çok iyi bilmek gerekir.

Siber güç, veri elde ederek saldırı ve savunma alanında kullanma sürecine dayanır. Saldırı, siber güç araçları kullanılarak düşmana zarar verme ve tehdit etme yeteneğini içerir. Küresel teknolojik gelişmeler, ülkelere ait büyük sektörlerin çoğunu internete bağlamıştır. Bunun amacı, işlemleri kolaylaştırmak, hizmet maliyetini azaltmak ve özellikle askeri sektör olmak üzere çeşitli sektörlerde başarıyı ve kaliteyi artırmaktır. En düşük maliyetle ve en az kayıpla etkili askeri operasyonlar gerçekleştiren insansız hava araçları gibi modern askeri endüstrilerin geliştirilmesi de modern iletişim sistemlerine ve özellikle de internete etkili bir şekilde bağımlıdır.

Siber güç bağlamında bilgi teknolojisine karşı artan güven, ülkeler arasındaki askeri güç dengeleri ve hesapları üzerinde önemli bir etkiye dönüştürmektedir (Hammes 2016).

Ayrıca, siber güç, askeri alanlarda güçsüz olan devletlere, kendilerinden daha güçlü olan ülkelere karşı savunma avantajı sağlamaktadır. Bu nedenle uluslararası arenada gücün yeniden dağıtılmasına katkı sunmaktadır. Kuzey Kore ve Çin’in binlerce hacker/ köstebek ve Çin’in bazı siber savaş taktikleri geliştirmesi buna bir örnektir. Zira bu ülkeler, Amerika Birleşik Devletleri’ne karşı çok sayıda casusluk kampanyası yapmakla suçlanmıştır.

Siber Gücü Maddi Güçten Ayıran Özellikler:

1- Bir ülkenin siber güç ve siber alandaki mücadele kapasitesini ölçmede Şeffaflığın olmaması nedeniyle bir takım zorluklarla karşılaşılmaktadır. Öte yandan siber dosyaları yöneten tarafların çoğunlukla askeri ve güvenlik kurumlarından oluşması nedeniyle karşılaşılan saldırı ile savunma kapasiteleri arasında sağlıklı bir değerlendirme yapılamamaktadır. Saldırgan tarafın amacının doğru bir şekilde yorumlanamaması, istenmeyen sorunların ortaya çıkmasına neden olmaktadır.

2- Saldırı kapasiteleri, esas olarak düşmanın savunma kapasitelerine göre belirlenmekte ve maliyet bakımından çok daha ucuza tedarik edilmektedir. Siber saldırılarlar, özellikle ekonomik alanda elektronik bilgi ve veri tabanlarına dayalı dijital sisteme geçmiş olan ülkelerde önemli maddi kayıplar getirebilir.

3- Geleneksel silahlardan farklı olarak, "siber silahlar" tekrar kullanılabilir ya da özel bir müdahale ile hepsi bozulabilir. Güvenlik açığı düzeltildiğinde veya saldırganların hedefi olan belirli bir güvenlik açığı kapatıldığında işe yaramaz hale gelebilir. Bütün bunlar silah ve mermi kullanılmadan gerçekleştirilebilir.

Henry Kissinger, güç algısının ve değerlendirmesinin sadece (silahların sayısı veya askeri kapasiteler) üzerine dayanan bir matematiksel hesaplama olmadığını, aynı zamanda ulus liderlerinin kalitesi, stratejilerinin türü ve benimsediği askeri doktrinler ve bu gücü etkili bir şekilde kullanma iradesini de dikkate alınması gerektiğini söylemektedir. Bu nedenle, bir ülkenin siber kapasitelerinin ortak algısı, eksik bir bilgi temelinde kurulmuş olsa bile, güç dengesini hesaplamak için bir temel oluşturabilir (Friedberg 1987).

Kissinger'in teorisine göre, kuvvetler dengesi sadece güce dayalı bir sistemdir. Bu nedenle, her karar bir silahlanma yarışına dönüştürülecektir. Oysa istikrarın özü, kısıtlamaların ana aktörler tarafından tanınmasıdır. Eğer uluslar barış istiyorlarsa, devletlerarasında istikrarlı ilişkiler yaratmaya odaklanmalıdır. Söz konusu istikrar iki temel koşula dayanmaktadır. Güçlü bir denge ve büyük güçler tarafından oluşturulacak uluslararası bir arabuluculuk faaliyeti ve meşruiyet sisteminin kabul edilmesidir. Buna genel anlamda "meşruiyet ilkesinin" kabulü denilmektedir. Bu sistemin ulusla-

rarası düzlemde, tüm büyük güçler tarafından kabul edilmesi anlamına gelir. Kissinger ayrıca, güç dengesinin, uluslararası sistemi devirme yeteneği ve caydırıcılığı açısından, ortak değerler üzerinde anlaşmaya varılmasının, bu arzuları engelleyebileceğine inanmaktadır" (Kissinger 1992).

Uluslararası ilişkilerin gerçekçi teorilerinin, siber güvenlik ve siber uzay ile ilgili konulara uyarlanabilir olduğu sonucuna vardık. Gerçekçi teori, devletlerin kendi gücünü en üst düzeye çıkarmak ve güvenlik çıkarlarını artırmak için siber uzayı nasıl kullandığını ve diğer ülkelerin İnternet kapasitelerine nasıl cevap verebileceklerini açıklamasına yardımcı olacaktır. Bundan dolayı uluslararası ilişkilerdeki rasyonel teorilerin, siber güvenlik ve siber savaş ile ilgili konularda daha geçerli olduğu sonucuna varılmıştır. Gerçekçi teori, ülkelerin kendi güçlerini en üst düzeye çıkarmak ve güvenlik çıkarlarını artırmak için siber teknolojiyi nasıl kullandıklarını ve diğer ülkelerin İnternet kapasitelerine nasıl yanıt verebileceklerini açıklamalarına yardımcı olmaktadır.

1.2.2. Liberal Teori ve Siber Güvenlik:

Liberal yaklaşım, özellikle barış araştırmaları konusunda uluslararası ilişkilere katkıda bulunan en önemli yaklaşımlardan biridir. Barışın, küresel siyasetin hedefi olup olmadığı ve küresel barışın nasıl sağlanabileceği konusu liberaller tarafından sürekli gündeme getirilmiştir. Uluslararası ilişkiler alanındaki ilk liberal fikirler, güçlüleri savaşlardan uzak tutmayı öğütleyen ve sulhun yönettiği bir dünyayı arzulayan Emmanuel Cruce (1623)'nin ve kalıcı barış teorisini savunan (Immanuel Kant)'ın makalelerinde görülmüştür. Robert Cohen ve Nye'nin realist teori eleştirisini gündeme getiren makalelerinde ortaya çıkmıştır. Bu fikirleriyle, uluslararası ilişkilerde devletin önemini inkâr etmemekle birlikte, küresel örgütlerin ve ulus ötesi şirketlerin önemi vurgulanmıştır. Uluslararası sistemdeki diğer eylemlerin yanı sıra, uluslararası iş birliği, ortak çıkarların gerçekleştirilmesi ve uluslararası sistemde barışın ve güvenliğin korunmasını sağlayacak siyasal örgütlerin ya da uluslararası örgütlerin kurulmasıyla barış ortamının sağlanacağı ve savaşların feshedilebileceği üzerinde durulmuştur (Nasruddin 2013).

Liberal Bakış Açısıyla Güvenlik Kavramı:

Güvenlik alanında liberalizmin savunduğu en önemli kavramlardan biri, kolektif güvenlik kavramıdır. Uluslararası sistemde bir aktöre karşı, yasadışı askeri güç tehditinde bulunan ya da uluslararası barışı ihlal eden üye veya aktörlere yönelik askeri müdahalede bulunmak bağlayıcı bir çözüm olarak görülüştür (Sur, 2013).

Bu sistem herhangi bir üyenin diğer üyelere saldırmasını önler ve uluslararası sistemde istikrarın sağlanmasına katkıda bulunur. Alman filozof Immanuel Kant, bu sistemin temellerini atan ilk düşünürlerden biridir. Bir ülkeye saldırıda bulunan ülkeyi caydırmak veya cezalandırmak için birlikte hareket edilebilecek uluslararası bir federasyonun kurulmasını önermiştir.

Birinci Dünya Savaşı'ndan sonra Milletler Cemiyeti'nin kurulmasıyla kolektif güvenlik sisteminin pratik uygulamasına geçilmiştir. Bu sistem, barışçı bir dünya vizyonuna sahip Amerikan başkanı Wilson tarafından savunulan uluslararası idealist ilişkiler teorisinin bir parçası olarak uygulanmaya konulmuştur (ÇALIŞ and Özlük 2007).

Liberal yaklaşımın savunduğu bir diğer kavram demokratik barıştır. Demokratik barış teorisi, Demokratik devletlerin birbirleriyle savaşa girmeyecekleri fikri üzerinde temellendirilmiştir. Çünkü bu yaklaşımda demokratik sistemler, halkların iradesini yansıtan sistemler ve politik anlaşmazlıkları çözmenin bir yöntemi olarak savaş ve yıkımı kabul etmeyen rasyonel iradeler varsayılmaktadır (Büyükbaş and Atici 2012).

Liberal düşüncede, güvenlik kavramı analizinde şu temel ve kalıcı dayanaklar benimsenmektedir:

1- Devlet, hükümetiyle, sivil toplum örgütleriyle, kanaat önderleriyle, ulusal kurum ve kuruluşlarıyla birlikte, uluslararası ilişkilerin önemli bir faktörüdür.

2- Devlet, kendi yaşamlarını organize etmek amacıyla yerel yönetimler oluşturan mahalli topluluklardan oluşmaktadır. Toplumun her bireyi, sistemde rol alan en önemli aktördür. Dolayısıyla liberal teoride toplum, devletten önceliklidir.

3- Devletler ulusal çıkarlarını aramaktadır. Bu nedenle ülkeler arasında ortak çıkarlar bulmak uluslararası barışı ve güvenliği koruyacaktır. Savaş ise dünya siyasetinde hiçbir zaman bir önkoşul değildir. Uluslararası iş birliği ve güvenliğinin sağlanması ve çatışma yoğunluğunun azaltılması için çalışan ilgili kurum ve kuruluşların güçlendirilmesi, barışın sağlanmasına katkı sunacaktır.

4- Demokratik sistemler, dünyada barışın yayılmasına katkı sağlayacak en önemli politik sistemlerdir.

5- Liberalizmin en önemli ilkelerinden birisi de ticaret özgürlüğüdür. Uluslararası ticari ilişkilerde karşılıklı çıkarların artırılması, ortak ekonomik bağların güçlendirilmesi ve ülke halklarının refah ve güvenliğinin temin edilmesi, bu anlamda değerli bulunmaktadır.

Liberalizm ve Siber Güvenlik:

Liberalizmde, siber uzayın toplumları etkileyebilecek en önemli alanlardan biri olduğuna inanılmaktadır. Zira modern toplumlarda, kitle iletişim araçları ve bilgi teknolojilerinin kullanımı yaygındır. Dolayısıyla bahsedilen mecrada sosyal ve siyasal değerlerin yayılması ve bu noktada kamuoyu eğilimlerinin şekillenmesi, devletin uluslararası sistemdeki duruşunu ortaya koymaktadır.

Siber Güvenlikte Liberal Teorinin En Önemli Uygulamaları

Devlet, uluslararası ilişkilerde önemli ve temel bir aktör olmakla beraber tek aktör değildir. Bu noktadan hareketle liberaller, Birleşmiş Milletlerin sadece siber güvenlik konusunda uzmanlaşmak üzere bir birim inşa etmesinin çok önemli olduğunu düşünmektedir. Onlara göre koşullar, uluslararası yasaların uygulanmasını içeren küresel yasaların hazırlanmasını gerektirmektedir. Siber alanda istikrarı sağlamak için uluslararası toplumun hepsini bağlayan bir mevzuat sağlanmalıdır. Zira Birleş-

miş Milletler örgütsel ve hukuki düzeyde siber güvenlikle ilgili görevleri tek başına yerine getiremeyecek ve tüm çabaları üstlenemeyecektir. Bu nedenle Avrupa Birliği, BM'yi beklemeksizin üyelerinin siber güvenliğin sağlanması için ciddi adımlar atmaları çağrısında bulunmuştur (Busannad 2016).

Beş üye devletin daimi üyeliğine dayalı Güvenlik Konseyi sistemi, II. Dünya Savaşı'ndan galip çıkan müttefiklerin zaferine dayanılarak tasarlanmıştır. Bu oluşum bir takım nükleer imkânlara ve gelişmiş bir siber kapasiteye sahip Kuzey Kore gibi birden çok devletin öne çıktığı siber dönemle çok uyumlu değildir. Dünyada siber savunma alanında öncü ülkeler arasında İsrail ve Finlandiya da bulunmaktadır (Shafqat and Masood 2016). 2013 yılında Birleşmiş Milletler siber güvenlik ve bilgi verileri konularını takip etmek için bir hukuk ve kamu yönetimi uzmanlarından bir ekip oluşturmuştur. Bu ekip, devletin bilgi iletişim teknolojisi alanındaki uygulamalrla ilgili olarak uluslararası hukuka uygunluğunun gerekliliğini ve devletlerin egemenlik kavramından doğan hak ve yükümlülüklerinin siber alanda da aynen geçerli olduğunu vurgulamıştır. Diğer aktörlerin bilgi ve iletişim teknolojilerinin yasadışı kullanımının, ülkenin ulusal güvenliği açısından durdurulmasının zorunlu olduğunu belirtmiştir (Kaljurand 2016).

Uluslararası hukukun siber alan için geçerli olduğuna dair genel bir kabul olmasına karşın, Pentagon'un hukuk ekibindeki üst düzey yetkililer, bu bağlamda egemenlik ilkesinin uluslararası bir temele sahip olmadığını vurgulamıştır. Bu açıklama doğrultusunda "yasadışı güç kullanımının, yasadışı müdahale düzeyine yükselmemesi şartıyla" başka bir ülkenin sivil altyapısına yönelik saldırılar yasaklanmamaktadır. Bu nedenle ABD Savunma Bakanlığına bağlı hukuk ekibinin, devletlerin egemenlik haklarını kısıtladığına dair görüş beyan ettikleri açıkça anlaşılmaktadır (Masahiro 2012).

Birey ve toplum, uluslararası ilişkilerde devletin davranışını anlamak için temel analiz araçlarıdır: Liberal düşünce, bireylerin ve içinde yaşadıkları toplumların önemini vurgulamaktadır. Devlet oluşumunun dayandığı temel çekirdek devlet mekanizmasıdır. Devlet yerel topluluğun bir parçasıdır ve toplumun çıkarına göre davranışını yönlendirmektedir. Dijital çağda, modern toplumlar giderek artan bir şekilde kü-

resel ağlar yoluyla iletişim ve bilgi teknolojilerine bağımlı olmuştur (Kymlicka 1989). Bu durum onları çağdaş dünyamızda hızla yayılan, birçok şekil ve yöntemle ülkelerin altyapısını hedef alan siber suçlara karşı savunmasız hale getirmektedir. Süper güç diye ifade edilen bir takım ülkeler, diğer ülke ve hükümetlerin altyapısına, sivil toplum kuruluşlarının veri tabanlarına ve bilgi sistemlerine saldırılar düzenlenmektedir. Bu teknolojik gelişmenin sonucu olarak, savaş yöntemleri ve hedefleri de kesinlikle değişmiştir.

Rakiplerin yok edilmesi ve topraklarının ele geçirilmesi geleneksel savaşlarda öncelikli hedeflerdendi ancak zaman ve külfet gerektirmekteydi. Günümüzde modern siber savaşlar daha az maliyetli, kontrol edilmesi ve hedeflenmesi daha kolay hale gelmiştir. Siber saldırılar yoluyla düşmanın motivasyonu düşürülebilmekte, manevi değerleri hedef alınabilmektedir. Halkın hükümete olan güvenini zayıflatarak devlet ve toplum arasında güven krizi oluşturulabilmektedrir. İletişim kanalları ve sosyal medya yoluyla ülke nüfusu üzerinde psikolojik savaş yürütmek için siber alanın kullanılmasıyla uygulanabilen bu tür politikalar, toplumun istikrar derecesini etkileyebilmektedir. Devlete ait kurumları temsil eden yetkililerin kendilerini güçsüz ve güvensiz hissetmelerini sağlamakta ve devletin otoritesini azaltmaktadır. Sosyal medya kullanımı ile siyasi çalkantıların ortaya çıkmasına tanık olan Arap Baharı ülkeleri bu durumun bir örneğidir (Adel Abdul. Sadek 2014a).

Liberaller tarafından savunulan en önemli ilkelerden biri; "Dünya barışı, ulusal ilişkiler ve işbirliği ile sağlanabilir. Savaşlar ise küresel politikada hiçbir zaman önkoşul değildir." Küresel barış için uluslararası işbirliği ve güvenliğin artırılması zorunludur. Birleşmiş Milletlere üye ülker 2001 yılında (GGE) Hükümet Uzmanları Grubu adlı bir yapı kurmayı kararlaştırmıştır: 2004 yılında bu amaçlarla çalışmasına başlayan gurup, Uluslararası bilgi güvenliği alanındaki potansiyel tehditleri tartışmak, küresel iletişim ve bilgi sistemlerinin güvenliğini güçlendirmenin zorunluluğu konusunda önemli tedbirler alınması gerektiğini deklere etmişti. Bu noktada 19 Aralık 2006 tarihli Genel Kurul'da bahsedilen tedbirleri pratik adımlara dönüştürmek için uluslararası düzeyde ilk kez siyasi bir karar alınmıştır. Bu kararın uygulanabilmesini de bu alanda çeşitli kurum ve kuruluşların oluşturulmasına bağlamışlardır.

Liberalizm, sivil toplum örgütleri, etnik örgütler ve ulusal yapılar gibi uluslararası sivil toplum aktörlerinin davranışlarının açıklanmasına yardımcı olmaktadır. Liberal teoriler, siber güvenlik, elektronik alan yönetimi ve dijital silahların kontrolü ile ilgili konularda devletlerarasındaki işbirliğini geliştirme konusundaki çabaları anlamak için önemli bulunmaktadır.

Liberal düşüncede, demokrasi en iyi politik sistemdir ve barışın dünyada yayılmasına katkıda bulunur: Liberaller, Alman düşünür İmmanuel Kant tarafından ünlü "To Perpetual Peace; A philosophical Sketch" makalesinde ortaya atılan bir teori olan demokratik barış ilkesine dayanır. Bazıları buna liberal barış teorisi demektedir. Bahsedilen fikir, "uluslararası ilişkilerde tecrübe edilmiş başarılı bir kanuna yakın bir olgu" olarak değerlendirmektedir. Demokratik süreçler, ülkeler arasında savaşsız geçen dönemlerin tarihi çalışmalarına dayanmaktadır.

Teoriye göre demokratik ülkeler, ülkelerinde bu sistemin olması ile yetinmemeli, tüm uluslararası toplum tarafından benimsenen uluslararası bir inanç olması için çaba sarf etmelidirler. Dolayısıyla demokratik barış teorisi gerçekleşene kadar, dünyanın tüm ülkelerindeki siyasi sistemler demokratik sistemlere dönüştürülmelidir. Bu teori, Soğuk Savaş döneminde Amerika Birleşik Devletleri tarafından benimsenmiştir. Irak'ın diktatör rejimini değiştirme ve kitle imha silahları geliştirmesini önleme iddiasıyla ülkenin işgal edilmesinin arka planında yer alan en önemli ilkelerden biri olmuştur. Başkan Bush, kitle imha silahı geliştirmeyen ve terörizme destek olmayan bir Irak'ın İsrail ve ABD'yi tehdit etmeyeceğini söylemiştir. Bu söylem doğrultusunda demokrasi, ülke ve toplumların isteğine bağlı bir yerel doktrin olmak yerine, diğer ülkelerle çatışma yaratma pahasına insanlara dayatılan uluslararası bir doktrine dönüştürülmüştür (Owen IV 2005).

Demokratik barış, temel olarak şu tezlerle şekillendirilmiştir:

1. Demokratik sistemlerde kurumlar arası çekişmeler, genellikle uzlaşma yoluyla çözüme kavuşturulur. Örneğin bir savaş kararı alınacağında demokratik sistem, Meclis iradesini gerekli kılmaktadır. Diktatörlerle yönetilen ülkelerde ise savaş kararları sadece devlet yöneticisinin talimatına bağlıdır.

2. Demokratik sistemler, bu sistemleri benimseyen insanların varlığını ve uluslararası ilişkilerde askeri gücün kullanılmasını reddeden medeni halkların çıkarlarına göre çalışan devlet kurumlarının varlığını gerekli kılar (Dixon 1993).

Demokratik Barış ve Siber Güvenlik Teorisi:

Demokratik sistem, insanların bilgi ve iletişim teknolojisinde meydana gelen bilimsel gelişmenin bir sonucu olarak ortaya çıkan tüm teknolojileri kullanmasına izin vermektedir. Teknik ilerlemelere izin verilmesi toplumun genel siyasi ve kültürel oluşumunu etkilemekte, sosyal medyayı kullanan ve sistemi destekleyen bir siyasi sınıfın yaratılmasını sağlamaktadır. Kamuoyunun yönlendirilmesinde ve iç ve dış politikasının desteklenmesinde modern bilgi teknolojisi önemlidir. Güvenlik ve Ekonomik İşbirliği Teşkilatı, bilgi sistemleri ve ağlarının güvenliğinin temel demokratik değerlerle uyumlu olması gerektiğini savunmaktadır (OECD 2004).

Demokratik yönetimin karşılaştığı en önemli zorluk, siber güvenlik alanında özel sektör ile demokratik hükümet kurumları arasında bir denge oluşturulamaması konusudur: Bilgi teknolojisi ve ağlar üzerindeki bilgi trafiğinin kontrolü, demokratik sistemin gizliliği, ifade özgürlüğü ve insan hakları gibi konular dengelenmelidir. Özellikle güvenlik alanında, kamu ve özel sektör arası ilişkilerde işbirliği ve denge olmalıdır (Buckland, et al. 2010).

Siber Güvenliğin Demokrasiyi Etkileme Biçimi:

Birçok demokratik ülke, ister otoriter hükümetler, ister STK'lar, ister terörist gruplar olsun, çeşitli aktörlerce siber saldırılara maruz kalmaktadır. Elektronik saldırı ve uygulamalarla düşünce özgürlüğü ve seçim bütünlüğüne müdahale edilmesi dünya çapında demokrasilere karşı açık ve büyüyen bir tehdit oluşturmakta, böylece toplumda demokratik sürece inancın kaybolmasına ve yönetimde kargaşaya yol açmaktadır.

Siber saldırıların seçimleri etkileme yolları:

a) Seçmen tutumları ile ilgili olgu ve görüşleri değiştirmek ve vatandaşların nasıl oy kullandığını bilmek.

b) Oy kullanma eylemine müdahale etmek: örneğin, seçmen kayıt dosyalarını ve verilerini hedef almak.

c) Oylama sonuçlarının, sayma ve sıralama mekanizmalarını, bunlarla ilgili veri ve bilgilerin değiştirilmesi.

d) Demokratik sürece siyasi katılım oranını azaltma ve meşruiyeti yansıtan oylamanın bütünlüğüne duyulan güveni ortadan kaldırmak.

Demokratik seçim çalışmaları sırasında siber saldırılara maruz kalan toplumların, genellikle demokrasiden uzak rejimlerle yönetilen ülkeler olduğu bir gerçektir. Rusya, Çin, Kuzey Kore ve İran gibi ülkelerde bu türden tehditlerin çoğunlukla otoriter rejim tarafından kaynaklandığı tespit edilmiştir.

ABD Ulusal İstihbarat Direktörü (John Ratcliffe) düzenlediği basın toplantısında, "Rusya ve İran'ın, ABD başkanlık seçimlerine müdahale etmek için vatandaşlarına ait bazı seçmen verilerini elektronik saldırılarla elde ederek, e-posta yoluyla iç karışıklık çıkartmayı amaçladıklarını ve bu dış müdahalelere karşı önlemler aldıklarını" açıklamıştır.

ABD'li yetkili, açıklamasında ayrıca "başta Başkan Donald Trump'a huzursuzluk ve zarar vermeyi amaçlayan bu dış güçlerin, ellerindeki verileri emelleri doğrultusunda kullanarak seçmenlere yanlış bilgi iletmek, onların kafasını karıştırmak ve Amerikan demokrasisine olan güveni zayıflatmak umuduyla kullanabileceklerini" dile getirmiştir.(aljazeera 2020) .

aynı zamanda New York Times, Kuzey Kore'nin siber gücü konusunda uyarıda bulunan uzun bir rapor yayınlamıştır. Raporda, Kuzey Kore'nin, ABD ile mücadelesinde yalnızca askeri gücüne güvenmediğine, aksine elinde bulundurduğu daha

tehlikeli bir gücün olduğuna işaret etmekte ve bu gücün kesinlikle küçümsenmemesi gereken bir tehdit olduğuna işaret etmiştir.

Rapor, geçen yıl New York Federal Rezerv Bankası'ndan bir milyar dolar çalma girişimine dikkatleri çekerek, Kuzey Koreli bilgisayar korsanlarının parayı Bangladeş Merkez Bankası hesabından elektronik saldırıyla çalmaya çalıştığını ve Kim Jong Un'un adamlarının bu hırsızlıktan 81 milyon dolar çekmeyi başarabildiklerinin altını çizilmiştir.

Rapor, Birleşik Devletler ve İngiltere güvenlik yetkililerinin ortaya çıkardığı bu ve benzeri büyüklükteki elektronik saldırıların Kuzey Kore bağlantılı olduğunu aktarmakta ve bu ülkenin elektronik ordusunun 6 binden fazla hacker içerdiğini, inkar edilemez bir güce sahip olduğunu ve gün geçtikçe bu gücün gelişmekte olduğunu belirtmektedir.(Sanger, et al. 2017)

Modern bilgi iletişim teknolojisine bağımlı toplumların, demokratik yapısının hedef haline gelmesi antidemokratik sistemlere boyun eğdirmeye zorlatacaktır. Bu saptama, siber alanda "Demokratik Barış" teorisini desteklemektedir. Örneğin, son dönemde Hollanda'daki Genel İstihbarat ve Güvenlik Kurumu, Ukrayna'daki oylama sırasında, internet sunucularından gelen saldırıların kaynağını Rusya, Çin ve İran olarak belirlemiştir. ABD Federal Soruşturma Bürosu (FBI) ve İç Güvenlik Bakanlığı (DHS) birimi Rusya'nın 2016 ABD seçimlerini etkileme amaçlı siber saldırılarıyla ilişkilerine dair çeşitli bilgiler yayınlamıştır (Norris and Grömping 2017).

WikiLeaks belgelerinin paylaşılması: E-posta yoluyla, seçmenleri etkileyebilecek bilgileri göstermek için "özel sunuculardan" erişilen belgeler özel bir zamanlamada yayınlanmıştır. Fransa Cumhurbaşkanı Emmanuel Macron da seçim sonuçlarını etkilemek amacıyla Rus resmi medyasını aldatıcı propaganda ve sahte haberler yaymakla suçlamıştır.

Böylesi tehditler seçimleri etkileyebilmekte veya bozabilmektedir. Bu durum, demokrasiye meydan okumakta, istikrarı ve ulusal güvenliği zayıflatmaktadır. Teknolojik zayıflık demokratik süreci de etkileyebilir. Çünkü bir devletin tüm mahremiyetini dış saldırılara açık hale getirmektedir (Williams, et al. 2016).

Bu nedenle, siber saldırılar demokratik sürecin bütünlüğüne doğrudan ve dolaylı bir tehdit olabilmektedir. Zira bu tehditler genellikle demokrasi ve meşruiyete karşı halk desteğini baltalamak niyetiyle yönlendirilirler.

Demokratik sistemler, bu tehditleri bertaraf edebilmek için uzmanlardan oluşan bir siber güvenlik çalışma grubu oluşturmalı, internet ve yönetim için küresel bir yasama mekanizması formüle etmelidirler. Bu mekanizma demokratik yönetimi ve şeffaflığı teşvik edip ortak değerleri yansıtmalıdır(Piccone 2017).

Joseph Nye, "Yumuşak Güç" ün uluslararası politikada diğer aktörleri "Kaba Kuvvet" kullanmadan daha iyi ikna ederek etkileyebileceğini savunmaktadır. "Yumuşak Güç", kendi içinde yeterli olmakla beraber, "Sert Güçle" birleştiğinde çok yönlü bir güç haline gelir. Bu kombinasyon yeni değildir. Tarihte Roma İmparatorluğu bu iki güç'e birden hükmediyordu. Roma lejyonlarının gücü ve Roma uygarlığının çekiciliğine dayanıyordu Amerikan liderliği de halen bu kombinasyona sahiptir (Nye Jr 2004).

ABD'nin, İzleyicileri, orduları ve karar vericileri etkilemek amacıyla belirli mesajları, fikirleri ve eğilimleri yaymak için modern medya ve internet hizmetlerini kullanarak siyasi düşünceleri, algıları ve seçim süreçlerini manipüle eden uzun bir geçmişi vardır. 2011'de Gelişmiş Savunma Araştırma Projeleri Ajansı (DARPA) stratejik iletişime ulaşmada sosyal medyanın önemine dair bir program açıklamıştır. Bu programın amacı, özellikle Amerikan kuvvetlerinin konuşlandırıldığı alanlarda Savunma Bakanlığı'nın sosyal medya üzerinde gerçek zamanlı ve eşgüdümlü hareket etme anlayışını geliştirmektir. ABD Savunma Bakanlığı'nın stratejik çıkarlarına hizmet eden medya mesajlarını yayınlamak için iletişim sitelerini kullanması da hedeflenmiştir (phys.org 2011).

Liberalizmin en önemli ilkelerinden biri serbest ticaret ilkesidir: Dış ticaret, ülkeler arasında mal ve hizmet alışverişine bağlı olmasından dolayı bir devletin ekonomik kalkınmasının temel direğidir. Ülkeleri ekonomik olarak birbirine bağlayan ve üretimlerinin fazlasını harcamasına veya ihtiyaçlarını diğer ülkelerin üretim fazlasın-

dan ithal etmelerine izin veren bir köprü olarak da düşünülebilir. İnternetin küresel olarak yayılmasından sonra, dijital veya elektronik ticaret terimi ortaya çıkmıştır.

E-Ticaret: "Elektronik ortamda ticari bilgilerin paylaşılması, ticari ilişkilerin sürdürülmesi ve telekomünikasyon ağları üzerinden ticari işlemlerin yapılması" şeklinde tanımlanmaktadır (Molla 2001).

Malların, hizmetlerin ve bilgilerin satılması ve alınması için çevrimiçi/online işlemlerin tümü bu terimin kapsamındadır. Ürünler, hizmetler, bilgi transferleri ve ticari talebleri artırmak gibi geri dönüşlerin üretilmesini destekleyen elektronik hareketlere izin veren bir sistem olan E-Ticaret, çevrimiçi satış ve müşteri destek operasyonlarının internet üzerinden para transferi yapmasını sağlamaktadır. Bu kavram ayrıca satıcıların, ithalatçıların, şirketlerin veya mağazaların (aracılar, alıcılar) iletişim kurduğu, ürün ve hizmetlerin elektronik parayla ödenen sanal veya dijital biçimde sunulduğu çevrimiçi bir pazara benzetilmektedir (Wigand 1997).

Liberal yaklaşım, sermayenin ve bir bütün olarak dünya ülkeleri arasında mal ve hizmet hareketini kolaylaştıran dijital ticaret de dâhil olmak üzere serbest ticaret ilkesinin en önemli destekçilerinden biri olarak kabul edilmektedir.

1.2.3. İnşacılık Teorisi ve Önemi:

İnşacılık, 1980'li yılların sonunda uluslararası ilişkilerde, hâkim eğilimlerin bir eleştirisi olarak ortaya çıkmıştır. inşacılığın temelleri Giambattista Vico'nun çalışmalarından kaynaklanmıştır. Bu terimi ilk defa kitabında 1989 yılında yapısal gerçekçiliği eleştiren Nicholas Onuf kullanmıştır. 1992 yılında yayınlanan (Anarchy Is What States Make of It: The Social Construction of Power Politics) başlıklı makalesinde yapılandırmacılığın duayen ismi olarak bilinen Alexandr Wendt, bahsedilen kavramı gündeme getirmiştir. Yapılandırmacı teori, liberal gerçekçi teorilerin uluslararası ilişkilerdeki küresel gelişmelere rasyonel açıklama konusundaki başarısızlığına bir tepki olarak ortaya çıkmıştır. Özellikle Soğuk Savaşın sona ermesinden, Sovyetler Birliği'nin çöküşünden ve egemen teorilerin gelişmeleri tahmin edememesinden ötürü uluslararası siyasette yeni arayışlar belirmiştir. Özellikle milliyetler ve azınlıklar, terörizm, terör örgütleri, kimlik ile ilgili meselelerin yeni ilişkilerin ortaya çıkması

üzerine bu sorunların uluslararası boyutları ve küresel politika alanındaki etkileri tartışılmıştır (Wendt 1995a). Uluslararası ilişkilerde yapılandırmacı teori, bir köprü vazifesi görmektedir; bilimsel gerçeklerin yorumlanmasındaki nesnel eğilime dayanan epistemolojik pozitivist teorilerle gerçeğin sosyal çerçevelerin ürünü olduğunu savunan post pozitivist teorileri birbirine bağlamaktadır. Post pozivist fikirler, düşünürlere yaşadıkları gerçeklik içinde problemleri yorumlamalarını gerektiren spesifik tarihsel süreçlerin bir sonucudur (Wiener 2006).

Robert Cox, "bir teorinin bir kişiye ya da belirli bir hedefe hizmet ettiğini" vurgulamaktadır. Kuramlar belirli bir konudan etkilenen düşünür ve teorisyenlerin kişisel motivasyonlarından kaynaklanmaktadır. Şahsi meraklarla incelemeye yönelen araştırmacılar, olguları yorumlamaya ve mevcut verilere göre analiz etmeye çalışmaktadır. Yapılandırmacı teori konu ve öz/özne arasındaki ayrımı esas almaktadır, çünkü onlara göre teorilerinin açıklamayı amaçladığı şeyleri yaratan insanlardır (Schouten 2009).

İnşacı Teorisinin Varsayımları:

Bu yaklaşımın en önemli hipotezi, uluslararası süreçlerin ve iç çatışmaların, uluslararası sistemin anarşisinin bir önkoşulu ve kaçınılmazlığı değil, daha ziyade küresel meşruiyet kapsamında egemen sınıfların kimlik/identy, din ve çıkarlarındaki tutarsızlıkların bir ürünü olduğudur. Böylece dünya, dini ve sosyal bir doğanın çatışmalarına ve anlaşmazlıklarına tanıklık edecektir. Samuel Huntington Medeniyetler Çatışması kitabında bu durumu öngörmektedir. Soğuk Savaş sonrası dünyada bir ideolojiler çatışması değil, medeniyetler çatışması olacağını düşünmektedir. Çin Konfüçyüsçülüğü ile birleşen İslam medeniyetinin Batı medeniyeti için büyük bir tehdit oluşturacağını görmektedir. Bu tez akademisyenler ve hatta karar vericiler arasında, özellikle 11 Eylül olaylarında ve Huntington tezinin tahminlerinin gerçekleştiği inancından sonra büyük ilgi görmüştür. Bush zamanında Amerikan dış politikasında medeniyetler çatışması tezinden yararlanılmıştır. Irak'ın işgaliyle Doğu ile Batı arasındaki mücadeleden Kuzey, "Batı Uygarlığı" ve Güney "İslam Medeniyeti" arasındaki mücaledeye geçileceği dillendirilmiştir (Henderson and Tucker 2001). Bu sav, çoğu Batılı ülkenin ve ABD'nin İslamofobi içerikli kampanyalar, bazı terörist

olaylardan ve eylemlerden faydalanarak İslam imajının kasıtlı ve sistematik bir şekilde bozulmasını hedefleyen çabalarla uyumludur. İslam ve Batı arasındaki çatışmanın en önemli araçlarından biri haline gelen sosyal medya ve bilgi teknolojisinin tüm teknolojik ve medya kapasiteleri söz konusu çerçevede kullanılmıştır.

Yapılandırmacılar bilinen şekildeki tanımları reddettiklerinden, ulusal çıkar, kimlik ve ulusal güvenlik gibi uluslararası ilişkilerdeki temel kavramlarda pozitivist teorilerden farklı bir konum almaktadır. Ulusal çıkarlara ulaşmada ve devletin dış ve iç politikasında yansıyan kamuoyu eğilimlerini belirlemede büyük rolleri nedeniyle, yapılandırmacılar, değer ve inançlara büyük önem verdiklerinden, çıkarların şekillendirilmesinde kimliklere bir rol vermektedir (Russett, et al. 2000).

Yapılandırmacı/sosyal inşacı bir bakış açısından, Soğuk Savaş sonrası dünyadaki ana sorun, farklı grupların kimliklerini ve çıkarlarını nasıl algıladıklarıdır. Yapılandırmacılık, faillerin kimliklerine olan ilginin artmasını sağlamaktadır, toplumların kimlikleri ifade eden ulusal algıyı, ülkeler arasında müşterek ve genel kurallar belirlenmesine dayanan küresel bir algıya dönüştürmemize imkân tanıyacak ortak çıkarlar saptanabilir. Dolayısıyla, ülkeler arasında otomatik bir güvenlik problemi yoktur.

Giderek artan bir şekilde, internetin çatışmalar sırasında kullanımı, kamuoyu veya belirli bir ülkenin görüşü üzerinde veya milliyetler, doktrinler ve dinler hakkında çeşitli şekillerde bir etki aracı olmaktadır. Çünkü iletişim özgürlüğü vasıtasıyla halklar arasında tanışma, kültür alışverişi ve karşılıklı etki için daha geniş bir alan temin edilmektedir.

İnternet iletişimi yoluyla modern çatışmalarda, toplumdaki bazı kültürel grupların arasında, din veya etnik kimliklerinin saldırı altında olduğu atmosferini oluşturmak için mesajlar yayılmaktadır.

Topluluk düzeyinde siber güvenliği artırmak için, ülkeler kamuoyuna farkındalık ve yardım eğitimi sunabilir, ayrıca internetteki yıkıcı kampanyaları denetleyebilen kanunları düzenleyebilir (Tiirmaa-Klaar 2011).

Toplum, eğitim kaynaklarından, sosyal ağ sitelerinden, web uygulamalarından, alışveriş sitelerinden, internet üzerinden pazarlama yollarından etkilenmektedir. Sosyal medya, belirli insan gruplarına dini nefret ve kötü ulusal ve ırkçı fikirlerin yayılmasına ve ideolojik ve dini çatışmaların gelişmesine kötü katkıda bulunabilmekte, aynı zamanda sosyal sistemdeki sınıfları da olumsuz etkilemektedir. Çünkü yoksullar ile zenginler arasındaki geniş uçurumun boyutunu açığa çıkarmakta ve böylece ülkedeki siyasi ve güvenlik gerçeğini yansıtacak sosyal huzursuzluklar yaratabilmektedir (Adel Abdul. Sadek 2014a).

Öte yandan web site oluşturma maliyetinin düşük olması, dağıtım kolaylığı ve verimliliğin artması, internette yeni ve çok sayıda aracı kurumun ortaya çıkmasını teşvik etmiştir. Sivil topluma ek olarak mevcut uluslararası hükümet veya hükümet dışı aktörlerin faaliyetleri internetle aktifleşmiştir. Belirli konular etrafında uluslararası kamuoyunu harekete geçirme kapasitesi bulunmaktadır. Modern ağlara sahip toplumlarda karar verme süreci kolaydır, krizlerle sosyal realiteyle uyumlu ve etkin politikaların belirlenmesi daha hızlıdır. Bu durum toplumda katılım ve rıza oluşturmakta, daha etkin ve hassas kararlar alınmasını öncelemektedir. Siber alanın, yeni toplumsal rollerin ortaya çıkmasında, siyasi performansların iyileştirilmesinde, kamusal alanda yeni aktörlerin ortaya çıkışında ve küresel düşüncenin rolünün yeniden şekillendirilmesinde etkisi vardır (Semenova 2011).

Siber Uzayın Devlet ve Toplum İlişkisi Üzerindeki Etkisi:

Siber alan, Facebook ve Twitter gibi sosyal ağlar aracılığıyla devrim-ayaklanma hareketlerinde rol oynamıştır. 2007 Myanmar, 2009 Moldovya ve 2009 İran olaylarındaki etkisinden dolayı bahsedilen olaylar, "Twitter" devrimi olarak bilinmiştir. Bu ağlar etkisiyle ortaya çıkan sosyal, kültürel ve politik değişimler çeşitli ülkelerde farklı seviyelerde yaşanmıştır. Son on yılda (Irak) dâhil Arap dünyasında iletişim ve bilgi teknolojisinin yayılmasının büyümesinde büyük bir sıçramaya tanık olunmuştur. 2000'den 2011'e kadar olan süreçte iletişim teknolojisindeki gelişme % 1250'ye ulaşmış, web 1,0 neslinden web 2,0 nesline geçilmiştir. Dolayısıyla medyada blogların, sosyal ağların dosya ve wiki paylaşım yazılımlarının ve haber değişim hizmetlerinin ortaya çıkmasını içeren bir devrim kaydedilmiştir. (Adel Abdul. Sadek

2014b). Uluslararası sistem yapılandırmacılar açısından bir dizi değer, kural ve yasa içeren sosyal bir yapıdır. Bu yapı, aktörlerin kimliğini ve çıkarlarını etkilemektedir. Uluslararası sistemin tabiatı, toplumun doğası, değerleri ve kültürünün ve sosyal etkileşimler devletin davranışına da yansımaktadır. Devletin davranışının devlet sınırları içindeki sosyal etkileşimlerin sonucu olduğunu ifade etmektedir. Yapılandırmacı teori, dünyanın bir grup ülkeden oluşan bir sosyal çevre olduğunu düşünmektedir. Alexander Wendt, 500 İngiliz nükleer silahının ABD'ye beş Kuzey Kore nükleer silahından daha az tehdit edici olduğunu açıkladığında gerçekliğin sosyal yapısını gösteren mükemmel bir örnek sunmaktadır (Wendt 1995b).

Ona göre, tarih boyunca genelde olumlu olan ABD ve İngiltere arasındaki sosyal ilişki, ABD ve Kuzey Kore arasındaki bağlantılardan farklıdır. O, nükleer silahları maddi niteliklerinden soyutlamıştır. Amerika Birleşik Devletleri ile İngiltere arasındaki sosyal bağın doğasını anlamaya yardımcı etkileşimler bulunduğunu ve bu durumun fikirlerin ve inançların dünya politikası üzerindeki etkisini kabul etmeyi gerektirdiğini savunmuştur.

Yapılandırmacılık, adından da anlaşılacağı gibi, uluslararası sistemi, aktörler ve yapının doğası arasındaki etkileşimden kaynaklanan sürekli bir inşa süreci olarak değerlendirmektedir. Yapılandırmacılar için dünya her zaman bir konudur. Siber alan, çeşitli sektörlere uygun bir teknolojik ortam yaratarak gayri resmi uluslararası etkileşim için yeni mekanizmalar yaratmıştır. Siber alan, çıkarları ve sorunları ifade etmek, halkı ve kamu işleri ile ilgilenenleri bilgilendirmek özellikleriyle; küresel vatandaş olarak bilinen genişleyen kullanıcı kitlesi ve çoklu iletişim kanalları oluşturma kapasitesiyle küresel meselelerle etkileşime giren birden fazla unsurun doğmasını sağlamıştır (Hacker and van Dijk 2000).

Temel analiz birimi olarak devlet: Yapılandırmacılar, devletin temel analiz birimi olduğu noktasında gerçekçi teori ile hemfikirdir ancak uluslararası örgütler ve sivil toplum örgütleri gibi devlet dışı aktörlerin çıkarlarına yaklaşımları gerçekçilikten/realizmden farklıdır. Ayrıca bu ekölün takipçileri, sistem içindeki birimlerin karşılıklı ilişkilerindeki etkileşimlerinden kaynaklanan bilişsel ve öznel konulara odaklanmaktadır.

1.2.4. Kopenhag Okulu

Soğuk Savaş'ın sona ermesi, uluslararası ilişkiler tarihinde önemli bir dönüm noktası oluşturmuştur. Ülkelerin siyasi, ekonomik ve sosyal yaşamını etkileyen yeni kavram ve algıların ortaya çıkmasına neden olmuştur. Yenidünya düzeninde kullanılan sözcükler, siyaset bilimi ve uluslararası ilişkiler araştırmalarında farklı bir eşik anlamına gelmiştir. Bu tarihten önce egemen olan birçok teori uluslararası fenomenleri ve zorluğu açıklamada yetersiz kalmıştır. Güvenlik çalışmaları, bir önceki dönemde geçerli olan, devletin önemine ve küresel sistem içinde devletin korunması için geleneksel askeri kuvvete odaklanan gerçekçi fikirlerin ve algıların başarısız olmasının bir sonucu olarak, önemli değişikliklere tanıklık eden en önemli alanlardan biriydi. Devletin bölgesel sınırlarının dışından değil devletten kaynaklanan yeni tehditlerin ortaya çıkmıştır. Kopenhag Okulu'nun ortaya attığı en önemli savlardan birisidir. Kopenhag Okulu, Kopenhag Barış Araştırma Enstitüsü ile ilişkili olarak Barry Buzan ve OLE Weaver tarafından yönetilen bir çalışma ve araştırma merkezi haline gelmiştir. Bu okul bir grup araştırmacıyı temsil etmemekte, aksine teorik bir çerçeveyi göstermektedir (Baran and macar 2017).

Kopenhag Okulu Varsayımları:

1. Kopenhag Okulu teorisyenleri, uluslararası ilişkilere konu olan bir hususun, varoluşsal bir tehdit olarak sunulduğunda bir güvenlik sorunu haline geldiğini, bu nedenle derhal istisnai tedbirlerle ele alınması gereken bir tehdit olarak algılanması gerektiğini savunmaktadır. Güvenlikleştirme adı verilen bu terim, belirli bir sorunu siyasallaştırdığı için güvenlik kavramı olarak kullanılmıştır. Ole Waever tarafından ilk kez 1995'te "Securitization and Desecuritization" adlı makalesinde yayınlanmıştır. Bu kavram, Soğuk Savaş'ın sona ermesinden sonra, güvenlik tehditleri ile ilgili tartışmaların genişlemesi sonucu ortaya çıkmıştır. Birçok düşünür, güvenlik fikrini diğer sektörlere genişletmeyi tercih etmiştir. Kopenhag Okulu'nun öncülerinden kabul edilen Weaver, bu kavramın bankacılık sistemlerinden alındığına ve uluslararası ilişkilere aktarıldığına inanmaktadır. Güvenlikleştirmenin halkı belirli bir konuda tehdit edildiğine ikna etmekten kaynaklandığını düşünmektir (Guzzini 2015).

Kopenhag Okulu taraftarları, güvenlik kavramının iki temel unsuru olduğuna inanmaktadır:

Birincisi: Kopenhag Güvenlik Araştırmaları Okulu'nun öncüleri olan "Barry Busan" ve "Ole Weaver", herhangi bir grubu, akımı, dini veya fikri yapıyı, "güvenlik tehdidi" olarak damgalamanın, nesnelliği gerektirmeyen ya da mantıksal bir kanıt sunmanın gerekli olmadığı bir süreç olarak görmektedir. Onlara göre; korku ve kaygı, tartışmayı ve mantığı değil, toplululakları harekete geçirmektedir. Bu nedenle tartışma ve mantığın esas alınmasına gerek yoktur.

İkincisi: Buzan ve Weaver, güvenlik sürecinin bir söylem evresi olduğunu vurgulamaktadır. Bir fikri ya da akımı şeytanlaştırmak ve onu bir "tehdit" olarak tasvir etmek isteyen partinin, bir güvenlik hamlesi yapması gerekir. Bunun için de bir kıvılcımla kalabalıkları ikna edici bir medya rolü buna yeterli olacaktır (Canan-Sokullu 2012)

2- Kopenhag Okulu güvenlik kavramını ve eksenlerini genişletme gerekliliğini benimsemektedir. Güvenlik Teorisi (Sektörel Güvenlik) olarak adlandırılan beş güvenlik sektörüne (askeri, politik, ekonomik, sosyal ve çevresel) ayrılabileceğine inanmaktadır.

Örneğin, siyaset arenasındaki darbeler, siyasi çalkantılar ya da demokrasinin işlevsiz hale getirilmesi, sistem için en önemli tehditler olarak kabul edilmektedir. İktisadi sektör; borçlar, ekonomik krizler, ekonomik abluka ve küreselleşme sorunları, çevre güvenliği açısından en önemli tehditler olarak görülmektedir. Kuraklık bu sektördeki en önemli tehdit faktörlerinden biridir. Burada, devletin hayatta kalması fikrinin askeri aktörlerin tehdidi üzerinde kurulduğu, ancak diğer ekonomik, politik, çevresel ve toplumsal düşüncelerin, askeri unsurla birleştirmenin gerekliliği savunulmaktadır (McDonald 2008).

3- Birey, devlet ve uluslararası sistem Kopenhag Okulu'nda (Baryi Busan) bireyin ve toplumun güvenliğinin, devletin güvenliğine bağlı olduğuna inandığı en önemli analizdir ve iç güvenlikten sorumludur.

Siber Güvenlik ve Kopenhag Okulu Varsayımları:

1. Güvenlikleştirme ve Siber Güvenlik:

Doksanların sonları ve üçüncü binyılın başlarında internet alanında büyük teknolojik gelişmelere tanıklık edilmiştir. Güvenlikleştirme alanında bilgi teknolojisinin geliştirilmesiyle, tehditlerin büyüklüğü ve oranı saptanabilmiştir. Siber güvenlik alanında, devlet ve toplum üzerinde çeşitli yerel, bölgesel ve uluslararası düzeylerde kamu, özel ve devlet sektörlerinde yer alan güvenlik operasyonlarının hedeflediği önemli sektörleri tanımlayarak, devletin yapması gereken politikalar belirlenmiştir (Tajine 2017).

Güvenlikleştirme/seküritizasyon operasyonları, Amerikalı Bilim adamı Harold Laswell'in "Bireylerin veya grupların fikirlerini veya eylemlerini etkileyecek şekilde bazı fikirlerin önceden belirlenmiş amaçlar doğrultusunda ifade edilmesi" şekilde tanımladığı medya propagandasında kullanılan gelişmiş bilgi teknolojisi araçları etrafında şekillenmiştir. (Lasswell 1927).

Alman diktatör Hitler döneminde Alman Propaganda Bakanı Joseph Goebbels bu hususta şöyle demektedir: "Propagandanın temel bir yöntemi yoktur, sadece bir amacı vardır, oda kalabalıkları itaat ettirmektir. Bu amaca hizmet eden her şey iyi bir araçtır." Böylelikle gayenin vesileyi meşru kıldığı ilkesini benimsemektedir. Tarih boyunca etkili olan propaganda, dünyanın global bir köy haline geldiği, tüm bölgeler arasındaki mesafelerin azaldığı bu çağda, önemli bir aktör olmayı sürdürmektedir.

2 - Güvenliğin Alt Kavram ve Sektörlere Bölünmesi:

Hansen ve Nissenbaum karmaşık yapıdaki siber güvenliği, Kopenhag Okulu'nda daha önce belirlenen diğer beş güvenlik sektörünün yanı sıra ayrı bir sektör olarak kavramsallaştırmıştır. Kopenhag Okuluna göre güvenlik kavramı, devlete ve topluma yönelik siber tehditleri teşhis etmek yoluyla dijital çevre ve siber uzayın güvenliği bağlamında da kullanılabilir (Hansen and Nissenbaum 2009).

1.3. Konu: Ulusal Güvenliğin ve Siber Güvenliğin Tanımı ve Boyutları

1.3.1. Ulusal Güvenliğin Boyutları

Ulusal güvenlik, kapsamlı bir kavram olup devletin toprak bütünlüğünü sağlaması ve kazanımlarını düşmanlar karşısında savunması demektir, ayrıca bilimsel ve teknolojik gelişmenin bir sonucu olarak her türlü tehdit ve tehlikeyle yüzleşmek için alınan önlemleri ifade etmektedir. Ulusal güvenlik, askeri konularla sınırlı kalmamaktadır, savaş ve saldırganlık dışında bir dizi ekonomik, kültürel, sosyal, politik önlemleri de içermektedir. Etnik ve sınıf temelli çatışmalar, zayıf gelir dağılımı, sosyal adaletin yokluğu, yoksulluk, siber güvenlik tehditleri ve sınır ötesi bilgi teknolojisi suçları gibi devletin iç istikrarını etkileyen iç tehditler ortaya çıkmıştır. Güvenliğin kapsamlı olması, birbirine bağlı ve birbirini tamamlayıcı özelliklere sahip çeşitli boyutlara sahip olması demektir:

a) Ulusal Güvenliğin Askeri Boyutu:

Askeri güç, silahlı dış saldırganlığa karşı, ülkenin sınırlarını, varlığını, birliğini, huzur ve güvenlik tehditlerini boşa çıkaran ve bunlara karşı caydırıcı rol oynayan güç demektir. Karşılıklı güven eksikliği üzerine kurulan uluslararası ilişkilerin kaotik yapısı, güçlü bir devlet ihtiyacını ortaya koymaktadır. Devlet, istikbal ve bekası için askeri gücüne güvenme ihtiyacı duyar. Bu nedenle ülkeyi dış saldırılardan korumak için askeri stratejik dengenin oluşturulması, uluslararsı düzeyde savunma ve caydırıcılık ihtiyaçlarını karşılayabilecek bir askeri güç inşa etme zorunluluğu vardır. Bu güç oluşumuna, öncelikle toplum, medya ve diğer kapasitelerden yararlanarak hedefe ulaşmak mümkün olacaktır (Sancak 2003).

Çoğu ülkeler, dış politikalarının hedeflerini bölgesel ve küresel çerçevede gerçekleştirmek için askeri gücü esas almaktadır. Dolayısıyla modern ve gelişmiş silahlar edinme zorunluluğuyla yüzleşmek, ulusal bağımsızlık için zorunlu hale gelmiştir. Dünyanın birçok ülkesi, özel şirketler ve teknik uzmanlıklar aracılığıyla ekonomik ve teknolojik atılımlar yaparak yerel askeri endüstrisini geliştirmeye ya da ithalat yoluyla silahlanma konusuna öncelik vermiştir (Paret 1989). Güçlü devletler, halkın özünde taşıdığı vatan sevgisi gibi vatandaşlık değerlerini geliştirerek, güçlerini halklarının

gücünden alırlar. Amerika Birleşik Devletleri'nin ilk kurucuları, iktidarın diğer unsurlarını ihmal etmeden, ilk etapta gerçekçi teoriyi benimseyerek ve askeri gücü artırarak uluslararası ilişkilerde öz-güç/kişisel güç kavramını yerleşik hale getirilmesi üzerinde çalışmalar yapmıştır. Bugün hâlâ sık sık dile getirilen Başkan Ronald Reagan'ın en önemli ifadelerinden biri "güç yoluyla barış" tır. Reagan, bu barışın ülkenin ekonomik ve askeri gücünü yeniden inşa etmek yoluyla ulaşılacak ezici Amerikan kuvvetine bağlı olduğuna inanıyordu.

Barış, seksen yıl önce Theodore Roosevelt geleneğinde stratejik bir kavramdı. Roosevelt ve diğer birçok Amerikalı lider için "barış", çatışmasızlık anlayışından doğmuştur. Amerika'nın menfaat ve idealleri, halkın refahını tamamen kapsamakta, bu ise diplomatik, ideolojik, ekonomik ve askeri dereceleri de içeren "ulusal güç" kavramına dayanmaktadır (Risse-Kappen 1991).

Kimi zaman nükleer silahlar başta olmak üzere, kesin çözümlü caydırıcılık sağlayan askeri güç elde etme ve geliştirme yarışı, "barış" fikri ile açıklanmaktadır. Bir ülkenin, kendisine yönelik herhangi bir askeri saldırı girişimini engelleyebilmesi için silahlanması gerekmektedir. Örneğin, İran ve Kuzey Kore, BM Güvenlik Konseyi kararlarına karşı çıkarak geliştirdiği nükleer programlarını ve balistik silahlarını, ABD'nin kenilerine yönelik düşmanlığını ileri sürerek ulusal güvenliğinin tehdit edildiğine karşılık caydırıcı bir güç olarak savunmaktadır. Bu hususlar ulusal güvenliğin askeri boyutunu ve önemini açıklamaktadır.

b) Ulusal Güvenliğin Siyasi Boyutu:

Ulusal güvenlik kavramı, politikanın en önemli bileşenlerinden biri olduğu için hem iç hem de dış politika ile yakından ilgilidir. İç politika bağlamında, ülkedeki siyasi istikrar ve sistemin biçimi, demokrasi, monarşi, cumhuriyet veya meşruiyet şeklinde olması, ulusal güvenliğinin sağlanmasında büyük rol oynamaktadır (Sarkesian, et al. 2012).

Demokratik rejimler, güvenlik ve istikrarı sağlayan en iyi rejimler olarak kabul edilmektedir. Çünkü etkili politik kurumların kurulmasına izin vermekte ve vatandaşlar arasında siyasi katılım ve eşitliğin genişlemesinin önünü açmaktadır. Böylelik-

le devlet otoritesini tehdit edebilecek güvenlik açıklarını doldurulmasını ve sistemin güçlendirilmesini sağlamaktadır.

Almond'a göre hükümet ile toplum arasındaki ilişki aşağıdaki göstergeler aracılığıyla değerlendirilmektedir:

1- **Çıkarılma Kapasitesi/ Extractive Capability:** Siyasal sistemin, ait olduğu çevresel kaynaklardan yararlanmayı sürdürmesi anlamına gelir.

2- **Düzenleme Kapasitesi/ Regulative Capability:** Siyasi sistemin bireysel ve grup faaliyetleri arasındaki koordinatör rolünü üstlenmesi, yani sosyal davranışı kontrol etme yeteneğidir.

3- **Dağıtım Kapasitesi/ Distribitive Capability:** Sistemin kendisine sağlanan kaynakları farklı gruplar arasında dağıtma kabiliyetidir.

4- **Sembolik Kapasite/ Symbolic Capability:** Sistemin, toplumun değerlerine bağlılığını pekiştirmesi ve vatandaşlar nezdinde bir destek zemini yaratması demektir.

5- **Duyarlılık Kapasitesi/ Responsive Capability:** Siyasi sistemin çevresel taleplere, "modern-yeni girdilere cevap verebilmesidir."

6- **Uluslararası Kapasite/ International Capability:** Siyasi mekanizmanın, diğer siyasi sahalara nüfuz etmesi, hibe, kredi ve teknik yardım sağlayarak onların politikalarını yönetme yeteneğini ortaya koymak anlamına gelir.

Bahsedilen kabiliyetlere sahip olan siyasi sistem, güvenlik, istikrar ve kalkınmayı sağlayabilecek, ülkenin ulusal birliğini koruyacak ve ülkeyi zayıflatan iç savaşlar ile meşgul olmayacaktır. Zayıf yönetim, topluma kötülük getirirken iyi idare, ülkenin ulusal güvenliğini korumak için gerekli ulusal stratejileri belirlemektedir. Stratejik hedeflere ulaşmak için gerekli araçları ve devletin ihtiyaçları karşılama kapasitelerini saptamakta, toplumlara huzur ve refah temin etmektedir. İç istikrarını pekiştirmekte, kitlelerin isteklerini ve desteklerini garanti edecek bireylerin taleplerini uygulamaktadır (Nekola 2006).

Dış boyuta ilişkin şunlar söylenebilir: Dış politika hakkında konuşmak, aslında iç politika hakkında konuşmaktır. Liderler planlar uygulayabilmek için halk desteğine muhtaçtır, dolayısıyla iç politika dış politikanın rotasını belirlemektedir.

Kapsamlı bir ulusal strateji, bölgesel ve küresel ortamda ülkenin ulusal güvenlik gereksinimlerini dikkate alan sabit unsurlara, kurallara ve dayanaklara bağlı olmalıdır (Baggott 2014). Dış politikaya ilişkin entelektüel yaklaşımlara değinen değerlendirmeler, modern bir ulusal güvenlik yaklaşımını vurgulamaktadır.

Ülkenin küresel düzlemde diplomasi kavramını ve kurallarını benimsemesi zorunludur. Ayrıca tehdit ve tehlikelerle yüzleşmeye dayalı bir dış politika formüle etmek için, çevredeki tehditler ve tehlikeler hakkında farkındalık gerekmektedir. Bu noktada diplomasi ve dış politika genellikle karıştırılmaktadır.

Diplomasi, siyasi liderlerin, kendilerine tavsiyede bulunabilecek diplomatlar (sivil ve askeri görevliler ve istihbarat mensupları) aracılığıyla geliştirdiği bir politika aracıdır. Hans Tuch kamu diplomasisini, bir ulusun, kurumlarının ve kültürünün yanı sıra ulusal hedefleri ve politikaları hakkındaki fikir ve ideallerini yabancı temsilcilere aktardığı bir iletişim süreci olarak tanımlamıştır. Diplomasinin amacı, devletin çıkarlarını belirlemek, başkalarıyla ilişkiler kurarak hizmet edilen devleti veya örgütü güçlendirmektir Diplomatlar, temsil ettiği ülkeye karşı iyi niyet oluşturmak ve iş birliği sağlamak amacıyla yabancı ülkeler ve halklarla ilişkilerini geliştirmek için profesyonel olarak çaba göstermek zorundadır (Melissen 2005).

Dış politikanın amacı ise devletin uluslararası arenadaki çıkarlarını gözetmek, ulusal bağımsızlığı, bölgesel güvenliği, siyaseti ve ekonomiyi korumaktır. Liderler, ulusal çıkarları takip ederek politikalarını dış çevredeki koşullar ve teknolojideki değişiklikler ışığında belirlerlemektedir. Politikanın uygulanmasını denetlemek, devlet veya hükümet başkanının, bir kolektif liderliğin veya devlet başkanının görevlilerinin ya da Dışişleri Bakanlığı'nın sorumluluğu olabilmektedir (Cabalza, 2010).

Dış boyut, devletin toprak ve kaynaklarına dair büyük güçlerin ve bölgesel güçlerin isteklerini değerlendirmekle bağlantılıdır. Ülke çıkarlarının diğer aktörlerle siyasi, ekonomik ve sosyal olarak ne ölçüde örtüştüğünü veya çeliştiğini saptamakla

ilgilidir. Siyasi boyut, dışa dönük resmi mekanizmaların öncelikleri ve özel görevlerini tanımlayan bir dizi stratejik ilkeyle yakından bağlantılıdır. Diplomat, öncelikle devletin varlığını korumayı, daha sonra bu devletin uluslararası sistem içindeki durumunu ve gücünü saptayıp yükseltmeyi hedefleyen bir dış politika ile görevini gerçekleştirmektedir.

c) Ulusal Güvenliğin Sosyal Boyutu:

Güvenliğin sosyal boyutu, ülkedeki sosyal yapının doğası ile ilgili her şeyde somutlaşmaktadır. Dini, mezhebi, ya da etnik köken ayırımı yapmaksızın tüm sosyal ve ulusal farklılıkların göz önünde bulundurularak güvenliğinin sağlanması esasına bağlıdır.

Bir ülkede sosyal uyum yaratmak ve toplumu sosyal parçalanmadan korumak, ülke yöneticileri için en önemli stratejilerden biridir. Zira bütünlüğün eksikliği dış müdahaleye izin verip iç güvenliği ve istikrarı tehdit edebilecek karışıklıklar üretebilmekte ve otoriteye karşı çıkan grupların ortaya çıkmasına yol açabilmektedir (Yalçın 2017). Güvenlik sorunları, ülkeye aidiyet ve bağlılık duygusunu artıran politikaların geliştirilmesini ve sosyal adaletin tesisi ile sınıflar ile hizmetler arasında yakın farklar sağlayarak birleşik bir ulusal kimlik oluşturmayı gerektirir. Toplumsal boyut, ulusal iradeyi, ulusal çıkarlar ve hedefleri üzerindeki fikir birliğini desteklemek için temel bir gereklilik olarak, ülkenin tüm bölgelerini kapsayan birleşik bir kimlik oluşturarak ulusal birliğin güçlendirilmesi ile de bağlantılıdır. Bazı araştırmacılar, sosyal faktörleri devletin askeri gücünün önemli bir bileşeni saymaktadır. Ulusal birlik, halkın uyumu, askeri desteği, siyasi liderliğe güvenin ulusal güvenliğe ulaşmada önemli faktörler olduğunu ve devletin ulusal ve uluslararası düzeydeki gücünü hazırlayan fenomenlerden olduğunu düşünmektedir (Waever 2008).

Çağımızda birçok insan kötü ekonomik koşullarının yanı sıra politik ve sosyal koşullarından, kültürel gecikmelerinden ve hızla gelişen teknoloji uygarlığına uyum sağlayamamaktan şikâyet etmektedir. İletişim araçlarının yaygınlaşması sayesinde toplumların dünyanın diğer gelişmiş ve müreffeh halkları ile kıyaslanması, özellikle üçüncü dünya ülkeleri ve Afrika'da olmak üzere şiddete yol açarak siyasi

sistemlerini değiştirmeye başlamıştır. Sudan'da, Pakistan ve Irak'ta etnik, mezhepsel veya aşiret şiddet eylemleri vb. olaylar ortaya çıkmıştır. Bu durum, ülkelerin ulusal güvenliğini istikrarsızlaştırarak onları güçlü ülkelerin müdahalesine karşı savunmasız hale getirmiş ve dünyayı militarizasyona sevk etmiştir (KURT 2015).

d) Ulusal Güvenliğin Ekonomik Boyutu:

Bugünün dünyası, tartışmasız ekonomi dünyası haline gelmiştir. Ekonomik parametlerde üstün olanlar, kelimenin tam anlamıyla iktidarın dizginlerine sahip olmaktadır. Ekonomik güç, devlet gücünün ve ulusal güvenliğin, en az askeri güç kadar etkili ve vazgeçilmez bir unsurudur.

Ekonomi, devleti ayakta tutan kuvvetlerden biridir. Ekonomi politikası ise her iktidarın birincil kaynağıdır. Ekonomi, askeri güçle beraber coğrafik ya da bölgesel yapılar gibi yan kuvvetlerin devletin gücünün oluşmasına katkı sundukları, ekonomik boyutun, ulusal güvenliği inşa etmenin en temel unsurlarından biri olarak kabul edildiği ve ekonomik yapısında zayıflık yaşayan bir ülkenin güvenlik ve sürekliliği garanti edemediği gözlemlenmiştir (B. Moller).

Güçlü ekonomiye sahip bir ulusun iktisadi gücü kaçınılmaz olarak muhalifleri için gizli bir tehdit oluşturmaktadır (Zukrowska 1999). Çünkü ulusal güvenlik ancak iç istikrara yol açan ve kalkınma projeleri, devletin bağımlılıktan uzak tutulmasına yol açan güçlü ve sağlam bir ekonomi ile elde edilebilir. Zayıf bir ekonomi, bu güvenliğe nüfuz edilmesine imkân tanır ve daha sonra devletin temellerine zarar verilir.

"Ekonomik Güvenlik" terimi 1940'larda doğmuştur. Ekonomik güvenlik, ulusal güvenliğin ayrılmaz bir parçasıdır. Bu terim uluslararası ekonomik sistemde farklı ülkelerin ticaret ve ekonomi politikalarının koordineli bir şekilde gerçekleştirilmesinin önemine atıfta bulunmaktadır. Zira uzlaşı eksikliği belirsizliğe ve çatışmalara yol açabilmektedir (Mesjasz 2008).

Uluslararası ilişkilerin yorumlanmasında ekonomik faktörler hakkında konuşmayı ihmal eden teoriler değişmeye başlamıştır. Akademisyenler devletin küresel ve bölgesel sahada konumunu belirlemede ekonominin rolünü teslim etmeye yönel-

miştir. Dünyanın şahit olduğu savaşların ve felaketlerin çoğu öncelikle ekonomik sebeplerden kaynaklanmıştır. Ayrıca ülkeler üzerindeki yaptırımlar ve ticaret kısıtlamaları gibi ekonomik tedbirler, dış politika hedeflerine ulaşmak bağlamında bazen askeri önlemlerden çok daha tesirli olmuştur, Amerika Birleşik Devletleri'nin birçok ülkeyle ilişkisinde bu tespit doğrulanmıştır (Neu and Wolf Jr 1994) .

Ekonomik büyüme ve bilimsel ilerleme; devletin güvenlik çıkarlarını elde etmesinde, stratejik ve caydırıcı bir güç oluşturmasında temel unsurdur. Ticari değişimi geliştirmek, istihdamı ihraç etmek ve teknolojinin, özellikle yüksek teknolojinin transferini sağlamak konusunda bilimsel ilerlemenin ve ekonomik büyümenin rolü inkâr edilemez.

Ayrıca, güçlü bir ekonomiye sahip olan ülkenin, düzenli istikrar ve iç gelişme yarattığı için uluslararası sistemde bir rolü, ağırlığı ve önemi vardır. Ekonomi, Sovyetler Birliği'nin çöküşü ve sosyalist ekonomik sistemin küresel kapitalizme rekabetinin sonlanmasıyla Soğuk Savaş'ın sona ermesi ve Yenidünya Düzeninin doğmasından sonra ülkelerin hayatta kalması ve devam etmesinde önemli bir faktör olarak ortaya çıkmıştır.

Sovyetler Birliği'nin çöküşüne büyük ölçüde, ekonominin zayıflaması neden olmuştur (Kalashnikov 2012).

e) Ulusal Güvenliğin Kültürel Boyutu:

Sosyal mühendislik veya sosyal politika araçlarından olan politik kültür, ulusun hayatta kalması için çok önemlidir. Bundan dolayı ulusal güvenlik kavramı ve genel kültür arasında hayati bir bağlantı vardır. Antropologlar, çalışmalarında bir toplumdaki insanlar üzerinde kültürün önemli bir etkisi olduğunu keşfetmiştir. Çünkü kültür insanın topluma uyum sağlamasına ve böylece hayatta kalma şansını artırmasına yardımcı olmaktadır. Sosyal politikalar, mevcut kültür temelinde geleceğe dair bir geniş görüşlülük sağlamaktadır. Bu nedenle toplumun arzu edilen belirli bir duruma yönlendirilmesi amacıyla geliştirilmiş politikalar olarak tanımlanmaktadır (Oladiran and Adadevoh 2008).

Bir toplumdaki politik sistem, o toplumun kültürü tarafından yaratılır. Demokratik sistemlerde güvenlik ve istikrarın en önemli nedenlerinden biri, insanların çeşitli düzeylerde yetki ve sorumluluk sahibi olarak ülkenin iradesine katılmasıdır. Böyelikle ortaya çıkan sistem, yerel kültür ile uyumlu ve ulusal çıkarları içeren bir ulusal güvenlik stratejisi oluşturulmasını sağlamaktadır (Yeşil 2009). Hiçbir ulusun mutlak güvenliğe ulaşamayacağı bilinmektedir, ancak hayatta kalmayı temin etmek için kültür unsurlarını uyarlamak ve ulusal güvenliğe yönelik beklenen tehditlerle baş etmek gereklidir. Kültürü ulusal güvenlik politikasıyla ilişkilendirme Thucydides ve Sun Tzu'nun yazıları da dâhil olmak üzere klasik eserlerde mevcuttur. 1977'de Jack Snyder, Sovyetler Birliği'nin askeri stratejisini açıklamak üzere stratejik bir kültür teorisini geliştirerek siyasi/politik kültür konusunu modern güvenlik çalışmalarının gündemine sokmuştur. Onun kültür kuramı güvenlik politikası çalışmalarında rasyonel bir aktörün varsayımına meydan okumaya yönelik bir girişim olarak görülmüştür. Çünkü bu kuram, nükleer faaliyetleri dahi salt kültürel unsurlarla anlamlandırmanın mümkün olduğunu ileri sürmüştür (Snyder 1977).

Kültürel kimlik, bir toplumu tarih ve medeniyet özelliklerine göre karakterize eden bir değerler ve algılar sistemidir. Her insan topluluğu diğerlerinden farklı bir kültüre aittir ve farklı kültürel kimliklerden sürekli etkilenen bir yapıdadır.

Arnold Woolfers'ın ifadesiyle her ülkede insanlar edinilmiş değerlere yönelik tehditlerle karşılaşıp tehdidi kişisel değerleri ile ilişkilendirdiğinde ulusal güvenlik kavramını kavramaktadırlar: "Ulusal güvenlik gizemli bir semboldür, farklı insanlara farklı şeyler ifade etmektedir."

Ulusal Güvenlik, nesnel olarak edinilen değerlere yönelik bir tehditin bulunmaması ve bu tür değerlerin saldırıya uğramasından korkulmaması anlamına gelmektedir. Dolayısıyla ulusal güvenliğe ulaşmak, düşünce ve inançları, gelenekleri ve değerleri korumaya bağlıdır (Katzenstein 1996). Kültürel rol, ülkeyi, özellikle küreselleşme ve medeniyetler çatışması aşamasında başka kültürlere dayalı tezlerin etkisinden uzak tutmada son derece önemlidir. Düşünce, kültür, eğitim, medya, sanat ve edebiyat gibi alanlar bakımından ulusal güvenlik, "insanların kendi bağımsız sistemlerinde kendi değer sistemlerini kullanmalarını sağlamak" demektir.

James Rosenaue, evrensel değerlerin yaygınlaştığı, insan ırkının tümü için geçerli olacak şekilde, din ve ırk ayrımı olmaksızın karşılaşılan sorunların beraber çözüleceği bir duruma dair özlem ve isteklere atıf yapmaktadır. Ulusal güvenliğin ana amacının, ulusa mensup insanın değerini korumak ve gözetmek olduğunu söylemek mümkündür.

1.3.2. Siber Güvenliğin Tanımı ve Boyutları:

İnsanlık uluslararası sistemdeki anarşik yapıdan büyük ölçüde zarar görmüştür. Milyonlarca insanın hayatına son veren, binlerce şehrin altyapısını yok eden, onlarca ülkenin ekonomisini tarumar eden ve milyonlarca insanın göçlerle yerinden edilmesine, maalesef acımasız savaşlar yol açmıştır. Bu nedenle devletin sürekliliğini ve hayatta kalmasını sağlamak hayati önem taşımaktadır. Bundan dolayı tarihin her zaman diliminde gerçekçilik, idealizm ve liberalizm teorisi gibi uluslararası sistemin tanık olduğu politik koşulları yansıtan çok sayıda teori ortaya çıkmıştır (Burchill, et al. 2013).

Sanayi devriminin ortaya çıkmasıyla dünyanın şahit olduğu büyük gelişme, bilgi ve iletişim teknolojisi alanında büyük bir ilerlemeye ve hizmet sunumunda önemli bir değişime sebep olmuştur. Daha sonraki teknolojik devrim ile son yıllarda bilgisayar teknolojilerinde baş döndürücü mesafeler katedilmiştir. Bütün ülkelerdeki toplumsal gelişmeler, devlet kurumlarının ve şirketlerin çalışmaları, kurumsal faaliyetler artık bilgi ve iletişim teknolojilerine bağımlı hale gelmiştir. Böylece dijital çağ'a girilmiş olduğu kanıtlanmaktadır. Dijital çağda şu an için en olağanüstü gelişme ise bir takım uygulamalar aracılığıyla yakından ve uzaktan bilgisayarların birbirine bağlanabilme imkânına ulaşmasıdır. İzleme ve denetleme kapasitelerinin geliştirilmesinin yanı sıra bilgisayar ve iletişim cihazlarının hergün yeni bir versiyonla piyasalara çıkması, bu alandaki gelişmelerin hızla sürmekte olduğunu göstermektedir (Reardon and Choucri 2012).

İnternet ağları, bütün dünyada sayısız faaliyetlerle insanlar tarafından bilgi ve fikir alışverişi için kullanılan küresel bir arenaya dönüşmüştür. Bilgisayarlarla en geniş anlamda bilgi depolamak, en karmaşık ve zor işlemleri kolayca yapabilmek, artık birkaç tuşa basmak kadar kolay hale gelmiştir. Siber ağa bağlı sistemler ve ilgili fi-

ziksel altyapılar arasında veri depolamak, değiştirmek ve aktarmak, elektronik ve elektromanyetik devrelerin kullanılmasıyla mümkün hale gelmiştir. Siber uzay fiziksel coğrafyadan bağımsız olarak bilgisayarlar ve iletişimle insanlar arasında bir ara bağlantı aracı olarak görülebilir (BBA. LLB September 2017).

Kanadalı bilim kurgu yazarı William Gibson, siber uzayı tanıttığı ünlü romanında "Neuromancer" siber uzay terimini kullanan ilk kişi olmuştur. Onun tanımı şu şekildedir: Siber uzay, her yerde milyarlarca yasal kullanıcı tarafından yaratılan bir süreçtir (Gibson) .

Siber (cyber) kelimesi, geminin dümenini yönlendiren kişi anlamındaki kybero/steersman kelimesinden geldiği düşünülmektedir. Bu sözcük mecazen hâkim/governor demektir. 1940'larda Amerikalı matematikçi Norbert Wiener, uzaktan kontrol sistemlerini açıkladığı Cybernetics Or Control And Communication İn The Animal And The Machine kitabında canlının aletle iletişimini anlatmak üzere cybernetic/sibernetic kavramını ortaya atmıştır (Wiener 1961).

Elektronik alanın, serbest bir alan olarak herkese açık olduğunu kavrayan bazı ülkeler, elektronik savaşların geleneksel savaşlardan daha ekonomik olduğunu, daha az maliyetle daha etkin rol oynayabildiğini, özellikle ekonomik, teknolojik ve askeri alanlarda rakiplerine önemli zararlar verebildiklerini keşfetmişlerdir. Bu tespit, ülkelerin birbirleriyle ilişkili alanlara (siyasi, ekonomik, cezai vb.) dair bilgi altyapısı ve güvenliklerini korumak için savunma araçları oluşturmasına neden olmuştur. Böylelikle finansal kurumlar, banka ve müşterilerin kayıtlarını tutan hassas devlet kurumlarına yönelik kötü niyetli saldırıları püskürtmek için elektronik sistemler geliştirmek ve tehditlere karşı koymak anlamında "siber güvenlik" terimi doğmuştur. Avrupa Konseyi'nin siber suçlarla ilgili anlaşması ve Birleşmiş Milletler'in bilgisayar suçları hakkındaki kararları gibi siber suçlarla mücadele etme amacıyla çeşitli anlaşmalar ortaya çıkmıştır.

Bilgi Güvenliği İle Siber Güvenliğin Farkı:

1. Bilgi güvenliği terimi, internetin ortaya çıkmasından önce vardı. Kâğıt üzerinde yazılı kayıtlarda ve arşivlerde saklanan bilgilerin güvenliğini sağlamayı anlat-

maktaydı. Bilgisayar ve elektronik arşivleme tekniklerinin kullanımından sonra, elektronik depolama ve arşivleme mekanizmaları, her türlü arşivleme için kapsamlı bir nitelik oluşturmuştur.

2. Siber güvenlik terimi, genellikle bilgi güvenliği terimi ile karıştırılmakta ve yanlışlıkla birbirinin yerine kullanılmaktadır. Ancak siber güvenlik, yalnızca bilgi kaynaklarının korunmasını değil, aynı zamanda diğer varlıkları da içerecek şekilde geleneksel bilgi güvenliğini de kapsamaktadır.

Bilgi güvenliği alanında, insan faktörüne yapılan atıf, genellikle insanların güvenlik sürecindeki rolü ile ilişkilidir. Siber güvenlikte bu faktörün ek bir boyutu vardır. Siber saldırıların potansiyel hedefi olan insanlar siber saldırıya maruz kalırlar. Bu boyutun bir bütün olarak toplum için etik etkileri vardır. Çünkü henüz genç ya da çocuk yaşlardaki bazı savunmasız grupların korunması sosyal bir sorumluluk olarak kabul edilir. Dolayısıyla siber güvenlik bu tür sosyal boyutlara sahiptir (Von Solms and Van Niekerk 2013).

3. Siber güvenlik, "bilgi güvenliği" de dâhil olmak üzere siber ortamda var olan her şeyin güvenliğini sağlarken, bilgi güvenliği alanı ise hem evrak dosyalarında hem de sanal bilgi güvenliği ile ilgilidir.

Aynı zamanda "Bilgi Güvenliği" ile "Siber Güvenlik" terimlerinin iki eş anlamlı sözcük olarak kullanılmamasına dikkat edilmelidir.

Siber güvenlik terimi modern bir terimdir ve evrensel olarak kabul edilmiş kapsamlı başka bir tanımı yoktur. Örneğin Merriam Webster Dictionary siber güvenliği şöyle tanımlamaktadır: Bilgisayar veya ağın yetkisiz erişimlere veya saldırılara karşı korumak için alınan eylemlerdir (Webster, 1 Jun 2018).

Uluslararası Telekomünikasyon Birliği (ITU) tarafından verilen raporda siber güvenliğin tanımı şöyledir: Gruplandırma araçları, politikalar, güvenlik önlemleri, kılavuz ilkeleri, risk yönetimi ve yaklaşımları, eğitim ve diğer uygulamalar gibi bir dizi görevlerle, işletme ve kullanıcı varlıklarını korumak için kullanılabilecek teknolojilerdir (Union, March 2011).

Siber güvenlik, siber uzayda iletişim ve bilgi teknolojilerine ilişkin insan ve finans kaynaklarını korumayı amaçlayan devletin, özel sektördeki kişilerin veya ku-

rumların faaliyeti olarak ortaya çıkan kayıp ve zararların miktarını azaltmakla tanımlanabilir. Ayrıca siber tehditlerin gerçekleşmesi halinde durumun mümkün olan en kısa sürede geriye döndürülmesidir. Böylece üretim tekerleği durmaz ve hasar kalıcı kayıplara dönüşmez (Delaney, 2013)

Siber güvenliğin en kapsamlı ve en kabul gören tanımı ise şöyledir: Bilgi sistemlerinde çalışmaların sürekliliğini sağlamak, kişisel verilerin korunması, gizliliğin güvence altına alınması, bilgi iletişim ve sistemlerinin yetkisiz ve kötüye kullanımını önlemek için kullanılan bir dizi teknik, örgütsel ve idari araçtır. Bunlar vatandaşları ve tüketicileri siber alandaki risklerden korumak için alınan önlemlerdir. Siber güvenlik, hükümetlerin ve bireylerin elinde, özellikle siber savaşın modern savaş taktikleri ve devletlerarası saldırı taktiklerinin ayrılmaz bir parçası haline geldiği için stratejik bir silahtır (Goutam, 2015).

Avrupa Siber Güvenlik Beyannamesine göre şu anlama gelmektedir: "Siber güvenlik, bilgi sisteminin bilgisayar korsanlığı girişimlerine veya verileri hedef alan beklenmedik olaylara direnme kapasitesidir." Neittaanmäki Pekka ve Lehto Martti, Cyber Security: Analytics, Technology and Automation adlı kitabında, siber güvenliğin, bilgisayar korsanlarının saldırılarına ve sonuçlarına karşı savunmada alınmış bir dizi önlem olduğunu ve gerekli karşı önlemlerin uygulanmasını içerdiğini vurgulamaktadır (Lehto ve Neittaanmäki, 2016). Kaliforniya Üniversitesi'nden İletişim Profesörü Richard Kemmerer ise bu çerçevede siber güvenliği; "korsanların teşebbüslerini açığa çıkarıp engelleyecek savunma araçları" olarak tanımlamıştır (Kemmerer, 2003).

Ancak bugünün dünyasında, ister kamu isterse özel, ticari veya kar amacı gütmeyen kuruluşlar, teknik gelişmeye ayak uydurarak, yasal, bilimsel ve güvenlik gereksinimlerine bağlı kalarak, siber alanda beklenen saldırılara karşı önlem almak suretiyle verilerini ve sistemlerini sağlamlaştırmalı ve güvence altına almalıdır.

Teknolojik yeniliklerin ve değişen jeopolitik koşulların sonucu olarak doğan ve Soğuk Savaş sonrası gündeme dayanan bir kavram olan siber güvenlikte saldırı tekniklerinin güvenlik teknolojilerinden daha hızlı gelişmesinden ötürü mutlak başarı

bulmak mümkün değildir. Başka bir deyişle, saldırının kaynağı çoğunlukla bilinmediği ve dış kaynaklı olabileceği için, donanım, yazılım veya diğer bilgi sistemi bileşenleri saldırılara her zaman açıktır. Çünkü siber uzaydaki saldırılar, ulus ötesi suçlardır. Saldırganlar hedeflerine ulaşmak için genellikle güvenlik sistemindeki bir boşluktan yararlanırlar (Czosseck ve Geers, 2009).

Siber Güvenlik Şu Özelliklere Sahiptir:

1- Siyasi uzmanlıkları, güvenlik çalışmalarını, bilgi teknolojilerini vb. konuları içeren disiplinlerarası sosyo-teknik bir doğayı içermektedir.

2- Standartları olmayan bir ağdır, ağdaki aktörlerin kapasiteleri büyük ölçüde birbiriyle benzeştir.

3- Yüksek derecede değişim, birbirine bağlılık ve etkileşim hızından ötürü multidisipliner gruplar içinde internetin standartlardan bağımsız bir ağ olduğu görüşü benimsenmiştir. Bu, tüm bireylerin ve kuruluşların aynı düzeyde riskle karşı karşıya kaldıkları anlamına gelmektedir (Craigen vd, 2014).

Dolayısıyla internet kullanıcıları tarafından kullanılan farklı güvenlik teknikleri, farklı ortamlardaki bireylerin pozisyonu, bunların ülkeler, kuruluşlar veya şirketler olup olmadıkları, ne tür donanım, yazılıma sahip oldukları gibi konular, güvenlik düzeyindeki farklılığa yol açar. Kullanıcılar açıktır, ancak belirsiz ve beklenen tehditler olduğu için güvenlik ve güvensizlik arasında açık bir sınır yoktur. Güvenlik oranı yüzde sıfır ile yüzde 100 arasında değişir. Bu nedenle Siber Güvenlik, göreceli bir kavramdır. Eğer güvenlik bir kullanıcı için mevcut değilse, diğer kullanıcılar için de yoktur. Siber Güvenlik önlemleri, yüksek verimlilikle güncellenmelip yenilenmeli ve açıklar her zaman kapatılmalıdır (Ivanova 2006).

Siber Güvenliğin Temel İlkeleri:

Siber güvenliğin temel amacı, İnternet hizmet kullanıcılarının karşılaştığı zorluklarla ve tehlikelerle yüzleşmek ve siber ortamda güvenlik ve istikrar durumuna ulaşmaktır. Siber güvenliğin ulaşmak istediği, bilgi güvenliğinin temel ilkeleri olarak adlandırılan (CIA'nın Üçlüsü) bir grup hedef vardır. Bunlar:

1- Gizlilik (Privacy): Bilginin gizliliğini ve mahremiyetini korumak: yetkilendirilmiş kişi dışındakilerin bilgilere erişimi engelleyerek ve kullanıcının kimliğini doğrulayarak gizliliği sağlamaktır.
2- Bütünlük/ Sağlamlık (İntegrity): Değişiklikleri ve verilere dokunulmasını önleyerek bilginin bütünlüğünü, geçerliliğini ve homojenliğini korumaktır.
3- Erişilebilirlik: Bilgi ve malzeme akışının sürekliliğini ve hazırlığını sürdürmek ve kimliğini doğruladıktan sonra yetkili kişiye talep üzerine bunları sunmaktır. (Sattarova Feruza ve Kim, 2007).

Siber Güvenliğin Amaç ve Dayanakları:

ABD İç Güvenlik Bakanlığı'nın siber güvenlik konusundaki stratejik vizyonuna göre siber güvenliğe ulaşmak için sağlanması gereken bir dizi hedef ve dayanak vardır, bunların en önemlileri şunlardır:

- **Risklerin Tanımlanması:** Siber güvenlik risklerinin değerlendirmesi yapılarak bu risklerin ulusal siber güvenlikteki gelişmelerini anlamak, risk yönetimi faaliyetlerini takip etmek, önceliklerini tanımlamak ve ulusal siber güvenlik risklerini yeterince yönetmektir.
- **Kırılganlığı Azaltmak:** Federal hükümetin bilgi sistemlerini korumak üzere güvenlik açıklarını azaltarak yeterli düzeyde siber güvenlik için kilit paydaşlarla işbirliği yaparak kritik altyapıyı korumaktır.
- **Tehditleri Azaltmak:** Gelişmiş sınır ötesi suç örgütleri ve siber suçlularla mücadele ederek tehditleri azaltmaktır.
- **Hasarları Azaltmak:** Topluluk düzeyindeki koordineli müdahale çabalarıyla elektronik olaylara etkili bir şekilde yanıt vermek ve büyük siber olayların potansiyelinden kaynaklanan zararı en aza indirmektir.
- **Siber Güvenlik Bağlamında Ulusal Güvenlik Sistemine Olan Güvenin Güçlendirilmesi:** İnternet ve elektronik sistemin güvenilirliğinin artırılması, Küresel siber güvenlik risklerinin daha iyi yönetilmesini sağlayan politikaları ve faaliyetleri desteklemektir (Security, 2018).

Siber Güvenlik Stratejileri:

Güvenlik stratejisi bakımınan siber uzay, en önemli ve stratejik alanlardan biri olarak kabul edilir. Bu alan, her an sızma ve manipülasyon hareketlerine müsait durumdadır. Devletin, hükümetlerin, bakanlıkların, kamu kurum ve kuruluşların verilerine zarar verilmesinin önlenmesi, dünyanın çeşitli ülkelerini ilgilendiren zorluklardan biridir.

Söz konusu fenomenin güçlenmesini önlemek için yoğun çabalar ve işbirliği şarttır. Bu konu, siber zorluklarla yüzleşmek için ülkelerin yol haritasının ana hatlarını çizen ulusal stratejiler geliştirmelerini gerektirmektedir. Böylelikle her ülke siber güvenliğini artırabilir, devletlerin ve uluslararası aktörlerin ulusal çıkarlarını korumak için güvenli bir sanal alan yaratılmasına ve geliştirilmesine katkıda bulunabilir (Luiijf, et al. 2011).

Bahsedilen stratejiler, devlet daireleri, bakanlıklar ve kamu kurumlarını, toplumların temel hak ve değerlerini korumalıdır. Aşağıda siber güvenlik stratejisinin dayanakları sunulmuştur:

1. Siber güvenlik için ulusal bir strateji geliştirmek ve hassas bilgi altyapısını korunması hedeflenmelidir.
2. Hükümetler ile telekomünikasyon ve bilgi endüstrisi toplulukları arasında ulusal iş birliği geliştirilmelidir.
3. Siber suçla mücadele mekanizmaları geliştirerek, kamu ve özel sektörlerde bu tür suçlarla ilgili güvenlik düzeyini yükseltmek amacıyla kurumlar ve bireyler üzerindeki tehlikeler ve yansımalar hakkında farkındalık oluşturulmalıdır.
4. Bilgi suçlarını yönetmek için her ülkede ulusal kapasiteler oluşturulmalıdır.
5. Çeşitli devlet kurumlarıyla işbirliği içinde siber güvenliği ulusal düzeyde güçlendirmeyi amaçlayan özel kurslar ve programlar düzenleyerek ulusal bir siber güvenlik kültürü teşvik edilmelidir. Bunun için Uluslararası düzeyde dernekler, kurumlar, araştırma merkezleri ve üniversitelerin deneyimlerinden faydalanmak, onlarla bilgi alışverişinde bulunmak üzere alanında uzmanlık ve deneyime sahip yetkili kişilerle koordinasyon sağlanması gerekmektedir.

6. Elektronik sistemleri daha güvenli, etkili ve verimli hale getirerek sınır ötesi suçları ve elektronik saldırıları engellemek için siber güvenliği tehdit eden zorluklarla yüzleşebilecek daha modern teknolojilere ve uygulamalara ayak uydurulmalıdır.
7. Bazı kurumların sistemlerinde gelişmeler olmasına rağmen, altyapı ağlarının korsanlığa karşı desteklenmesi gerekmektedir. Elektronik korsanların mekanizmalarının ve yöntemlerinin ilerlemesi nedeniyle siber saldırılara karşı bağışıklığın/direncin sağlanmamasından ötürü tüm kurumların bilgi ve iletişim teknolojisi altyapısını bir plan çerçevesinde inşa ve takviye etmesi gerekmektedir. Her kuruluşun, bilgi güvenliğini sağlamak ve onu riske atacak herhangi bir korsanlıkla mücadele etmek için bir bilgi güvenliği sistemi ve iyi planmış bir politika oluşturulması zaruridir (Fischer 2005).

Siber Güvenliğin Boyutları:

Siber güvenlik, potansiyel siber saldırılara karşı duran ve siber uzayda ulusal güvenliğin korunması için; politik, askeri, ekonomik, hukuk ve sosyal alanlar gibi mecralarda varlığını gösteren bir sistemdir. Siber güvenliğin en önemli boyutları şunlardır:

1- **Askeri Boyut:**

Amerikan askeri gücün desteklenmesi üzere 1969'da kurulan ve bilimsel araştırmalarla ilgilenen üniversite ve kurumları birbiriyle ilişkilendirmeyi ve savaşta bilgi alışverişini sağlamayı amaçlayan "Arbant" projesi bunun bir örneğidir. Pentagon tarafından kabul edilen proje aracılığıyla keşfedilen internet daha sonra 1983'te gelişmiş askeri kuruluşlarla sınırlı bir hizmetken sivil kurumları da içeren bir yapı kazanmıştır. İki bölümden oluşmaktadır. Bu bölümlerden askeri ağ "mil.net" (military networkten) sadece askeri alanda kullanılırken, diğeri ise sivil hat "Arba.net" olarak adlandırılmış ve halkın hizmetine sunulmuştur. Küresel şirketler bu teknolojiyi elde etmek ve yatırım yapmak için yarışmıştır (Naughton 2016). Bu teknolojiyle askeri emirlerin hızlı verilmesi ve iletilmesi, askeri hedefleri uzaktan vurma, yüksek doğrulukla imha etmek yanında askeri birimleri birbirine bağlayan ve bilgi alışveri-

şini kolaylaştıran bir ağ oluşturarak doğru haritalarla hedefleri belirleme kapasitesi hedeflenmiştir. Bu oluşum, ABD silahlı kuvvetleri için bir avantaj sağlamıştır. Bu avantajı korumak, elektronik saldırılara karşı özel bir siber güvenlik sistemi gerektirmiştir. Bu saldırılar tüm devlet kapasitelerini ve istihbarat güçlerini bozabilecek ve askeri veritabanlarını yok edebilecek, mali hasarlar doğurabilecek ve ordu ağlarına yönelik gerçekleştirilecek bir nitelikte olabilmektedir.

Siber savaş, siber suç, siber terörizm ve elektronik/siber koruma alanları, askeri boyuta dâhildir. Bu terimler arasındaki ayrım aşağıdaki şekilde olacaktır:

Siber Savaş: Sistematik savaş bir çatışma alanında saptanan askeri hedeflere ulaşmak için düzenli ordular tarafından, ayarlanan bir zamanda belirli bir ülke veya gruba karşı özel savaş araçlarının kullanımı gibi koşulları içerir. Bu koşullar, askeri olmayan hedeflere görünmez saldırılarla karakterize edilen siber savaşlar için geçerli değildir, bu nedenle siber savaş kavramının net bir tarifini sunmak zordur (Erendor and Tamer 2017).

Tallinn El Kitabı (The Tallinn Manual draws), siber savaşı içermektedir. Siber saldırıyı, "saldırma veya savunma amaçlı olsun, insanlara yaralanma, ölüm, hasar veya yıkımla sonuçlanması beklenen bir elektronik işlem" olarak tanımlamaktadır (Zeadally and Flowers 2014). Siber savaş kavramı, silahlanma, savaş, savunma ve saldırı konuları bağlamında karşılıklı bir çerçevede veya tek taraflı bir siber saldırı başlatılarak devlet ya da devlet dışı aktörlerin hedef alınması şeklinde tanımlanabilen askeri uygulamalarla ilgilidir. Medyada "elektronik savaş" esas olarak iletişim sistemleri, radar ve alarm cihazlarına müdahale vakalarını izlemekle sınırlı eski bir terimken, siber sahadaki veriler, iletişim ağlarını askeri teşkilatların yapısına ve kapsamına sokmaktadır (Adel Abdul - Sadiq 2017).

İletişim/bilişim savaşı terimi, elektronik savaşla aynı anlamda kullanılmaktadır. Bu terim, devletler ve temsilcileri tarafından bilgi teknolojisi ya da bilgisayar sistemlerine karşı planlı bir saldırı olarak tanımlanabilir.

Siber Suç: Bilgi teknolojisinin kullanılmasıyla işlenen bir suçtur (Colarik and Janczewski 2008).

Siber Savaşın Araçları: Siber savaşın en önemli araçları şunlardır:

1- İnsanlar ve insan grupları,
2- İletişim ve bilgi altyapılarını içeren cihazlar ya da sistemler,
3- Uygulanmakta olan programlar.

Bahsedilen program, casusluk operasyonu veya veri çalmak gibi hedeflere ulaşma ve nüfuz etme kapasitesini sağlayacak şekilde yeni, şaşırtıcı ve bilinmeyen bir niteliktedir (Cornish, et al. 2010) .

Siber savaş, stratejik operasyonel merkezlere siber saldırılar yoluyla keşif, komuta, kontrol, iletişim ve istihbarat sistemlerini yıkmayı amaçlayan askeri bir görevdir. Siber saldırıların en önemli örneklerinden biri, İran nükleer programına "Stuxnet" yazılımı ile yapılan ataktır. Bu saldırı, İran'a ait 1000'den fazla santrifüj cihazını yok etmiş ve İran'ın uranyum zenginleştirme sürecini büyük ölçüde geciktirmiştir. Söz konusu operasyon, ABD ve İsrail'e atfedilirken, bazı analistler İran'ın 2012 ve 2013 yıllarında ABD finans kurumlarını kesintiye uğratan ve hizmet dışı bırakan Stuxnet saldırılarına misilleme olarak yaptığına inanmaktadır. ABD ordusunun sahip olduğu üstün saldırı ve savunma kuvvetine rağmen siber uzayda karşılaştığı en büyük zorluk, savunma sistemlerini rakip saldırılarından engelleyecek şekilde etkin kullanma, elektronik saldırıları caydırma ve düşmanın karşılık vermesini önleme kapasitesini işletme biçimidir. Çünkü modern bilgi teknolojisi, casus yazılımlarla askeri ve ticari bilgilerin çalınması riskini artırmaktadır (Lynn 2010).

ABD ordusu, siber alanı, ülkenin Kara Kuvvetleri, Deniz Kuvvetleri ve Hava Kuvvetleri gibi önemli bir birlik olarak görmektedir. İnternet çağında etkin bir strateji ile "Elektronik Caydırıcılık" gerçekleştirmek istemektedir. Bunun için de yumuşak güç ve siber güçle birlikte geleneksel güç kullanımını öngörmektedir. Düşmanın ABD'ye vereceği tepkinin kapsamlı ve maliyetli olabileceği hesaba katılarak elektronik caydırıcılığın amacına ulaşmasını hedeflemektedir. Savunma Bakanı Yardımcısı Robert Work, siber caydırıcılığın siber alanla sınırlı olmaması gerektiğini ve ABD'nin siber saldırılara yanıtlar verebileceğini söylemiştir (Work 2017). İnternet komutanlığına ve Ulusal Güvenlik Ajansı'nın direktörlüğüne aday olan General Paul Nakasone, Senato İstihbarat Komitesine altyapı ağlarına yönelik siber saldırıların Amerikan güvenliğine büyük bir tehdit oluşturduğunu ve ABD askeri güçlerinin sal-

dırıları caydırmak için hayati altyapılarına yönelik her türlü saldırıya yanıt vereceğini belirtmiştir. Konvansiyonel askeri gücün kullanımı hakkında sorulan bir soruyu şu şekilde cevap vermiştir: "Evet, uygun ve etkili bir şekilde tepki verebilmek caydırma stratejisinin önemli bir ayağıdır." (Sulmeyer, 2018.).

ABD ordusunun resmi doktrini, bir siber saldırıya gerekli ve orantılı görülen bir yolla cevap verme hakkının saklı tutulacağını belirtmektedir. 2011 Beyaz Saray Uluslararası Siber Uzay Stratejisi'nin ifadesiyle, ABD "diplomatik, medya, askeri ve ekonomik tüm araçları, uygun ve geçerli uluslararası hukuka uygun olarak" kullanma hakkını saklı tutmaktadır (McKenzie 2017).

Son yıllarda, ABD hükümeti siber savunmanın kurumsallaştırılması yönünde büyük adımlar atmıştır. Bunlar:

- Howard Schmidt, Aralık 2009'da Obama döneminde Siber Güvenlik Koordinatörü olarak atanmıştır.
- Ekim 2010'da İç Güvenlik Bakanlığı ile Savunma Bakanlığı arasındaki resmi iletişim ve ortaklık uygulaması ile sorumlulukları tanımlanmıştır.
- Mayıs 2010'da ABD elektronik komutanlığı kurulmuş ve tüm askeri kurumları birleştirecek şekilde oluşturulmuştur. Bunlar; Siber İletişim Komutanlığı, ABD Deniz Filosu, Elektronik Komuta, Hava Kuvvetleri ve 24. Deniz Piyadeleri Komutanlığı'dır.

Beyaz Saray'daki bürokratik çabalara rağmen, siber uzaydaki tehdidin ve bunun askeri etkilerinin değerlendirilmesi konusunda özellikle Savunma Bakanlığı'nda hala bir fikir birliği sağlanamamıştır (Samaan 2011).

2- Ekonomik Boyut:

İnternetin ve bilgisayarın yayılmasından sonra, ticari operasyonların çoğu bilgisayara bağımlı hale gelmiş yeni bir ticari faaliyet türü ortaya çıkmıştır. E-Ticaret, Bilgisayar sistemleri aracılığıyla ticaret yapmak şekilde tanımlanabilir. Bu kavramı, mal ve hizmetlerin elektronik ortamda üretildiği, dağıtıldığı, pazarlandığı, satıldığı ve alıcıya teslim edildiği bir dizi faaliyet olarak değerlendirmek de mümkündür. Elektronik ticaret, işlemlerin kolaylığı, hızı ve esnekliği nedeniyle eski geleneksel ticaret konseptine etkili bir rakip olmuştur.

Dijital/sanal çekler, dijital/sanal para, bankalar tarafından desteklenen diğer elektronik ödeme yöntemleri gibi ileri teknikler yoluyla ticari işlemlerin temeli haline gelen e-ticaret, satışlarla sınırlı olmayıp, pazarlama faaliyetlerini de kapsamıştır. E-ticaret elektronik ticaret faaliyetlerinin çoğunun internet üzerinden gerçekleştirilmesi sonucu önem kazanmıştır (Brangetto and Aubyn 2015).

Geniş çaplı teknolojik gelişmeyle birlikte ekonomik faaliyetlerin internet üzerinden yürütülmesi sonucu büyük riskler ortaya çıkmıştır. Tüm modern teknolojilerde kötüye kullanımdan kaynaklanan riskler, özellikle elektronik ticaret konusunda ciddi maddi hasarlara neden olmuş, ekonomik faaliyeti olumsuz etkilemiştir. Tüketiciler, tüccarlar ve yatırımcılar arasında güvenli bir siber alanın oluşmasını gerektirmiştir.

Ağ Koruma Mekanizması Oluşturulmasının Nedenleri:

İnternette büyük mali kayıplara yol açan saldırılar görülmektedir: ABD Yeminli Mali Müşavirler Enstitüsü'nün internet sitesindeki bilgilere göre, kimi raporlar ABD şirketlerinin kredi kartı ihlallerinden kaynaklanan zararlarının milyarlarca doları bulan astronomik rakamları aştığını göstermektedir.

Eski Amerikan Başkanı Obama, 2009 yılındaki eserinde, dünya çapında 49 şehirdeki 130 ATM'den milyonlarca dolar çalmak için kredi kartı bilgilerini kullanan hırsızların yarım saat içinde bir elektronik saldırı düzenlediğini ve bunun devasa bir ekonomik etki doğurduğunu vurgulamıştır. Obama, ABD'de bir şirket çalışanının sanal yollarla 400 milyon dolar çalmaktan suçlu bulunduğunu da belirtmiştir. Ona göre küresel düzlemde bilgisayar korsanlarınca fikri mülkiyete dair hakları çalınan şirketlerin zararları 1 trilyon dolara ulaşmıştır (Obama 2009) .

Tahminler ABD ekonomisi üzerinde belirgin bir baskıya yol açan siber saldırıların ekonomik etkisinin büyüklüğünü vurgulamaktadır. Başkan Obama bu bağlamda yeni bir ulusal güvenlik ajansı oluşturmuştur. Bu ajans bağlamında Beyaz Saray'da siber güvenlik koordinatörü tarafından yönetilen ve bir siber saldırı durumunda koordineli yanıt sağlanması için çalışmalar yürütecek bir ofis kurdurmuştur. (Sanger and Markoff 2009).

Siber güvenlik için küresel ekonomik pazarın ayırdığı bütçenin 2020 yılına kadar 177 milyar dolar artarak 9 trilyon dolara kadar çıkacağı tahmin edilmektedir. Ancak siber saldırılar, şirketlere yıllık 500 milyar dolardan fazla sarfiyata mal olmaktadır (Conferences and Limited 2017). Bu gerçekler ışığında siber tehditlerden ötürü siber alanda bir koruma mekanizması kurulmasına ihtiyaç duyulmaktadır. Aşağıda elektronik ticarete dair bir takım saldırı ve risklere yer verdik. Bunlar:

- **Kasıtlı saldırılar/ Intentional attacks:** Bir şirkete ya da organizasyona zarar vermek amacıyla müşterilerin verilerini elde ederek kasıtlı saldırılar gerçekleştirilmesidir.

- **Mahremiyet problemi ile mücadele/ The privacy debate:** Mevcut dönemde, şirketler ile müşterileri arasındaki işlemlerin çoğu, elektronik niteliktedir. Bu nedenle şirket tarafından kullanılan dijital ve elektronik sistemlere herhangi bir şekilde sızılması kesinlikle gizlilik ihlallerine yol açacaktır. Böylelikle şirket, müşterileri önünde güvenilirliğini kaybedecek ve müşterilerinin mahremiyetini koruyamadığı için pazarlama güvenilirliği eksi yönde etkilenecektir (Jarupunphol and Mitchell 2002).

- **Güven kaybı/ Loss of trust:** Burada şirketin müşterisinin/temsilcisinin güvenini yitirmesi durumu mevcuttur. Müşteri/temsilci istediği işlemi tamamlamak üzere şirketin sistemine girmek için Dijital İmza kullanmaktadır. Bu nedenle yanlış kişinin imza kullanarak girmeyi başarması güvenlik problemini doğruracaktır.

- **Transfer Hataları/ Transmission Failures:** İletim hataları, yani, emtia bedelinin ödenmesi sırasında veya alıcının hesabından satıcının hesabına para aktarılması esnasında yaşanabilecek başarısızlık, satın alma ve satış işlemlerini bozacaktır.

- **Belgelendirme Eksikliği/: Lack of Authentication:** Resmi sözleşme mekanizmasının olmayışı demektir: Geleneksel ticarette anlaşmalar genellikle şirket logosunu içeren kâğıtlarla ve resmi daireler önünde yetkili kişiler tarafından imzalanır. Satıcı ile alıcı arasında kişisel ve doğrudan temas yoluyla

onaylanan evrakla belgelenir. Bu konular sanal mecrada neredeyse tamamen kaybolmuştur.

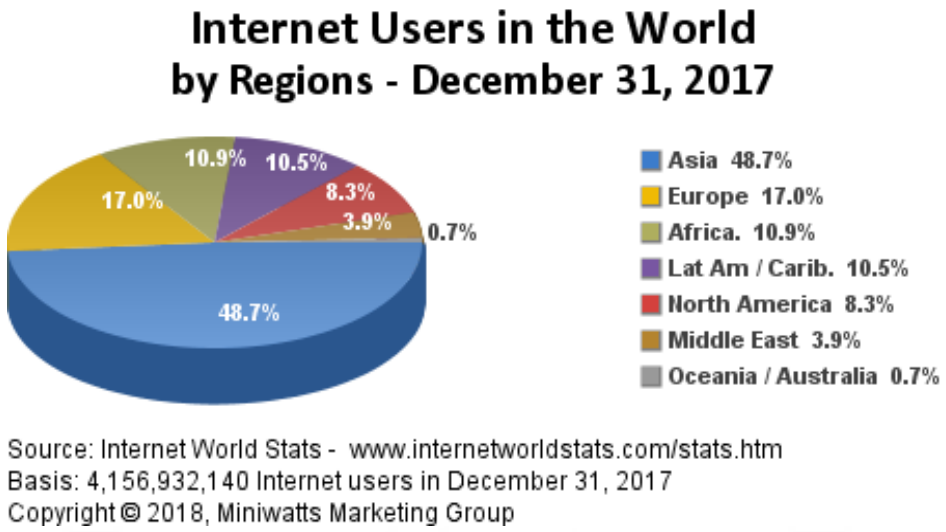
- **Kimlik hırsızlığı/ Theft of Identity:** Müşteri veya vekilin bilgilerine erişerek onun adına bilgisi olmadan alışveriş yapılabilmektedir. Bu durum, müşteri ile şirket arasındaki ilişkiyi sonlandırmaktadır.

- **Gerçeklerin Saptırılması/Window Dressing:** Elektronik ticaretteki ürünlerin çoğu kalitesiz ürünler olabilmektedir. Satılanlar şirketin web sitesinde yayınlananlar dışında olabilmektedir, gerekli özelliklere sahip olmayan sahte ürünler satılabilmektedir.

- **Ekonomik Baskıların Etkileri/ Effects of Economic Pressures:** Elektronik ticaretin hızla büyümesi sonucu pazarlar rekabetçi bir kimlik almıştır. Şirketin gerçek gücünü, muhasebe sisteminin güvenlirliği, önemli güvenilirlik mekanizmalarını oluşturmaktadır. Söz konusu mekanizmaları işleten kuruluşlar bu teknolojik pazarda daha büyük miktardaki sermayelere sahip olmaktadır (Allam 2010).

1- Sosyal Boyut:

İstatistikler, bütün dünya çapında internet kullanıcılarının yüzdesinde büyük bir artış olduğunu göstermektedir. Günümüzde internet üzerinde çeşitli kıtalara dağılmış şekilde 4,15 milyardan fazla kişi bulunmaktadır. Asya kıtası, yaklaşık % 48,7 oranı ile dünyada en çok internet kullanıcısını barındırmaktadır. İnternet kullanımı, dünyadaki birçok toplumun genel sosyal yaşamının ve ekonomik dokusunun ayrılmaz bir parçası haline gelmiştir. Bilimsel teknolojideki gelişmeler, sosyal ve ekonomik alanlarda insanlık tarihindeki en büyük devrime yol açmış, nispeten çok kısa bir sürede ekonomik değişim oluşmuştur. 2000 yılında 400 milyon kişinin eriştiği internet, 2018 yılında 4,15 milyar kullanıcıya varana dek yaklaşık %900 büyümüştür (2018 İstatistikleri). Böylelikle ekonomiye ve toplumlara insanlık tarihinde benzeri görülmemiş bir etki yaratmıştır.



Sosyal medya araçlarının, sosyal, politik, bilimsel, ekonomik ya da kültürel alanlarda yayınlanmış materyallerle olumlu etkiler oluşturabildiklerini, insanların değişik özlemlerini ifade etme fırsatı sunmasında büyük rolü olduğunu unutmamak gerekir. Bazı eğitim ve öğretim programları, gençler arasında aşırılık yanlısı düşüncenin yayılması gibi toplumun değerlerine tehditler oluşturmaktadır (Helfstein 2012).

Dünyaya açılım, sosyal yapı üzerinde önemli değişikliklere ulaşmayı kolaylaştırmakta ve ulusal kimliklerden uzaklaşılabilmektedir. Bu durum, fikirleri ve gelenekleri etkileyebilmektedir. Devletin kamusal yapısı ve sosyal barışı tehlikeye atan tehditlerin giderilmesi için vatandaşın siber güvenliğini sağlamak üzere bu tür risklere karşı bilinçlendirilmesi gerekmektedir. Kültürlendirme hükümetlerin bir görevidir. Sosyal medya, genel olarak toplumun sosyal, güvenlik ve psikolojik durumunu etkileyen söylenti ve haberleri yaymak için kullanılan bir alan haline gelmiştir. Sorunların önlenmesi ve çözülmesi için internet kontrol/sansür sistemi çerçevesinde bu tür meseleleri ele alan bir devlet müdahalesi zorunludur (Liu, et al. 2014).

Dünya çapında genel ve ortak bir kültürün benimsenmesi anlamına gelen küreselleşme fikrinin yaygınlaşmasıyla birlikte internet, yerel söylemleri sınır ötesi ve kıtalararası söylemlere dönüştüren “global” (küresel) kavramın desteklenmesi için bir araç olarak kullanılmaktadır. İnternetin belirli amaçlar doğrultusunda kullanımı, ulusal kültürlerin erozyonuna ve küreselleşme kültürü lehine zayıflamasına yol açmaktadır. Batı veya Amerikan medeniyeti küreselleşme fikrinin kaynağını teşkil et-

mektedir. Üçüncü dünya ülkelerinde kültürel işgal olarak nitelendirilen bu olguya karşı ilgili ülkelerin yöneticileri, toplum üyeleri tarafından atalarından gelen miras ve gelenekleri muhafaza edebilecek bir siber güvenlik sistemi hazırlamayı değerlendirmektedir (mahiroğulları 2005).

2- Siyasi Boyut

Siber güvenliğin siyasi boyutu, sanal dünyada tanık olunan muazzam teknolojik ilerlemelerden ötürü en etkin boyutlardan biri olarak kabul edilmektedir. Süper güçlerdeki politik rejimlerin geleceğini etkileyebilmektedir. Amerikan seçimlerine Rus müdahalesinden sonra Amerikan demokratik sisteminin siyasî güvenirliliği konusunda şüphe ile karşılaşılmıştır (Persily 2017). Arap baharında da sanal alan büyük rol oynamış, devrime yol açan sürecin ilk günlerinde Mısır hükümeti, Mısırlıların sosyal ağ sitelerinin kullanımına devam etmesinin önemini anlayarak telekomünikasyon ve internet hizmetlerini kesmeye çalışmıştır (Abbott 2012).

Siber güvenliğin siyasal boyutuna dikkat çeken birçok konu vardır. Özellikle de seçim kampanyalarını organize etmek ve parti programlarını yaymak, politik farkındalık sağlamak, birçok politik gerçeklerin ortaya çıkması (WikiLeaks örneği) gibi konularda sosyal medyanın değişik rolleri olmuştur. Siyasi yönelimler, devletlerin ilişkilerini etkilemiştir. Bu durum, devletlerin dış politikalarına sızan haberler doğrultusunda, politikalarını yeniden gözden geçirmeye zorlamıştır. Bilgi ve belge korsanlığına ve büyük miktarlarda sırların toplanmasına dayanan ve hükümetlerin erişemeyeceği bir yerde Wikileaks benzer siteler yaratılmıştır. Küresel düzeyde, özellikle de Irak savaşıyla ilgili bilgiler açığa çıkarılıp yayınlanmış ve piyasaya sürülmüştür (Burns and Somaiya 2010).

Siyasi içerikli saldırılar, özellikle fikirlerini yaymaya çalışan aşırı milliyetçi gruplar tarafından ortaya çıkarılmaktadır. Bu grupların kullanılması ve finanse edilmesi yanında siyasi, askeri, dini bloklar ve örgütler oluşturulması için sosyal medyadan yararlanılması, güvenlik ve istikrarı tehdit etmektedir. Politik kargaşa ve siyasi düşmanları karalamak amacıyla birbirleriyle yarışan blokların başvurduğu sanal saldırılar bulunmaktadır. Sosyal paylaşım siteleri ve internet aracılığıyla destekçilerin belirli bir yöne ya da bir kampanyaya yönlendirilmesinin yanı sıra hükümet karşıtı gösteriler ve her türlü eleştiri ve protestolarla hükümetin halkça değerlendirilmesi de

gerçekleştirilmektedir. Siber güvenliğin politika ile ilgili boyutunu, yasalara veya kamu belgelerine karşı protesto ve eylemler, fiziksel şiddete yönelme gibi sosyal ya da siyasal girişimler, hükümetin uygulamarını belirlemektedir (Gandhi, et al. 2011).

3- Yasal (Hukuki) Boyut:

Dijital çağ, bilişim teknolojileri hizmetlerinin ve tesislerin kullanılabilirliği ve hayattaki her şeyin internet ile bağlantılı olması açısından insanlar için refah dönemi olarak görülmektedir. Şu an internete bağlı 25 milyar cihaz vardır ve bu miktar, 2021 yılına kadar ikiye katlanarak 50 milyara yükselecektir. Dijital veri hacmi şu anda her 18 ila 24 ayda bir, iki kata çıkmaktadır. Yeni gelişmeler, günlük hayatımızda ev sağlık hizmetlerinden ulaşım ve sigortaya kadar her alanda tüketici olan insana büyük faydalar sağlayacaktır. Gelecekte ise tahmin edilemeyen faydaları olacaktır. Bağlı cihazlar tarafından oluşturulan ve kullanılan verilerin çoğunun kişisel olması büyük bir problemdir. Verilerin değişimi ve işlenmesi ile özel bilgilerin yayılması ve şahsi hayatın güvenliği hakkında sorunlar yaşanmaktadır. Bu durum nesnelerin interneti ile ilgili yasal konuların merkezinde yer almaktadır (Kemp 2017).

Hukuk ve teknoloji arasındaki ilişki karşılıklı bir ilişkidir. Teknik gelişmeler ve onların uygulanmasından kaynaklanan hukuki konular doğrultusunda yasal mevzuatın uyarlanmasını gerekmektedir. Siber uzay içinde faaliyet gösteren internet teknolojileri sınır ötesi nitelikte olduğundan, siber suçlar, yargı ve uyuşmazlık sorunlarının çözümünü sınırlamak için yasal çerçeveler ve mevzuat hazırlanmalıdır. İnternetin hayata geçmesiyle bu bağlamda çeşitli zorluklarla karşılaşılmıştır.

- Belli bir zaman ve mekâna bağlı olmaması sebebiyle ölçümü zor olan siber suçların doğasından ve özelliklerinden kaynaklanan zorluklar bulunmaktadır. Bu tür suçlara dair yeni yasalar çıkarmak için teknolojik gelişmeler doğrultusunda mevzuat ve yasalar yönlendirilmeli ve güncellenmelidir.
- Bağlantı kurmanın ve suçu belirli bir kişiye veya uluslararası aktöre tahsis etmenin zorluğu: Suçların faillerinin tespit edilmesi güçtür. Dolayısıyla suçların faillerini tespit etmek için en son tekniklerin aktif bir şekilde uygulanması gerekmektedir.
- Siber suçlar, ülkelerin siber uzayda güvenliği sağlamak için önlemler almalarını zorunlu kılmaktadır. Bu da uluslararası işbirliği ve anlaşmalarının

devreye sokulmasını zaruri hale getirmektedir. Zira ülke, sınırları ile kısıtlanabilecek bir yapıda değildir (Shinder 2011).

Siber güvenlik ile ilgili farklı devletlerde bazı kanunlar tamamlanmıştır. 2015'in sonlarında Amerika Birleşik Devletleri'nde elektronik emniyete dair bir düzenleme yapılmış, yıllarca süren teşebbüslerden sonra kongrece şirketlerin federal hükümet ve diğer şirketlerle siber güvenlik tehditleri (hacker girişimleri gibi) hakkında bir kanun çıkarılmıştır. "Siber Güvenlik Yasası 2015" başlıklı tasarı, Evrensel Harcamalar Kanunu, Bilgi Paylaşım Hükümleri adı altında yer almıştır. Siber Güvenlik Yasası'nın Evrensel Harcamalar Yasası'nın N bölümünde 136 sayfa tutmuştur. Özel şebeke operatörlerinin kendilerini savunmaları, potansiyel tehditleri izlemeleri ve federal hükümetle iş birliği yapma kurallarını detaylandırmaktadır. Yeni yasa, DHS'nin/İç Güvenlik Bakanlığı'nın siber alandaki çabalarını da desteklemektedir (Rosenzweig 2015).

Kamu ve Özel Sektör iş birliğinin önündeki engelleri ele almaya dair Siber Güvenlik Yasası'nın birçok hükümleri arasında özel kuruluşlara aşağıdaki konularda yetki veren maddeler bulunmaktadır:

- ✓ Siber güvenlik için bilgi sistemlerinin gözetimi.
- ✓ Siber güvenlik amacıyla "savunma önlemlerinin" işletilmesi.
- ✓ Siber tehdit göstergeleri veya savunma önlemleri hakkında bilgi alışverişi.

Amerika Birleşik Devletleri'nde tek bir "siber güvenlik" yasası yoktur. Amerika Birleşik Devletleri, yüzlerce federal ve eyalet kanunu, mahkemelerdeki veri güvenliği, mahremiyet ve "siber güvenlik" çatısı altındaki diğer yaygın problemler bağlamında kurucu ve zorlayıcı düzenlemeleri ve kuralları bir araya getirmektedir.

Bu siber güvenlik karışımı, hukuk alanlarında altı geniş çaplı yasadan oluşmaktadır:

- ✓ Özel sektör veri güvenliği yasaları
- ✓ Korsanlıkla mücadele yasaları
- ✓ Siber güvenlik için kamu ve özel güvenlik çalışmaları
- ✓ Hükümet kontrol yasaları

- ✓ Devletle sözleşme yapanlar için siber güvenlik gereksinimleri
- ✓ Gizlilik Yasası

ABD şirketlerinin başka ülkelerde temsilci veya çalışanı varsa, bu kişilerin de verilerinin korunması ve güvenliği için o ülkedeki cari yasaları ve düzenlemeleri dikkate almaları gerekir (Mirasola 2016).

Çin'de bilgisayar virüslerini önlemek ve bilgi güvenliğinin hiyerarşik biçimde korunmasını sağlamak için idari önlemler alınmasını içeren, bazı yasalar, kurallar ve düzenlemeler mevcuttur. Bununla birlikte, Çin'in giderek siber güvenliğe odaklandığını gösterecek şekilde bir siber güvenlik mevzuatı başlatılmıştır. Hukuki altyapısı ve yasama çalışmalarının bir yıl sürdüğü mevzuat ulusal güvenliği sağlama hedefiyle, Kasım 2016'da Ulusal Halk Meclisi (NPC) tarafından kabul edilmiş, 1 Haziran 2017'de ise yürürlüğe girmiştir.

Söz konusu kanun hakkında şunları söylemek mümkündür: Bölgesel huzurun, sosyoekonomik istikrarın ve kamu düzeninin gerçekleştirilmesini hedefleyen bir yasadır. Kuruluş ve işletmelerin, hangi şartlarda sistemlerini Çin dışına taşıyabileceğine dair dijital bilgileri saklama ve kollama yollarını belirlemektedir. Ayrıca internet sistemlerini, ürünleri ve hizmetlerini siber saldırılara karşı korumayı amaçlayan çeşitli önlemler de sağlamaktadır (Lindsay, et al. 2015).

Birinci Bölümün Özeti:

Bu bölümde tez çalışmamızın konusu çerçevesinde bazı temel kavramların tanımına yer verilmiştir. Bunlar: Ulusal güvenlik çerçevesinde siber güvenliğin önemini, boyutlarını ve temel etkenlerini belirleme hedefi çerçevesinde ele alınan ulusal güvenlik ve siber güvenlik kavramlarıdır. Çalışmada, ulusal güvenlik kavramının, Batı Amerika menşeli olduğu ve siyasi amaçlarla ortaya çıktığına vurgu yapılmıştır. Nitekim güçsüz ülkelerde istikrarsızlık ve güvensizlik tezahürlerinin eşlik ettiği Soğuk Savaş ve uluslararası kutuplaşma döneminde, büyük güçlerin dış politikalarının odağı olarak ortaya çıkması, dünyanın çeşitli ülkelerinde ulusal güvenliğe ilginin artmasına neden olmuştur. Bu durum ise milli güvenliğin siyaset biliminde yeni bir dal haline gelmesini, farklı teorilerin ve okulların ortaya çıkmasını beraberinde ge-

tirmiştir. Çalışma, ulusal güvenliği farklı açılardan (askeri, ekonomik, toplumsal vb.), iç ve dış düzeyde (bölgesel ve küresel) ulusal güvenliğin farklı yönlerini incelemeyi gerekli kılmıştır. Bu bölümde ele alınan düzeyler arasındaki ilişki, konuların birbiriyle bağlantısının önemini ortaya koymaktadır. Örneğin, ulusal güvenlik kavramı ile diğer benzer kavramları birbirinden ayırmanın yanı sıra, ulusal güvenlik ile güç faktörleri ve tehdit faktörleri incelenerek ulusal güvenliğin önemi ortaya konulmuştur.

Çalışmada, ulusal güvelik kavramını sadece askeri boyutu ile yetinmeyerek mevcut toplumsal koşullara göre değişiklik ve gelişmeyi kabul eden analitik bir mantığa göre güvenlik kavramının farklı boyutlarını (askeri ve askeri olmayan, dış ve iç) içeren geniş bir ulusal güvenlik kavramı olarak işlemeyi ön görmüştür. Araştırmada Ulusal güvenlik kavramının boyutları ele alınırken modern ve metodolojik gelişmeye ayak uydurulması gerektiğine vurgu yapılmış ve ulusal güvenlik olgusunda yeni değişkenlerin özümsenmesinin altı çizilmiştir.İkinci kısımda ise gerçekçi teori, liberal teori, yapılandırma teorisi, Kopenhag Okulu ve ulusal güvenlik konularıyla ilgili uluslararası ilişkilerdeki en önemli düşünce okullarına değinilerek açıklığa kavuşturulmuştur.Üçüncü kısım da ise siber güvenlik kavramının tanımı, boyutları, temelleriyle diğer sektörler arasına eklenecek yeni bir sektör olarak önemi ele alınmıştır.

İKİNCİ BÖLÜM

2. ULUSAL GÜVENLİK VE SİBER TEHDİTLER

2.1. Siber Tehditlerin Karakteristik Özellikleri ve Bunların Küresel Güvenlik Üzerindeki Etkileri:

Dünyanın bilgi ve iletişim teknolojisi bağlamında siber uzay adı verilen sanal bir alanda tanık olduğu devrim ile birlikte küresel güvenlik konusunda çeşitli sivil ve askeri sektörleri içeren yeni tehdit modelleri ortaya çıkmıştır. Ülkeler ve diğer aktörlerin siber uzayda büyük etki ve güce sahip olmaları yeni bir çatışma sahasını ortaya çıkarmıştır. Devletlerarasında gerek saldırı gerekse savunma arasındaki rekabet diğer uluslararası aktörlerin askeri, ekonomik ve hatta sosyal hedeflerine saldırmak için kullanılan casus programların ve virüslerin geliştirilmesine dayanan bir siber silahlanma yarışını tetiklemiştir (Craig and Valeriano 2016).

Teknolojik gelişmeler ışığında küresel güvenlik, ekonomik, sosyal, politik, askeri vb. tüm sektörleri kapsayacak şekilde geniş etki alanları ile karakterize edilen çok sayıda tür ve biçimdeki tehditle karşı karşıya kalacaktır. Çağımızda güvenlik tehditlerinin en önemlisi, en yeni, en ciddi, en yaygın ve en etkili olanı siberuzayla ilişkili Siber elektronik tehditlerdir. Özellikle form ve kaynaklarının değişikliği, hızlı ve sürekli gelişimi, onları tamamen çözmek için karmaşık stratejiler belirlemeyi, hazırlamayı zorunlu hale getirmiştir (Limnéll 2016).

Modern çağda teknolojik mekanizmaların gelişimi ışığında elektronik tehditler, çeşitli alanlarda küresel güvenliğin karşılaştığı geleneksel güvenlik tehditlerinden daha az tehlikeli hale gelmemiştir. Bu nedenle, her ülke güvenlik ve savunma politikalarında bu tehditlere karşı koymak için özel bir strateji geliştirmelidir (Akyeşilmen 2016a). Siber güvenlik alanındaki büyük teknolojik gelişmeye ayak uydurmak amacıyla özellikle zamansal, mekânsal ve çevresel koşulların etkilerin ortadan kalkmasından ve siber saldırıların beklenmedik yerde ve çok kısa sürede gerçekleştirilmesinden sonra, devasa bütçeler ve finansal kaynaklar tahsis edilmiştir. Güç dengesi değişmiş, stratejik avantaj ve kapasite artık sadece coğrafi konum ve savaş kapasite-

lerine bağlı olmaktan çıkmış, ileri düzeyde teknoloji edinmeye ve bilgi teknolojilerini dahada geliştirmeye bağlanmıştır. Dolayısıyla siber tehditlere karşı etkili koruma sağlamak için uluslararası işbirliği ve istihbarat paylaşımı, en önemli gereksinimlerden biri olarak kabul edilmiştir (Mastapeter 2008).

Siber tehditlerin kaynakları çoğunlukla organize suçlular, teröristler ve bilgisayar yazılımı ve internet kullanımında uzmanlaşan aşırılık yanlısı gruplardır. Bu nedenle, siber saldırılara karşı önleme becerileri geliştirme ve savunma araçları geliştirme ihtiyacı, özellikle siber saldırıların daha sık, daha organize ve karmaşık hale gelebileceği ve bunlardan kaynaklanan ekonomik hasarın daha yüksek olacağı netleştikten sonra, birçok ülke için güvenlik politikalarının en önemli ilkeleri arasında yer almıştır. Mali hasarın büyük olması, hükümete yönetim, iş dünyası, ekonomi, ulaşım ve tedarik açısından zarar verecektir. Siber saldırılar, tüm dünyada ulusal refahı, güvenliği ve barışı tehdit eden düzeylere ulaşabilir (Clapper 2011).

Siber uzayda güvenlik riskleri, modern çağda artan zorluklarla birlikte çoğalmaktadır. Ayrıca, siber güvenlik 21. yüzyılda uluslararası ilişkileri büyük ölçüde uluslararası düzeyde etkilerken, problemler de önemli ölçüde artacaktır (Kundu 2018).

Bilgi güvenliği alanında uluslararası sistemde aktörlerin karşılaştığı en önemli sorun, bilgi tehditlerinin doğasını ve yıkıcı potansiyelini tanımlamaktır. Kraliyet Uluslararası İlişkiler Enstitüsü'nden (Chatham House) P. Cornish, bilgi güvenliğine yönelik tehditlerin bir sınıflandırmasını vermektedir. Bunların bazıları şunlardır:

- Bireysel bilgisayar korsanlarının faaliyetleri,
- İnternette işlenen organize suçlar,
- İdeolojik ve politik aşırılık,
- Ülke ile ilgili bilgilere karşı saldırganlık (Paul Cornish 2009)

Savunma Merkezi uzmanları, internetin militarizasyonunun/askerileşmesinin siber alanın gelişimindeki en önemli ve tehlikeli küresel eyilimlerden biri olduğuna inanmakta ve modern askeri sistemlerde bilgi teknolojisini, gelecekteki çatışmalarda paralel bir savaş taktiği olarak kullanmaya hazır olduklarını söylemektedir. Aynı za-

manda NATO savunma merkezi, siber uzayda yeteneklere dayalı bir siber saldırının bağımsız bir biçimde gerçekleşmesinin pek mümkün olmadığından, siber savaş için "konvansiyonel savaştan ayrı olamayacağından eminiz"der. Ancak tahminler, siber alandaki agresif eylemlerin, gelecekte geleneksel saldırı silahlarına ilave edilerek operasyonların etkisini arttırmak için kullanılması olasılığını göstermektedir. Yani, geleneksel silahlara ek olarak siber silahların kullanılması, gelecekteki çatışmalarda standart operasyolara, stratejik dijital savaş araçlarının ekleneceği öngörülmektedir (Gomez 2016).

Günümüzde bilgi ve iletişim teknolojisinin hızla gelişmesi uluslararası ilişkiler üzerinde ciddi bir etkiye sahiptir. Bu teknolojilere sadece bilgi alışverişi ve işleme aracı olarak değil, aynı zamanda son yıllarda olduğu gibi zarar ve imha aracı olarak da başvurulmaktadır. İnternet ve siber alanlarla ilgili terimler uluslararası politik söylemde yaygın olarak kullanılmaktadır. Bunlar sadece ülkelerin stratejik teorilerine değil, NATO da dâhil olmak üzere uluslararası örgütlere de yansımaktadır (köse 2017).

Elektronik tehditlerin insanlara doğrudan zarar vermesi değil, yaşamlarının önemli bir bileşeni haline gelen siber alanı etkilemesi amaçlandığı gözlemlenmektedir. Bireylerin kullandığı ve bağlı olduğu sistemleri, ağları ve cihazları tesiri altına almak ve böylece yaşam biçimini bir bütün olarak devletin güvenliğini tehdit edecek şekilde etkilemek hedeflenmektedir. Ancak öldürme için kullanılabilecek konvansiyonel silahlarda olduğu gibi insanlara doğrudan yönelik değildir.

Siber tehditler güvenlik görevlileri için büyük bir zorluk teşkil etmektedir, Bugün, birden fazla cephede tehditlerle başa çıkmak zorunda kalmaktadır ve bu durum dış alanı genişletmekte ve derinleştirmektedir. FBI, her gün 4.000'den fazla siber saldırı gerçekleştiğini bildirirken, diğer araştırma kaynakları her gün 230.000 yeni kötü amaçlı yazılım örneği üretildiğini söylemektedir (Hai 2018)

Son yıllarda yaşanan kötü saldırılar siber güvenliği birçok şirket, ülke ve uluslararası organizasyonda gündemin zirvesine taşımış ve utanç düzeyini yeni boyutlara yükseltti. Sonuç olarak, küresel siber güvenlik harcamaları 2017 yılında herhangi bir

azalma belirtisi olmadan 86,4 milyar dolara ulaştı. Aksine, güvenlik duvarları ve antivirüs programları gibi geleneksel güvenlik önlemleri yetersiz olduğundan, virüsler ve ağları hedef alan erken solucanlar daha güçlü ve sorunlu bir hale geldiğinden, 2018 yılında siber güvenlik sektöründeki harcamalar 93 milyar dolara ulaştı. Siber uzaydaki uluslararası aktörleri, siber tehditler hakkındaki bilgilerini artırarak ağlarını içeriden korumak için yeni araçlar, taktikler ve süreçler kullanmaya ve benimsemeye zorluyorlar (Radanliev 2018).

Bilgisayar korsanları daha karmaşık deneyimler kazandıkça, mevcut güvenlik kontrolleri onlara eşlik etmede yetersiz kalacaktır. Güvenlik personelinin azlığı ve onlara duyulan ihtiyaç, durumu daha da kötüleştirmektedir. Önümüzdeki yıllarda e-güvenlik alanıyla ilgili ihtiyaç büyük ölçüde artacaktır.

2.1.1. Siber Tehditlerin Değişen Güç, Savaş ve Barış Algıları Üzerindeki Etkisi:

1. İktidar kavramındaki değişim: Teknolojik gelişmeler geleneksel iktidar biçimlerini değiştirmiş ve daha önce var olmayan yeni kavramlar getirmiştir. Siber güç, yeni bir güç türü ortaya çıkmıştır. Şu anda bu terimin resmi bir tanımı olmamasına rağmen, ABD Savunma Bakanlığı'nın askeri terimler sözlüğü bu bağlamda bazı ilgili kavramlar sunmuştur. Bu kavramlar yoluyla sözlükte siber kuvvetin siber alanda operasyonlar yürüten kişiler tarafından oluşturulabileceğini ve faaliyetlerinin saldırı, savunma ve açıklardan yararlanma içeren bilgisayar ağı operasyonlarını içerdiğine işaret edilmiştir. Siber Güç, siber savaş ve güvenliğe ayrılmış bir askeri bölümdür. Sorumlulukları siber terörle mücadele operasyonlarını da içerebilir. Siber güç askeri bir birimin parçası veya ortak bir komuta içinde olabilir (Paul 2014). Ayrıca ister yumuşak ister sert nitelikli olsun, geleneksel güç biçimleriyle birlikte çalışmasından dolayı devletler için sadece dış politika değil aynı zamanda iç politika bakımından en önemli araçlardan biri haline gelmiştir.

Joseph Nye bunu "bilgi alanına elektronik olarak bağlı bilgi kaynaklarının kullanımı yoluyla istenen sonuçları elde etme yeteneği" olarak tanımlamaktadır (Nye Jr 2010).

Siber gücün başka bir tanımı daha vardır: “Failin (çok uluslu şirketler, uluslararası örgütler, terörist hareketler, suç örgütleri, bireyler ve diğerleri gibi bir devlet ya da devlet dışı aktörler) bilgisayar ağlarında ve internette belirli hedeflere ulaşmak için modern teknoloji ve iletişim kullanma yeteneği.” Bu güç önemli verilerin çalınması, imhası veya değiştirilmesi, elektronik sistemlerin kapatılması veya sıfırlanmasını içerebilmektedir (Rogan 2006).

Günümüzde ülkeler ve diğer uluslararası aktörler tarafından siber saldırı tehlikesini fark edildikten sonra teknolojik kapasitelerin hızla ilerlemesi göz önüne alınarak yeni stratejiler geliştirme ihtiyacı ortaya çıkmıştır. Stratejiler, güç, caydırıcılık ve savaş hesaplamalarının farklılaştığı dijital çağa internetin kişisel, kamusal, askeri, siyasi, ekonomik veya sosyal olmak üzere tüm etkileşimlerini yöneten genel çerçeve olduğu döneme uymalıdır.

Devlet genellikle dış hedeflerine ulaşma kapasitelerini, en önemlisi “diplomasi, askeri güç, propaganda ve ekonomik araçlar” olan çeşitli araçlarla gerçekleştirmektedir. Ancak modern çağımızda küresel realitenin dayattığı teknik ilerlemeler bağlantılı yeni faktörlerin girmesi neticesinde geleneksel faktörler artık ülkenin gücü üzerindeki ana etkenler olma kapasitesini yitirmiştir. Güç modelleri zaman zaman değişebilmektedir. Özellikle devletin kendisini uluslararası bir güç olarak ortaya koymasında, gücünün de açık bir zayıflığa indirgenmesinde temel kriterin onun seçimi olmadığı, daha ziyade çevredeki uluslararası koşullara tabi olduğu realitede bu durum daha net bir şekilde gözlemlenmektedir. Güç modelleri, ülkelerin modern bilimsel, teknolojik ve medya altyapılarına göre farklılık göstermektedir. Uluslararası ilişkiler alanında, maddi güç kaynakları ve biçimlerinin her zaman değiştiği bir norm haline gelmiştir (Petreski 2015).

Sert/kaba güç (hard power) denilen maddi askeri ve ekonomik kapasitelere dayanan geleneksel askeri güç, maddi olmayan boyutların da kullanıldığı devletin dış politikasını tek başına yönlendirme olanağına sahip değildir. Bu nedenle, ikna etme yeteneğine ve hükümet modelinin çekiciliğine bağlı olan yumuşak gücün önemi ortaya çıkmıştır. Siber alanda bilgi teknolojisinin sürekli gelişmesi ile yaşanan bilgi devrimi yeni bir tür gücü oluşturmuştur. Bu da Siber güç’tür.

Siber güç, özellikle siber saldırıların düşük maliyeti ve kapsamlarının devlet sınırları dışında genişlemesi ve ekonomik alandaki somut etkisinin gücü benzeri avantajlarının bilinmesinin ardından yerel ve uluslararası güç dengelerini değiştirmede büyük rol oynamıştır. Bu durum genç aktörlerin büyük miktarda güç ve etki kazanmasını sağlamıştır. (Yasar, et al. 2012).

2- Savaş kavramındaki değişim: Dünyada eski zamanlardan beri ülkeler, kabileler, toplumlar ve çeşitli biçimlerde olan ve rakibe zarar vermeyi amaçlayan farklı araçlar kullanan gruplar arasında savaş ve çatışmalara tanık olunmuştur. Geleneksel savaş kavramıyla- esas olarak - bir devletin geleneksel yöntemler uygulayarak bir veya daha fazla ülkeye karşı daha fazla düzenli kuvvetleri ile mücadele etmesi anlatılmaktadır (Hoffman 2007.)

Düşmana saldırmak veya onun saldırılarına karşı kendini korumak durumunda zafer elde etmek için gereklilikler sağlanması yoluyla taraflarca savaşa hazırlık yapılmaktadır. Modern savaşlar ise kapsayıcılık ile karakterize edilir, yani askeri ve ekonomik, sosyal, bilimsel ve politik yönler gibi çeşitli sektörler üzerinde kapsamlı bir etkiye sahiptirler. Modern dönemdeki geleneksel savaşlar, Geleneksel savaşlar ülkelerin arazisine, doğal sınırlarına ve coğrafi konumlarına büyük önem vermektedir. Askeri çalışmalarla ilgili teorilerin çoğu jeopolitik kavramlarına dayanarak ortaya çıkmış, devlet egemenliğinin gerçekleşmesi terimi çerçevesinde ilerlemiştir (Hirst 1995.).

Modern çağ, özellikle teknolojik bir devrime tanık olan gelişmiş ülkelerde savaş yöntemlerinde büyük bir değişikliğe tanık olmuş ve askeri ordular bilgi savaşı olarak adlandırılan kavrama büyük önem vermeye başlamıştır. Bu savaş, uluslararası insancıl hukuk dâhilinde silahlı çatışma düzeyine yükselen veya gerçekleşen siber uzay operasyonlarından oluşan mücadele araçları ve yöntemleri kullanılarak uygulanmaktadır.

Siber savaşlar genellikle doğrudan insan kayıplarına yol açmaz, ancak genellikle maddi kayıplara yol açmaktadır. Bir ülkeye bağlı bilgisayarlar veya ağlar saldırıya uğradığında, onlara nüfuz edildiğinde veya onların çalışması engellendiğinde siviller

içme suyu, tıbbi bakım ve elektrik gibi temel ihtiyaçlardan yoksun kalabilir. Örneğin GPS sistemleri çalışmazsa, kurtarma helikopteri kalkışlarını kesintiye uğratarak sivil kayıplar meydana gelebilir. Barajlar, nükleer santraller ve uçak kontrol sistemleri bilgisayarlara bağımlı olmaları nedeniyle siber saldırılara maruz kalabilir. Ağlar o kadar birbirine bağlıdır ki, diğer parçalara zarar vermeden veya tüm sistemi bozmadan sistemin bir bölümüne karşı yapılan bir saldırının tesirini belirlemek zordur. Yüzbinlerce insanın çıkarları, sağlığı ve hatta yaşamları bundan etkilenebilir (Arquilla and Ronfeldt 1993).

Birçok ülkenin savunma stratejisi artık siber operasyonlar için askeri bir strateji içermektedir. Siber güvenlik ve bilgi güvenliği alanına yönelik devasa finansal mekanizmalar ve tahsisler, geleneksel savaşların yanı sıra önemli bir çatışma sahası olacak siber alanda gerçekleşmesini beklenilen savaşlardaki role de yöneliktir. Gelişmiş ülkeler, siber güvenlik alanındaki kadrolarının kapasitelerini geliştirerek siber alandaki stratejik üstünlüklerini garanti etmeye çalışmaktadır.

Uluslararası Hukuk ve Siber Savaş:

Uluslararası insani hukuk alanındaki hukuk uzmanları, siber savaş teriminin günümüzde ülkelerin karşı karşıya olduğu ulusal güvenlik tehditlerinin ön saflarında yer aldığını düşünmektedir, bu nedenle uluslararası kamu hukukunun kuralları açısından bir bilgisayar veya İnternet kullanarak yapılan saldırıların silahlı saldırı tanımında değerlendirilmesi konusu ortaya çıkmıştır. (Shackelford 2009). Bu durum mevcut yasal düzenleme ve kuralların, yeni teknolojinin ortaya çıkması ışığında meydana gelen gelişmelerle ne ölçüde uyduğu ve bu teknolojinin özellikleri ve bunlardan kaynaklanabilecek insani etkiler açısından yeterince açık olup olmadığını bilmeyi gerektirmiştir. Geçmiş yıllar, modern savaş alanına çok çeşitli yeni teknolojilerin tanıtılmasına tanıklık etmiş ve bilgi alanı yeni bir savaş sahası yaratmıştır (Shaalan 2016).

Uluslararası hukuk dalındaki birçok uzman, yasal kuralların ve uluslararası mevzuatın uygunluğunu incelemek ve anlamak ve bunların siber alanda gerçekleşen elektronik savaşlara uygulanmasını araştırmaktadır. Uluslararası mevzuat ve yasal

kuralların siber saldırıları sınırlandırmaya ve azaltmaya ve caydırıcılık stratejisi özellikle de askeri operasyonların örgütlenmesinin temelini oluşturan silahlı çatışmalar etrafında şekillenmiştir (Şafak 2020).

NATO, siber savaşlar ve internet üzerinden operasyonlara katılıma dönük kuralların düzenlenmesini içeren 282 sayfalık "Tallinn" rehberi adlı uluslararası bir yasalar dizini yayınlamıştır. "Tallinn" rehberi bir devlete karşı bir elektronik siber saldırı savaşı yürüten bir ülkenin hücumu altındaki ülkeye hak vermektedir. "Tallinn" rehberi, bir ülkeye siber saldırının başlatılması durumunda gerçek askeri gücün kullanılabileceğinden söz etmektedir ve bu saldırı insan hayatının kaybedilmesine yol açabileceğini belirtmektedir. Aynı zamanda uluslararası insancıl hukukun siber savaş için geçerli olduğunu ve onun kurallarının bu alanda oynayacağı rolü tanımladığını göstermektedir.

Tallinn Rehberi bu konuda ilgi çekici bilgiler sunmaktadır. Rehber, uluslararası silahlı çatışmaların ve uluslararası olmayan silahlı çatışmaların geleneksel dualizmine bağlı kalmakta, elektronik operasyonların koşullara bağlı olarak silahlı çatışma oluşturabileceğini kabul etmektedir - özellikle bu operasyonların zararlı etkileri üzerinde durmaktadır. Bu bağlamda, uluslararası insancıl hukuk kapsamında "siber saldırı" tanımını "ya saldırgan ya da defansif (savunmaya dayalı) olarak, insanlarda yaralanmaya ya da ölüme, nesnelere zarar ya da yıkıma neden olması beklenen" bir elektronik süreç olarak tanımlamaktadır. Ancak konunun özü ayrıntılarda bulunmaktadır, yani elektronik dünyada "zarar" olarak neyin anlaşılması gerektiğinde yatmaktadır (Michael, et al. 2003).

Ayrıca, uluslararası hukuk, siber uzayda aşılan önemli konulardan biri olarak kabul edilen, devletin bölgesel sınırları üzerindeki egemenliği meselesini dolaylı olarak tanımaktadır. Siber alanda jeopolitik sınırların olmaması, hemen hemen her yerde saldırgan operasyonların yürütülmesine izin vermekte ve bu küresel güvenliğe doğrudan bir tehdit oluşturmaktadır.

2.1.2. Siber Tehditlerin Uluslararası İlişkiler Üzerindeki Etkisi

Bilgi ve iletişim teknolojisi alanındaki küresel devrimden sonra, ülkeler ve diğer tüm uluslararası aktörler dünya çapındaki etkileşimlerinin yönetiminde bu modern teknolojilere dayanmış, bu durum uluslararası ilişkilerin sorunları ve kavramlarında önemli değişikliklere neden olmuştur. Özellikle enerji, sanayi, tarım, iletişim, ulaştırma, devlet hizmetleri, e-ticaret, bankalar ve finansal kuruluşların yeni teknolojiler kullanılmaktadır. Bu çıkarların elektronik alanı, ulusal bilgi altyapısı (NII), olarak bilinen tek bir çalışma ortamında birbiriyle bağlantılıdır.

Tüm sektörlere elektronik hizmetler sağlayan (NII) altyapının tek olması bu çıkarların birine veya tümüne yapılan herhangi bir saldırı sonucu stratejik bir dengesizliğin oluşmasına sebep olmaktadır. Aynı zamanda yeni bir çatışma şekli ve ulusal güvenlik tehdidi türü sunmaktadır. Uluslararası ilişkilerin durumu, dijital ekonomiye ve bilgi teknolojisine bağımlı hale gelen güç ölçülerindeki değişimin bir sonucu olarak ana güçler arasındaki gerginlik durumunu yansıtmaktadır (Sassen 1999).

Bu durum, dünyanın siber alanla bağlantısını artırmakta, küresel bilgi altyapısına siber saldırı riskini yükseltmektedir. Özellikle çok uluslu şirketler, küresel politika üzerinde önemli bir etkiye sahip yeni uluslararası oyuncular olarak önemli bir rol üstlendikten sonra bazı devletlerin kapasitelerinin ve potansiyellerinin ötesinde bir konum edinmiştir ve siber alan aktörlerinin amaçlarını ve devletin egemenliği üzerindeki etkilerini gerçekleştirmesini sağlamıştır. Devletin özel sektör lehine stratejik sektörlerden çekilmesi, özellikle hayati tesisler ve devletin altyapısında elektronik sistemlere olan bağımlılığını artırması, onları özellikle bir sivil ve askeri eşgüdüme - çift yöne sahip oldukları için onları saldırı hedefi haline getirmektir. Dolayısıyla devlet topraklarına fiziksel ve doğal biçimde girilmesine ihtiyaç duyulmadan insanlara fiziksel ve ekonomik zarar vermek mümkün hale gelmiştir (Cohen 1996). Bundan dolayı ötürü elektronik savaşın küresel ve bölgesel oyuncular için rekabetin ana arenası haline gelen siber alanın kullanım özgürlüğü üzerindeki etkisi önem kazanmaktadır. Korku ve endişeler, artık geleneksel ve nükleer askeri kapasitelerin geliştirilmesiyle değil, özellikle ekonomi sahasında, askeri alanlarda altyapıları yok etme kapasitelerinin artması ve siber kapasitelere odaklanılması ile ilgilidir. Siber saldırıların

yayılması ve kaynakların çeşitliliğinin bir sonucu olarak, ABD Savunma Bakanlığı'nın siber tehditlerle karşı karşıya olan eksenlerden biri olarak uluslararası ittifak inşa etmesi fikri ortaya atılmış ve savunulmuştur. Bu bağlamda, Savunma Bakanlığı'nın 2015 stratejisi, ortak siber tehditleri engellemek ve uluslararası güvenlik ve istikrarı artırmak için uluslararası ittifaklar ve ortaklıklar kurma ve sürdürme hedefini barındırmıştır (Barack. 2015).

Dünya medeniyetleri ve kültürleri arasındaki çatışma, bilginin değeri ve uluslararası ilişkilerde kullanımı artmaktadır. Sanayileşmiş Batı'nın uyguladığı bilgi akışı bugün üçüncü dünya ülkelerinde ulusal kültürlere yeni tehditler ve tehlikeler getirmektedir. Bazı ülkelerdeki yerel medyanın, bilgi teknolojisinin gelişimi ışığında batı medyasına bağımlılığı, mevcut yerel kültürlerden farklı olan yeni değerlerin ve etik değerlerin transferine yol açarak toplumlarda bir tür kültürel istilaya ve bir tür kültürel ve sosyal istikrarsızlığa yol açacaktır.

Bu nedenle, birçok ülke, bilgi ve iletişim teknolojilerinin geliştirmesinin getirdiği bu sosyal, kültürel ve dini müdahalenin ortasında kültürel, sosyal ve dini güvenliklerini korumaya ve çalışmaktadır.

2.1.3. Siber Tehditler ve Küreselleşme

Küreselleşme, belirli bir zaman ve çerçevede tanımlanabilen ve böylesi bir genel çatıya dâhil edilebilen tek bir kavram olmadığı gibi belirli bir başlangıç ve bitişle nitelenebilecek bir süreç değildir. Ayrıca net bir şekilde açıklanmamaktadır, tüm insanlar ve her durumda uygulanabilir yapıdadır. Küreselleşme ekonomik entegrasyonu kapsamaktadır. Sınır ötesi politikaların taşınması, bilgi aktarımı, kültürel istikrarın sağlanması ve iktidar söyleminin yaygınlaşmasıdır. Evrensel bir süreci kapsayan kavram, "sosyal ve politik kontrol içermeyen küresel bir piyasa kurumudur (Al-Rodhan and Stoudmann 2006).

Bilgi teknolojisi ve elektronik iletişim çağında, küreselleşme iş birliğine ve karşılıklı bağımlılığa dayanmaktadır ve dolayısıyla sorunlar da küreselleşmektedir. Aynı zamanda devletin geleneksel biçiminde kayda değer bir düşüş ve onun bir dizi stratejik ve hayati sektörlerin gerilemesi gözlemlenmektedir. Özel sektörün yararına

gelişmeler yaşanmış ve aynı zamanda, yabancı ve çokuluslu şirketlerin, özellikle teknoloji alanındaki rolleri artmış, özellikle bazı ülkelerin hükümetlerinin teknik kapasitelerinden üstün olmaları nedeniyle siber alanda etkili oyunculardan haline gelmiştir (Glass, et al. 2008).

Küreselleşme, internet ve ulus ötesi grupların, siber uzayda ulus devletlerin egemenliğini tehdit etmesini mümkün kılmıştır. Bilgisayar korsanları, programcılar ve saldırganlar artık hükümet operasyonlarını, bankacılık işlemlerini, kentlerin elektrik şebekelerini ve hatta askeri silah sistemlerini bozma veya yok etme yeteneğine sahip olabilmektedir. Bu nedenle, küreselleşme ve dijital ara bağlantı döneminde ulus devletler, yıkıcı siber saldırılara ve etkilerine karşı koymak ve bunları önlemek için savunma işbirliği faaliyetlerine katılmalıdır (Podhorec 2012).

Ayrıca, hükümetler iletişim altyapısını tamamen yeniden biçimlendirmeli, ülke içindeki ve dışındaki bilgi akışını sınırlamalı, ülkelerin bu süreçte uluslararası ticareti zedelemeden verilerinin sınırlar arası akışını etkin bir şekilde izleme yeteneğini kontrol etmeli ve desteklemelidir. Dolayısıyla ülkeler tutarlılıklarını ve işbirliklerini daha da derinleştirmelidirler (Cory 2017). Küreselleşme sistemi, ABD ve uluslararası güçlerin "terörizmle mücadele" başlığı altında sınırlarına bağlı olmayan politikaları benimsemelerine izin vermiştir. ABD ve Avrupa Birliği'ndeki müttefiklerinde Amerikan güçlerinin konuşlandırılmasıyla veya Amerikan istihbarat varlığı veya diğer biçimler Amerikan topraklarından binlerce mil uzakta bulunmasıyla temsil edilen yeni bir Amerikan güvenliği kavramı sunmuştur. Küreselleşme, dünyadaki elektronik bilgi savaşını içerecek şekilde genişlemiştir. Söz gelimi Amerika Birleşik Devletleri, örneğin, Prism programı ve NASA'nın uydu kanalı aracılığıyla Avrupa Birliği üyeleri ve diğer ülkeler hakkında bir casusluk skandalına tanıklık etmiştir. Bu ayrıntılar, ABD Ulusal Güvenlik Ajansı ile sözleşme yapan Edward Snowden tarafından Haziran 2013'te Rusya'ya iltica edildikten sonra açıklanmıştır (Chen 2017).

Küreselleşme sürecinin son boyutu ticaret, savaş ve kültür de dâhil olmak üzere her yaşam biçimini değiştiren dijital devrimdir. Askeri kolejler internet üzerinden güvenlik konularına odaklandıkça, küreselleşme ve yeni teknolojilerin rolleri

istihbarat, terörle mücadele ve stratejik güvenlik konularının ayrılmaz bir parçası haline gelmektedir.

Küreselleşme Sürecinde Siber Tehditler ve İnsan Hakları:

Küreselleşme meselesinin olumlu ve olumsuz birkaç boyutu vardır. İnsan hakları konusu, özellikle internet hizmetleri ve bilgi teknolojilerinin yayılmasının ardından küreselleşme ışığında önemli ölçüde gelişmiştir. Bu da insanların özgürlük, eşitlik ve güvenlik hakkı gibi haklarına ilişkin bilgilerine büyük katkı sağlamıştır.

Liberal hareketler, bireylerin özgürleştirilmelerine, güçlendirilmelerine, devlet sistemini daha şeffaf hale getirmelerine yardımcı olma ve çeşitli düzeylerde insan hakları ihlallerine karşı mücadele etme konusunda önemli bir rol oynamıştır (Moravcsik 2010). Özellikle Birleşmiş Milletler'in kuruluş yasası tarafından güvence altına alınan ve siyasi, sosyal ve ekonomik haklar gibi önemli temel hakları tanıyan, tüm devletler tarafından imzalanan Evrensel İnsan Hakları Beyannamesi bu şeffaflığa atıfta bulunmuştur.

2013 yılında Birleşmiş Milletler Genel Kurulu, özellikle dünyadaki siber casusluk operasyonlarının yayılmasından sonra, insanların dijital çağda gizlilik hakkını onaylamayı içeren bir belgeyi oylamış ve bu belge, internette gizliliğin ve ifade özgürlüğünün korunmasının önemini kararlaştırmıştır.

Küresel çevre insan yapımı olduğu ve bilimsel gelişme ölçeğiyle genişlediği için, siber alan her ülkenin, siber güvenliğinin ve vatandaşlarının haklarının korunmasını sağlamak için atılacak adımlara odaklanmak amacıyla özel ulusal stratejik belgelere sahip olmasını gerektirmektedir (Akyeşilmen 2016b).

Bazı eleştirmenler, insan haklarının küreselleşmeden, örneğin eşitlik hakkı ve diğer ekonomik ve sosyal haklardan olumsuz etkilendiğini söylüyor. Birleşmiş Milletlerin insan haklarının bölünmezliğine olan bağlılığı, İnsan Hakları Evrensel Beyannamesi'ne yansımaktadır. İnsan hakları hükümetlerin birincil sorumluluğudur. Küreselleşme büyük fırsatlar sunsa da, faydalarının maliyetlerinin eşit ve adil olmayan bir dağılımıyla paylaşılması, özellikle gelişmekte olan ülkelerde, tüm insan hak-

larından tam olarak yararlanılmasını etkileyen sürecin bir yönüdür. Mevcut küreselleşme döneminde eşitsizlik önemli ölçüde artmıştır ve küresel kalkınma bazen yoksunluk, sömürü ve diğer insan hakları ihlallerinden sorumlu olarak görülmektedir (Rabet 2009).

2011 yılında Birleşmiş Milletler İnsan Hakları Yüksek Komiserliği şunları söylemiştir: Dijital dünyada veya basılı belgelerle çalışılması sırasında insan hakları aynı oranda eşittir. Bu hakları koruma yükümlülüğü, tüm iletişimleri şifrelemek ve eski ve gereksiz verilerin süresiz olarak dünya çapında tutulmasından ziyade yeni siber güvenlik politikalarının geliştirilmesini içerir.

Zaman içinde, internetin küresel ölçekte yaygınlaşmasının bir sonucu olarak internete bir insan hakkı olarak erişim hakkını tanımak mümkün olacaktır. Bu, küreselleşme ışığında dijital veri ve bilgilerin güvence altına alınmasına yönelik talebin artmasına neden olacaktır (Hughes 2002)

2.2. Siber Uzayda Risk ve Tehdit Türleri:

Siber tehditlerin ve tehlikelerin etkisinin değerlendirilmesi, bu saldırıların niteliği ve türleri ve hedeflerine ulaşmadaki doğruluğu hakkında tam bilgi gerektirmektedir. Siber saldırıların ne ölçüde mücadele edilebileceği ve aşılabileceğine dair malumat, hedeflediği veri ve bilgilerin tam olarak korunması ve güvence altına alınması sağlanmalıdır, internet tehditleri hızla değişmektedir.

Yeni taktiklerin ve çeşitli ve modern saldırı yöntemlerinin geliştirilmesi sürekli olarak ilerlemekte ve hedeflerine nüfuz etme ve ulaşma kapasitelerini arttırmaktadır.

Saldırganlar genellikle “saldırı vektörleri” olarak adlandırılabilecek birden çok yol kullanarak hedef ağ sunucusuna veya bilgisayara erişir (Ingols, et al. 2009).

2.2.1. Bilgisayar veya Ağlara Yapılan Korsanlık Yöntemleri:

USB ana bilgisayar özelliği ve disk sürücüleri üzerinden özel hesapların veri tabanlarının çalınması, şifrelenmiş verilerin şifrelerinin deneme yanılma yöntemiyle kırılarak elde edilmesi gibi daha birçok korsanlık yöntemleri bulunmaktadır. Bunlardan bazıları şunlardır:

- **Sözlük saldırısı/ Dictionary Attack:** Bu teknik, kullanılan şifrelerin çoğunu içeren bir kitaplığa veya dosyaya dayanır. Saldırgan, eşleşen bir parola bulana kadar bu kitaplığı deneme yanılma yoluyla hedef alır. Kütüphanede yer alan sık kullanılan kelimeler, çoğu kişinin şifrelerini oluştururken kullandığı normal kelimelerdir, böylece bunları kolayca hatırlayabilirler, örneğin, "iloveu" veya "MySuperPassword" gibi kelimelere çokça başvurulmaktadır.

- **Kaba kuvvet saldırısı/ Brute force:** Önceki metoda benzer ama bir saldırganın kütüphanede olmayan şifreleri de denemesini içerir, örneğin şu şifreyi "Aa14vB3", "sözlük saldırısı" tekniği ile çalmak çok zordur. Ancak "kaba kuvvet saldırısı" teknolojisi ile bulmak kolaydır. Çünkü bu durumda saldırgan harfleri (a-z A-Z) ve sayıları (9-0) karıştırmak için mümkün olan tüm olasılıkları deneyecek özel bir program kullanacaktır. Ancak bu teknolojinin de sınırlamaları vardır ve bu esas olarak zaman faktöründe belirgindir. Parola ne kadar uzun olursa, onu tahmin etmek ya da bulmak da o kadar uzun sürer. Program, yalnızca bir bileşen içerebilen tüm parola olasılıklarını denemeye başlayacağından, iki bileşenin, ardından üç, dört, beş şeklinde yukarıya doğru sıralayacaktır.

- **Gökkuşağı Tablo Saldırısı/ Rainbow Tables:** Çoğu programcı uygulamalarında parolaları bile şifrelediğinden, "gökkuşağı tabloları" tekniği tüm olası şifre olasılıklarını ve her biri için karşılık gelen şifrelemeyi içeren devasa tablolara dayanır (Jablon 1997).

- Kodlama yöntemleri bir programcıdan diğerine farklılık gösterdiğinden, tablolar kodlama türüne göre dallanmaktadır. Ancak çoğu yüzlerce gigabaytı (GB) hatta binlerce gigabaytı aşan çok büyük boyutlara ulaşmaktadır.
- Web veya e-posta saldırıları,
- Farklı devlet kurum ve kuruluşlarının sistem ayrıcalıklarının yetkisiz kullanımı,
- Gizli bilgiler içeren kaybolmuş veya çalınmış cihazlar.

"Siber suçlar" kavramı, birçok farklı saldırı türünü içerir. Bu suçların iki gruba ayrılması mümkündür:

A) Hedef üzerinde sınırlı etkiye sahip olması ve çok az zarar vermesi ile karakterize edilen küçük suçlar.

B) Ülkelerde, uluslararası kuruluşlarda ve şirketlerde elektronik sistemleri hedef alan ve uzun süre uzayabilecek önemli etkileri ile karakterize edilen büyük ve küresel suçlar.

Birden fazla aracın elektronik silah olarak adlandırılabildiği ve çeşitli ve yıkıcı hasarlara neden olabildiği çok çeşitli siber tehditler vardır ve bunların ciddiyeti ve karmaşıklığı açısından farklılık gösterirler, ancak genellikle gizlilik, bütünlük saldırıları ve kullanılabilirlik bakımından temsil edilen üç farklı kategoriye ayrılırlar.

2.2.2. Siber Saldırı Türleri:

Elektronik silah olarak adlandırılabilecek çok sayıda araç kullanan birçok siber tehdit türü vardır:

Çok çeşitli yıkıcı hasarlara neden olabilirler. Şiddeti ve karmaşıklığı bakımından değişkenlik gösterir, ancak genellikle üç farklı kategoriye ayrılır:

- Gizlilik Saldırıları,
- Bütünlük Saldırıları,
- Bulunabilirlik (Ben-Asher and Gonzalez 2015).

- **Gizlilik Saldırıları/ Confidentiality Attacks:**

Bireysel hakkındaki kişisel bilgilere, banka hesaplarının çalınmasına veya kredi kartı bilgilerine yapılan saldırılara dayanır. Dark Web, saldırganlar tarafından satıldığı ve dijital para birimlerinin yasadışı olarak kullanıldığı için bu bilgileri satın almak için birincil pazardır. World Wide Web'den arama motorları tarafından endekslenmez ve erişmek için özel programlar gerektirir. Giriş yaptıktan sonra, diğer web sitelerine ve servislere normal web ile aynı şekilde bir tarayıcı aracılığıyla erişilebilir (Garfinkel, et al. 2002).

- **Bütünlük Saldırıları/ Integrity Attacks:**

Verileri ifşa etmek ve halkı bu kurum veya kişiliğe olan güvenini kaybetmek amacıyla etkileyen, hassas bilgilerine erişilen, daha sonra yayınlanan ve sızdırılan kişileri veya kurumları hedefleyen bir saldırı türüdür (Giani, et al. 2013).

- **Erişilebilirlik Saldırıları/ Availability Attacks:**

Amacı, kullanıcıların belirli bir mali ücret veya fidye ödeyene kadar özel verilerine erişmesini önlemektir (Giani, et al. 2013).

2.2.3. Siber tehdit türleri ayrıca şunları içerir:

Gizliliği ihlal etmeyi amaçlayan kötü amaçlı yazılımlar da büyük bir endişe kaynağı haline gelmiştir. Kötü amaçlı yazılımlar birkaç yıldır gizliliği ihlal etse de, son zamanlarda giderek daha popüler olmuştur. Casus yazılımlar kişisel faaliyetleri izlemek ve finansal sahtekârlıklar yürütmek için birçok sistemi istila etmiştir (McGraw and Morrisett 2000).

Arka kapı saldırıları: Bir bilgisayar sistemindeki veya uygulamadaki arka uç kapıları, uygulama programcıları tarafından uygulamaya kolayca girebilmeleri için oluşturulan konumlardır, genellikle sınıflandırılırlar. Bazen tasarımcılar ve programcılar, daha sonra geliştirme ve bakım amacıyla kullanılmak üzere bilgisayar ve ağlara erişmek için gizli yollar bırakırlar. Saldırganlar, bilgisayarlara ve ağlara yasadışı bir şekilde girdikleri tespit edildiğinde bu yöntemlerden yararlanırlar. Ağ işletim sistem-

leri ve birden çok kullanıcı için yaygınlaştığında arka kapılardaki tehdit ortaya çıkmıştır. (Bagdasaryan, et al. 2020).

Aktarım katmanından saldırı protokolünü ele geçirme: Aktarım katmanı güvenliği, bir uygulama ve kullanıcı iletişim kurduğunda, adresleme uygulamaları ve Internet üzerindeki kullanıcıları arasında gizliliği garanti eden bir protokoldür, aktarım katmanı güvenliği, hiçbir üçüncü tarafın herhangi bir mesajla dinlememesini veya kurcalanmamasını sağlar. Aktarım katmanı güvenliği, ağdan geçen veri paketlerini yakalamak ve sonra bunları değiştirmek ve ardından yolunu tamamlamak için ağa geri döndürmek için bu saldırıda oluşan güvenli soket katmanının halefidir, böylece veriler bu saldırı yoluyla değiştirilir (Gagandeep and Kumar 2012).

Dağıtılmış Hizmet Reddi Saldırısı (DDoS) Saldırısı:

Bir grup bilgisayarın, engellemek için bir sunucuya saldırması anlamına gelir: Dağıtılmış hizmet reddi (DDoS) saldırısı, hedeflenen bir sunucunun, hizmetin veya ağın normal trafiğini, internet trafiğinin akışıyla hedefe ya da onun içinde yer alan altyapısına çok yüklenerek hizmeti yavaşlama ya da geçiciengellemeye yönelik kötü niyetli bir girişim olarak görülmektedir. Bu tür saldırılar, hedef alınan makineye çok sayıda istek göndermektedir. Durdurulana ve hizmet dışı bırakılıncaya kadar, sunucu veya sunucu kaynaklarını kullanıcı tarafından kullanılamaz hale getirmeye çalışmaktadır. Bu, bir "DoS saldırısı" gerçekleştiğinde sitenin "trafiği"nin tüketilmesi anlamına gelmektedir, bu da sitenin çalışmayı ve ziyaretçilere görünmesini durdurmaktadır (Chang 2002).

Kimlik avı saldırıları: İletinin güvenilir bir yetkiliden geliyor gibi görünmesini sağlayan bir internet adresi içeren kimlik avı iletileri göndererek aygıtlara yasadışı olarak erişmenin bir yöntemi ve kimlik avı genellikle veriler de dâhil olmak üzere kullanıcı verilerini çalmak için kullanılır. Giriş ve kredi kartı numaralarının onaylanması. Bu, güvenilen bir varlık olarak gizlenen bir saldırgan, bir e-postayı, anlık iletiyi veya kısa iletiyi açarak kurbanı hayal kırıklığına uğrattığında oluşur. Alıcı daha sonra kötü amaçlı bir bağlantıyı tıklatmak için kandırılır, bu da kötü amaçlı yazılım yüklemeye, fidye saldırısının bir parçası olarak sistemi dondurmaya veya hassas

bilgileri ortaya çıkarmaya neden olabilir ve saldırının yıkıcı sonuçları olabilir. Bireyler için buna yetkisiz satın alımlar, fon hırsızlığı veya hırsızlık tespiti dâhildir (Hong 2012)

E-posta yoluyla spam: Spam ve Scam, her iki terimin de özel bir anlamı vardır. Scam kurumsal sahtekarlık ve spam damping demektir. İnternet dolandırıcılığı demek olan scam, internet servislerinin kullanılarak insanları dolandırmak, kullanmak veya kişisel bilgilerini çalmak amaçlıdır. E-postamızda genellikle her iki posta türünün de gelmesinden sıkıntı yaşanmaktadır. Birincisi scam sahipleri, bankada örneğin büyük miktarda paraya sahip olduklarını iddia ederek kendisine gönderilen postanın sahibini dolandırılmaktadır. Bu paradan kazanmasını isteyerek hesabına aktarım yapılmasını talep etmektedirler. Sonra kişi onlara para transfer etmekte ve bazen yüzbinlerce olduğu tahmin edilen bu işlemin sonucu olarak iyi bir komisyon alacağını düşünmektedir ancak hesabını vermekte ve para kaybetmektedir. Spam'e gelince, kötü niyetli e- posta olarak bilinmektedir. Ticari bir amaç için veya hatta belirli bir hedef yalnızca boş bir mesaj ve zararlı ekler gelebilmektedir. Spam, milyonlarca posta adresine bir e-posta gönderir. Messenger programlarında, spim adı verilen, telefon üzerinden ve hatta bloglar aracılığıyla yollanan spam formları vardır (Yardi, et al. 2010).

Sosyal mühendislik saldırıları: Sosyal mühendislik, insan etkileşimleri yoluyla gerçekleşen çok çeşitli kötü amaçlı faaliyetler anlatan bir terimdir. Psikolojik manipülasyon, kullanıcıları kandırmak ve mağdurun hassas bilgileri bıraktığı güvenlik hataları yapmalarını sağlamak için kullanılır. Sosyal mühendislik saldırıları bir veya daha fazla adımda gerçekleşir. Fail amaçlanan mağduru izler ve saldırıyı ilerletmek için gerekli olan olası giriş noktaları ve zayıf güvenlik protokolleri gibi temel bilgileri toplar. Bundan sonra, saldırgan, mağdurun güvenini kazanmak için hareket eder ve hassas bilgileri ifşa etmek veya hayati kaynaklara erişmek amacıyla güvenlik uygulamalarını parçalayan ve bunlara sızan sonraki eylemler için teşvikler sağlar (Krombholz, et al. 2015).

Zorunlu Tarama Saldırısı: Güçlü tarama, bir URL'yi doğrudan uygulayarak kısıtlı sayfalara veya diğer hassas kaynaklara erişmek için kullanılan saldırı yöntemi-

dir. Güçlü tarama aynı zamanda zorunlu tarama olarak da bilinir, saldırgan kısıtlı dosyalara erişebilir ve bilgileri görüntüleyebilir. Çoğu web uygulaması, yeterli haklara sahip kullanıcıların yalnızca belirli sayfalara erişebilmesini sağlamak için kimlik doğrulaması kullanır. Kullanıcıların erişmelerine izin vermeden önce bir kullanıcı adı ve parola sağlamaları gerekir. Zorunlu tarama, bu denetimleri atlatmaya çalışan basit bir tarayıcı saldırısıdır. (Bennetts 2013).

2.2.4. Siber Tehditlerin Bazı Alanları:

Sosyal mühendislik/ Social engineering

• Bu, gizliliğe yönelik bir saldırı türüdür ve işin performansında psikolojik manipülasyon sürecini veya mağduru önemli bilgileri bırakmaya itme sürecini içerir.

İleri Kalıcı Tehditler/Advanced Persistent Threats

Kısaca APT'ler olarak bilinirler, yetkisiz bir kullanıcının keşfedilmemiş bir ağa sızdığı ve uzun süre kaldığı bir tür bütünlük saldırısıdır.

• APT'nin amacı ağa zarar vermeden veri çalmaktır.

- APT'ler en çok ulusal savunma, imalat şirketleri ve finansman platformları gibi yüksek değerli bilgilere sahip sektörlerde görülür (Chen, et al. 2014).
- Kötü Amaçlı Yazılım ve Casus Yazılım
- • Erişime uygunluk durumuna bağlı bir saldırı türüdür.
- • Bilgisayarın sahibinin bilgisi olmadan erişimi çıkarmak veya yok etmek için tasarlanmış bir programa başvurulur.

Yaygın kötü amaçlı yazılım türleri arasında casus yazılımlar, keylogger'lar, virüsler ve daha fazlası bulunur (Yen and Reiter 2008).- Siber Tehditlerden Korunma ve Siber Güvenliğin Sağlanma Biçimi:

Aşağıdaki basit adımlar, iyi bir siber güvenlik ve güvenlik düzeyini korumanıza yardımcı olabilir:

- Güvenilirlik: Herhangi bir kişisel bilgi verirken yalnızca güvenilir siteleri kullanırken web siteleri araştırılmalı ve girilmelidir. Buradaki tercih edilen kural URL'yi doğrulamaktır. Site başlangıçta https içeriyorsa, bu güvenli bir site olduğu anlamına gelir, ancak URL olmadan http içeriyorsa, kredi kartı verile-

ri veya sosyal güvenlik numarası gibi hassas bilgileri girmekten kaçınılmalıdır.

- Gelen Kutusu: E-posta eklerini açarken veya bilinmeyen kaynaklardan gelen ileti bağlantılarını tıklatırken dikkatli olunmalıdır, çünkü bunlar genellikle e-postanın çalındığı ve saldırıya uğradığı virüsler içerir.
- Güncellemeler (Her zaman güncel tutulmalı): Yazılım güncellemeleri genellikle güvenlik sorunlarını çözmek için önemli düzeltmeler içerir, bu nedenle programları, özellikle korumayı güncellemek ve yazılım geliştirmelerine ayak uydurmak gerekir.
- Yedekleme: Dosyaları güvenli ve bağımsız bir yerde saklamak, bir saldırı durumunda kurtarılmalarını sağlamaktadır ve bu da hasar riskini büyük ölçüde azaltmaktadır (Heartfield ve Loukas, 2016).

2.3. Uluslararası Sistemin En Önemli Aktörü Olan Devlet, Kamu Hukukuna Göre Siber Güvenliğin Yasal Sorumlusudur:

Ülkeler, mevzuat, siber suç müdahale ekipleri ve siber alandaki her türlü tehdidin geliştirilmesinde ve son kullanıcılara siber güvenlik konusunda önemli ilkelerin öğretilmesinde büyük adımlar atmıştır. Siber güvenliğin önemli bilgi ve iletişim altyapısını ve diğer ülkelerle olan ilişkilerini nasıl etkileyebileceğini daha fazla ülke fark etmektedir.

Bu nedenle, siber güvenlik alanındaki sınır ötesi güvenlik sorunlarıyla mücadele etmek için ülkeler, aralarında siber suçlarla ilgili Avrupa Konseyi anlaşması ve Dünya Bilgi Toplumu Zirvesi gibi siber güvenlik sorunlarının ele alınmasını içeren yeni uluslararası anlaşmalar yapmıştır (Keyser 2017). Kritik altyapı, askeri operasyonlar ve istihbarat toplama / yönetme için dijital teknolojinin artan kullanımı ve kapsamlı ulusal siber güvenlik planlarının geliştirilmesini gerektirdiği için siber güvenlik genellikle ulusal güvenlikle ilişkilidir. Ticaret, sağlık ve eğitimde çeşitli alanlarda devlet işlemlerinde bilgi teknolojisini kullanmaya ve dijital altyapıda interneti kullanmasına duydukları ilgi nedeniyle ülkeler için siber güvenliğin öneminin arttığına dikkat edilmelidir. ABD gibi gelişmiş ülkeler için siber güvenlik, ülkenin ulusal güvenliği içinde büyük önem taşımaktadır, çünkü tüm sektörler dijital teknoloji kul-

lanmaktadır (Castells 1996). Siber güvenlik alanındaki önemli düşünürler Richard A. Clarke, John Arquilla, David Ronfeldt ve Peter L. Levin gibi isimler, siber savaşın kaçınılmaz olduğuna ve er ya da geç özellikle Abd benzeri güçlerde tüm ulusun devrileceği bir felakete yol açacağına inanmaktadır. Bu düşünürler bu süreçte birçok insanın - belki de "Pearl Harbor" şeklinde ya da 11 Eylül 2001 olaylarında olanlara benzer şekilde öldürülmesini beklemektedir. Ünlü senaryo Clarke ve Knake böyle bir olayın temsili bir açıklamasını sunar. Kısacası, bu senaryo, daha önce görülmemiş bir şekilde hassas ulusal altyapıyı (CNI), elektrik ve iletişim ağlarının yanı sıra finansal ve ulaşım sistemleri de dâhil olmak üzere çeşitli sektörleri hedef alan elektronik silahlar tarafından düzenlenen bir dizi eşzamanlı saldırıyı ve hepsinin bir anda felç olmasını öngörmektedir (Arquilla and Ronfeldt 1993). Bu durumda, Bu durumda Clark ve Knake, hükümetin ulusun ve askeri ve sivil yapılarının kontrolünü etkili bir şekilde kaybettiğini ve geleneksel saldırıya maruz kalmasının muhtemel (yani, liderliği nüfusu işgal etmeye ve boyun eğdirmeye karar veren bir düşman tarafından) olduğunu söylemiştir (Clark and Levin 2009)

Bu duygu, siber uzayın birkaç (varsayılan) benzersiz özelliği açısından haklıdır. Bu hususların en önemlisi, siber operasyonlarda suçun savunmaya üstünlüğü ve siber uzayın doğası gereği herkesin önünde kilitli ve açık bir alan olması ve sınırsız ve çeşitli kullanıcılarla ilişkili olmasıyla ilgilidir. Bu duygu Amerika Birleşik Devletleri'nin siber alandaki ulusal güvenliğini korumak için gerekli önlemleri almasını gerektirir (Cole, et al. 2008).

Ayrıca, elektronik oylama kullanan Amerika Birleşik Devletleri'ndeki seçim sonuçları üzerinde de etkisi vardır. Rusya'nın görevdeki ABD Başkanı Donald Trump lehine sonuçlarını kontrol etmeye yönelik müdahalesini gösteren bir soruşturma sürüyor. Gelişmiş ülkeler için ulusal güvenliğin bir bileşeni olarak siber güvenliğin önemini göstermektedir. Başkan Obama ise saldırıyı "uluslararası standartların ve yerleşik davranışların ihlali" olarak nitelendirirken, birçok politikacının bu terimin politik veya diplomatik söylemde kullanıldığı şekliyle "egemenliğin ihlali" olarak nitelendirdiği müdahaleyi, Amerikan siyasi sürecine korkunç bir müdahaleyi temsil etmektedir (Ohlin, 2016).

Bazıları bu 2016 seçimini Soğuk Savaş sonrası dönemde Amerikan siyasetine sınır koyan eski kurumların dağılmasındaki en son bölüm olarak gördüler. Adayların, dünyanın çeşitli ülkelerinde kamuoyunu şekillendirme üzerinde büyük etkisi olan (Facebook, Twitter, YouTube) gibi sosyal medyaya (Facebook, Twitter, YouTube) güvenmesi nedeniyle ana medya ve siyasi partilerin temsil ettiği yerleşik kurumların çöküşünün başlangıcını işaret ediyor (Persily 2017).

2.3.1. Siber Güvenlik ve Devletin Teknolojik Gelişimi:

Bu konuyu tartışmak için aşağıdaki soruya cevap vermeliyiz.

Gelişmekte olan ülkeler ve gelişmiş ülkeler için siber güvenliğin bir ulusal güvenlik unsuru olarak önemi nedir?

Cevap: Gelişmekte olan ülkelerin çoğunda dijital kontrol sistemleri veya yüksek tanımlı dijital ordu kullanan sağlam bir altyapı yoktur. Aynı şekilde, eğitimli ulusal kadrolar bilgi teknolojisi alanında gelişmiş kapasitelere sahip değildir ve güvenlik konuları hakkında strateji ve düşünme yollarına sahip değildir. Gelişmiş ülkeler ile diğer ülkeler arasında büyük bir dijital uçurum var. Ayrıca, ileri sistemlere dayalı bilgi teknolojisini benimsemenin önündeki kurumsal engeller de vardır. Bu engeller, önceki nesil ekipmanlardan vazgeçme konusunda isteksizlikte açığa çıkmaktadır. Örneğin telekomünikasyon alanında (yani tellere dayalı elektromekanik altyapı), gelişmekte olan ülkelerde daha az önemlidir, bu nedenle bilgi teknolojisinin sanayileşmiş ülkelerde büyük ölçüde uygulanması daha olasıdır (Kenaroğlu and TAI 2003).

Örneğin, gelişmekte olan ülkelerden biri olan Irak, devlet kurumlarının elektronik uygulamalarının uygulanabileceği fiziksel ve beşeri bileşenleri içerecek bilgi teknolojisi için gelişmiş ve entegre bir altyapıya sahip değildir. Irak, devlet kurumları yapısında elektronik yönetişim sistemlerini benimseme yolunda ilk adımlarını attığı için bu yapı, dünyadaki çeşitli güvenlik, ekonomi ve sağlık sektörlerine tanık olan teknolojik devrime rağmen, kuruluşunun başındadır. Ulusal ekonominin ve küresel ekonominin entegrasyonuna katkıda bulunan faktörlerden biridir. Sonuç olarak, mevcut altyapısını korumak için gelişmiş siber güvenlik sistemleri bulunmamaktadır. Bu durum, Irak'ın dünyanın birçok ülkesi veya bölgesel komşu ülkeler için nüfuz

etmesi ve Irak güvenlik kurumlarıyla ilgili bilgileri gözetlemesi için açık bir alan olmasına yol açmıştır. Elektronik çalışma alanındaki zayıf güvenlik, kullanıcılarını memnun etmek için elektronik sistemler içinde sağlanması en önemli noktası olarak görülen karşılıklı güvenin ve güvenliğin ihlalini doğurmaktadır (Al-Jibouri 2016).

Irak kurumlarının çoğu, Irak sınırlarının dışında yer alan bir hizmet kaynağı ile uydudan bilgilerini temin etmek için sözleşme yapmaktadır ve yaygın finansal ve idari yolsuzluk nedeniyle güvenilir tedarikçilerle sözleşme yapmayı seçmemektedirler. Dolayısıyla bilgiler bu ülkelerin sunucularına aktarılmakta ve ardından Irak'a dönmektedir. Bu önlem Irak'ın bilgi güvenliğinin ihlali anlamına geldiğinden ve Irak'taki bilgi hareketinin bu tür büyük ihlallerinden kaçınmak için entegre bir bilgi güvenliği sistemi inşa edilmelidir (Awadi 2016). Bundan hareketle, gelişmekte olan ülkelerin, devlet anlaşmalarında elektronik ve dijital bilgi işlem sistemlerine güvenmedikleri için, şu anda ulusal güvenliklerinde yüksek siber güvenlik bulunmadığına inanıyoruz. Zira onlar görevlerini tamamlarken zayıflık, yavaşlık ve yanlışlık ile karakterize edilen kâğıt sistemleri ile çalışmaktadır.

2.3.2. Siber Güvenlik ile Ulusal Güvenlik ve "Devlet Egemenliği" Kavramlarının Birbiriyle İlişkisi:

Vestfalya Antlaşması'ndan bu yana ortaya çıkan ulus-devlet, vatandaşlarını her alanda korumaktan sorumludur ve askeri veya sivil olsun, çeşitli kurumları aracılığıyla ulusal güvenliğini korumaktan sorumludur.

Bireyler veya şirketler olsun. Bireyler güvenli iletişim araçlarına geri dönerek kendilerini tecrit etmedikçe artık gizliliklerini koruyamazlar. Bu nedenle devletin egemen toprakları, bireyleri ve kaynakları korumak için müdahale etmesi gerekir. Dolayısıyla, kendisi ve vatandaşları hakkındaki veri ve bilgiler üzerindeki egemenliğin yönetilmesi ulusal bir sorumluluktur ve uygun uluslararası ve ulusal çerçeveler geliştirilmelidir (Şener 2014).

Şirketlerin, medya kuruluşlarının, telekomünikasyon ve dijital teknolojilerin küresel boyutu, sistemlerin coğrafi kısıtlamalarını aşmalarını ve ülke sınırlarına sızmalarını sağlamaktadır. Bu, devletin egemenliğini tehdit etmekte ve özellikle şu anda

tanımlanabilecek küreselleşme devletinin yayılmasıyla otoritenin kalıcı olarak aşınmasını ve azaltılmasını sağlamaktadır. Küreselleşme, farklı ülkelerden insanlar, şirketler ve hükümetler arasında bir etkileşim ve entegrasyon sürecidir. Bu süreç, uluslararası ticaret ve yatırım tarafından yönlendirilen ve bilgi teknolojisinin desteklediği bir süreçtir. Çevre, kültür, siyasi sistemler, ekonomik kalkınma ve refah ve dünyadaki toplumların insanın fiziksel iyiliği üzerindeki etkiler (Fjäder 2014). Bu nedenle küreselleşme, devletin İnternet ve dijital bilgi teknolojisi aracılığıyla egemenliğinin karşı karşıya kaldığı en önemli tehditlerden biridir. İnternet, ülkelerin geleneksel işlevlerinin üç ana boyutuna meydan okumaktadır:

- Ekonominin düzenlenmesi
- Ulusal Güvenlik
- Ulusal Kimlik ve Değerlerin Korunması (akdenizli 2011).

Bazı süper güçler, kendilerinin ve vatandaşlarının ulusal güvenliğini korumaya ve siber alanın kullanımını düzenleyerek ve uygun mevzuat düzenleyerek devletin egemenliğini korumaya çalışmıştır. Bu nedenle, Çin'de, Çin Siber Uzay Kurumu, 1 Haziran 2017'de yürürlüğe giren Çin Siber Güvenlik Yasasının, sanal dünyada ulusal güvenlik, kamu yararı ve vatandaşların, şirketlerin ve kuruluşların hak ve menfaatlerini korumayı amaçladığını açıklamıştır. Bu, yabancı şirketlerin veya teknolojilerinin ve ürünlerinin Çin pazarına girişine herhangi bir kısıtlama getirmemekte ve yasalara uygun olarak serbest ve organize veri akışını sınırlamamaktadır.

Çin, ülke çıkarlarının gerektirdiği ve bu konudaki uluslararası uygulamalara uygun olarak siber alanı düzenlemek için egemen ülkelerin yasa ve kurallar koyma hakkı olduğuna inanmaktadır. Siber güvenlik Çin'de Batı dünyasından daha yaygın olarak tanımlandığından, sosyal veya politik istikrarı tehdit eden herhangi bir dijital bilgi ulusal güvenliği tehdit edici olarak görülecektir. Ayrıca, siber güvenlik hukukunda kişisel bilgilerin işlenmesi, Çin'in insan hakları felsefesini yansıtmaktadır. Çin, bu mevzuatın ülkenin ulusal güvenliği teşvik etme konusundaki yasal çabalarının bir parçası olduğuna inanmaktadır (Lee 2018). Bu yasa uyarınca, İnternet servis sağlayıcılarının kullanıcılara kişisel bilgi toplaması ve satması yasaklanacaktır. Yasa, şirketlerin verilerini Çin içinde depolamasını ve finans ve iletişim gibi sektörlerdeki

şirketlere güvenlik kontrolleri uygulamalarını gerektirecek. Bireysel kullanıcılar mesajlaşma servislerini kullanmak için gerçek adlarıyla kayıt yapmalıdırlar. Internet servis sağlayıcıları, servislerle ilgisi olmayan kullanıcılardan bilgi toplayamazlar ve bu bilgilerle yasalara ve eyalete özgü kurallara uygun olarak ilgilenmelidirler. Hizmetler, yanlış kullanıldıklarında bilgilerini siler.

Kanun, İnternet güvenlik personelinin elde edilen bilgileri koruması gerektiğini ve özel bilgiler ve ticari sırlar da dâhil olmak üzere bilgi sızdırmasını veya satmasını yasakladığını belirtmektedir.

Bu mevzuata göre kanunları çiğneyen ve kişisel bilgileri ihlal edenler ağır para cezalarıyla karşı karşıya kalacaktır (Wee 2017).

2.3.3. Siber Tehditlerin Sadakat ve Devlete Aidiyet Durumuna Etkisi:

Gelişmekte olan ülkelerin karşılaştığı en önemli sorunlardan biri, küresel ortamın ortasında ulusal güvenliklerini koruma sorunudur. Ve bu ortam, siyasi, ekonomik ve sosyal çıkarlarını bu ülkeler pahasına elde etmeye çalışan büyük güçler tarafından yönetiliyor. Büyük güçler, çeşitli alanlarda teknolojik patlamalardan yararlandılar. Ve bilgi ve iletişim teknolojisi ile ilgilenen ve bu ülkelerin yayılmasını istediği fikirlerin aktarılması yoluyla dünyanın birçok halkının kültürel, sosyal ve entelektüel mirasını değiştirmek için çalıştı. Bu teknolojik gelişmeler, farklı toplumlar ve halklar arasındaki iletişimi sağlayarak kültürler ve dinler arasında karışmaya yardımcı oldu ve küreselleşme ışığında diğer ülkelerin ekonomik, sosyal ve politik deneyimleri hakkında bilgi edinmelerini sağladı. Azınlıkların rolünü teşvik eder ve ulusun ahlakını sorgulayan konuşmaları teşvik eder, modern teknoloji kullanılarak postmodern dönemde ulusların kültürel normlarını değiştirmeyi mümkün kılar. (Jameson and Miyoshi 1998).

21. yüzyılın başında, Siber Toplum kavramı yayılmıştır. Siber alan içinde Bireyler arasındaki ilişkilere dayanır ve siber alandaki kolektif iletişim araçlarıyla aralarındaki kişisel bağlantıyı gösterir. İletişim teknolojisinin toplumdaki kamuoyu eğilimlerinin oluşması üzerindeki etkisine baktığımızda, toplumun küreselleşme olgusu ve halkların entelektüel ve kültürel kazanımlarıyla ortaya çıktığını görebiliriz. Bu

gelişmeler de siteler tarafından garanti edilen mutlak özgürlüğün bir sonucu olarak ortaya çıkmaktadır (Jones 1995). Gelişmekte olan ülkelerdeki karar vericiler, etkili dış ülkeler tarafından siyasi karar ve ülkedeki politikacıların seçimini etkileyebilme ve diğer ülkelerdeki iç sorunları ülkenin iç kısmına, özellikle mezhepsel, ırksal, dini ve milliyetçi sorunlara aktararak bu ülkelerin ulusal güvenliğine yönelik tehditlerin farkındadır. . Bu siyasi, ekonomik, askeri, ideolojik ve sosyal güvenliğinin egemenliği, istikrarı ve güvenliği için bir tehdit oluşturmaktadır. Çünkü vatandaşın vatanı ile devlet arasındaki ilişkiyi, vatandaşın kimliğini ve vatanına aidiyet duygusunu olumsuz etkilemektedir. Vatana aidiyet hissetme, ona katılma, bizi ona bağlayıp en yüksek sadakat düzeylerine ulaştıran güçlü bir ilişki kurma anlamına gelir.

Sadakat/bağlılık, bir kişinin bir topluluğa, doğumla birlikte taşıdığı ve ailesine, topluma ve ülkesine dönük beslediği histir, ailesine, topluma ve ülkesine ahlaki ve maddi olarak bağlanmak, onun topluluğunu inşa etmek için değerli ve kıymetli olmasını sağlayan ulusal bir değerdir (Isin and Turner 2002).

Sosyal medya, terör örgütlerinin kullandığı en önemli araçlardan biri haline gelmiştir. Şiddet, kaos, terörizm ve suç eylemlerini yayma, farklı bölgelerden savaşçıları görevlendirme ve özellikle genç insanlar arasında dini fikirleri ve inançları manipüle etme ve radikal görüşleri yayma eğilimi görülmektedir. Bu durum, vatansever hisleri zayıflatmaktadır ve hatta vatandaşlık kavramına duyarsız kılabilmektedir.

Ulusal kimliğini ortadan kaldırmaya çalışılması mümkündür, böylesi gelişmeler toplum içinde karışıklık yaratmakta ve ülkelerin ulusal güvenliğini tehdit etmektedir (Labban 2016).

Yukarıda belirtilenlerin tümü, devlet ve devlet kurumlarında bilgi güvenliği sorununu ortaya koymaktadır.

Sonuç olarak, ülkenin elektronik güvenliğini sağlamak, elektronik sınırlarını korumak ve internet kullanımı sırasında vatandaşların devlete güveninin zedelenmesini önleyen bir bilgi bağışıklık sistemi (Antivirüs) uygulamak için hükümet içinde "Bilgi Güvenliği Denetleme Birimi" gibi yeni teşkilatlar geliştirilmesi gerekmektedir.

2.3.4. Siber Savaşlar ve Devletin Siber Alanda Zorluklarla Yüzleşmedeki Rolü:

Çağdaş dünyamızda, tanık olduğumuz teknolojik gelişmeyle uyumlu yeni savaş kalıpları ortaya çıkmıştır. Elektronik saldırılara "siber savaş" denmektedir, çünkü fiziksel savaşa benzemektedir. Bilgisayar korsanları ülkeler, insanlar ve şirketlerden başkalarına ait dosyalara, sitelere ve bilgilere çeşitli programlar aracılığıyla ve çeşitli siyasi yollarla, belirli siyasi, ekonomik ve ekonomik hedeflere ulaşmak için saldırırlar.

Siber savaş terimi, bir ulus devletin başka bir ülkenin bilgisayarlarına veya ağlarına çeşitli amaçlarla sızmak için yaptığı eylemleri ifade eder.

Bu tür savaşların ayırıcı özelliği, saldırganlar ve korsanlar için geleneksel savaşlardan daha ucuz olması, yeni teknolojilere dayanan insan becerileri ve modern elektronik silahlar gerektirmesidir. Barış, savaş veya kriz zamanlarında, istenilen herhangi bir vakitte bu tür saldırılar düzenlenebilmektedir. Korsanlar ve saldırganlar, ülke veya başka bir aktör olsun, bu yöntemi tercih etmektedir. Çünkü siber suçları tespit etme ve destekleme zorluğu nedeniyle onlar için daha güvenli. Çünkü sınır ötesi olabilir ve onu bulmak veya saldırganı hassas bir şekilde bilmek zordur. (Clarke and Knake 2014).

Siber savaşlar çoğu zaman saldıran devletin başka bir ülkeye verebileceği ciddi hasarlara yol açmaktadır. Saldırganın hedef topraklara fiziksel olarak girmesi gerektirmeyen bu hamleler, maddi ve ekonomik hasarlara, hatta büyük ülkelerin elektronik sistemleri etken kullanması nedeniyle can kaybına neden olabilmektedir. Bu nedenle devletler, yeterli bir güvenlik derecesini sağlayan birçok stratejiyi takip ederek zorluklarla ve siber saldırılarla yüzleşmek için önlemler almak durumundadır, bu stratejiler bağlamında siber caydırıcılıktan bahsedilmektedi

Siber Caydırma Stratejisi:

Siber caydırıcılık, siber uzayda ulusal konulara karşı zararlı eylemleri önlemeyi amaçlamayan faaliyetler bütünüdür ve üç temele dayanmaktadır: Güven oluşturan savunma, intikam alma kapasitesi, intikam alma ve rakibi tehdit edebilme kabiliyetidir.

Birçok araştırmacı caydırıcılığın siber alanda etkili bir strateji olmadığına inanmaktadır. Siber uzaydaki saldırganların ister devlet ister birey olsun, sınırlı bir etkisi vardır. Caydırıcılığın kaynağını nasıl olacağını belirlemek ve saldırganın büyük bir doğrulukla tanımlanmasının zorluğunun yanı sıra, siber saldırının kaynağını tanımlamanın zorluğu ile ilgili zorlukların yanı sıra kullanılan saldırı yöntemlerinin geliştirilmesi nedeniyle (Lupovici 2011).

Son yıllarda siber saldırıların sayısı keskin bir şekilde artmış, elektronik caydırmanın mümkün olup olmadığı sıklıkla sorulmuştur.

Caydırma stratejilerinin arkasındaki teorilerin veya kavramların anlamak ve siber uzaya nasıl uygulandıklarını bilmek bu soruyu cevaplamak için altyapıyı oluşturacaktır. Caydırıcılık şu şekilde tanımlanır: "Kararlı ve etkili bir tepki ile muhtemel bir tehdidin etkisizleştirilmesi veya düşmanın eylem maliyetlerinin arzulanan faydalardan daha ağır bastığına ikna edilerek, saldırgan eylemin önlenmesi. (McKenzie 2017). Devletin maddi, askeri ve teknolojik kabiliyetleri ile ilgili iki tür caydırma seçeneği vardır:

- Pasif caydırıcılık: Düşmanı inkâr yoluyla caydırmak: Saldırıları önleme yeteneği olup aşağıdakilerle açıklanabilir: Bir saldırı başlatılırsa, o zaman savunma önlemleri o saldırıyı etkisiz hale getirir, bu nedenle atak başarısız olur ve boşa gider. Saldırı savunma sistemlerine sızsa bile hedef üzerinde arzulanan etkiyi oluşturamaz.
- Aktif caydırıcılık: Ceza yoluyla caydırma (İntikam tehdidi): Elektronik açıdan gerekirse maddi askeri güç kullanımı da dâhil olmak üzere, düşmana karşı tüm savunma araçlarını kullanmak demektir (Libicki 2009).

Birçok araştırmacı ve teorisyen, nükleer caydırıcılık gibi fiziksel gücü kullanmasını içeren geleneksel caydırıcılık teorilerinin siber uzayda nasıl uygulandığını görmeye çalışmıştır. Caydırıcılık teorisinin gereksinimlerinin ve koşullarının siber alanda geçerli olmadığını, çünkü siber çatışmanın doğasının askeri olandan farklı olduğunu bulmuşlardır. Soğuk Savaş döneminde, nükleer silaha sahip ve düşmana maddi zarar verme kapasitesine sahip az sayıda ülkede caydırıcılık sağlanmıştır. Ancak siber alanda elektronik silahlarını geliştirmek isteyen 140'tan fazla ülke vardır.

Ayrıca, bazı insanlar ellerindeki teknik ve teknolojik kapasitelerle kişisel hedeflerine ulaşmak için süper güçlere saldırabilir. Saldıran tarafı siber alanda intikamla tehdit etmek zor olacak ve böylesi bir tehdit çok fazla güvenilirlik taşımayacaktır. Çünkü onun kimliğini ve yerini siber uzayda tespit etmedeki güçtür, bahsedilenlerle birlikte siber caydırıcılık hala kısmen etkilidir (Bahi 2017).

Devletin siber saldırıların neden olduğu zararı azaltmak için alabileceği ve uygulayabileceği birçok yol vardır, bunların en önemlileri şunlardır:

Birincisi :İlk darbeye dayanabilme, mümkün olduğunca çabuk atlatma ve manevra kabiliyeti: Bu, alternatif dijital sistemlerin geliştirilmesini gerektirir, çünkü bir ülkenin bir sisteme bağımlılığı, bir siber saldırı durumunda devletin altyapısında çalışmanın durmasına yol açacaktır. Dolayısıyla devletler, gerektiğinde devletin kullanabilmesi için alternatif sistemler oluşturabilirler.

İkincisi: Bilim ve teknolojide egemenliği korumak çok önemlidir. Siber alanda rahatsız edici zorluklara teknik çözümler bulunabilmektedir.

Üçüncüsü: Yeniden yapılanma: Eğer devlet saldırısını çabucak yenebilir ve sistemi yeniden başlatabilirse, etkiler asgari düzeyde kalacaktır (Cilluffo, et al. 2012).

2.3.5. Uluslararası Hukuka Göre Siber Saldırılardan Doğan Sorumluluk:

Hızlanan teknolojik gelişme, ülkelerin bir şekilde yüzleşmesi ve ele alması gereken birçok zor yasal soru ortaya çıkarmıştır. Bu sorunların en göze çarpanı, diğer ülkelerdeki elektronik sistemlerle çeşitli kurumlara saldırmak için elektronik teknolojik araçları kullanma yeteneğindeki hızlı büyümedir. Saldıran ülke herhangi bir açık ve beyan edilmiş askeri davranış sergilemeden ve hücumu gerçekleştirmek için askeri parçalardan herhangi birini kullanmadan başka devletlere zarar vermektedir.

Alışılmış olduğu gibi, siber saldırıları genellikle hedef saptamak ve onlardan kimin sorumlu olduğunu belirlemek için fail ve kaynak arama operasyonları izlemektedir, zira ülkeler tehlikenin siber uzaydan gelebileceğini algılamaktadır.

Birçok devlet yetkilileri, bir "siber" saldırının terörist bir eylem olduğunu ya da geniş çaplı bir silahlı saldırıya eşdeğer olduğunu ve realitenin siber saldırıların kurban sayısında, değişen derecelerde şiddet ve zarar olduğunu kanıtladığını düşünmektedir.

Saldırgan veya savunmacı olması fark etmeksizin her ülke, siber alanda askeri yeteneklerini geliştirmek için çalışmaya başlamıştır. Hava, uzay, kara ve deniz gibi savaşlarda bu mecra siber silahlarla kapsamlı maddi hasara neden olabilen bir alan olarak değerlendirilmiştir. Bahsedilen teknoloji aynı zamanda elektronik ağı, askeri operasyonları yürütmek için bir çıkış noktası olarak kullanılabilmektedir. Günümüzde ülkeler, siber saldırılara ve elektronik savaşlara uygulanması gereken kanunun tanımlanmasıyla ilgilenmektedir.

Birçok ülke ulusal ve uluslararası düzeyde girişimler benimsemiştir, örneğin Avrupa Birliği 2013 yılında siber güvenliğin özel boyutuna odaklanan "Siber Güvenlik Stratejisi ve Rehberlik Projesi"ni esas almış, Avrupa Birliği siber suçla ilgili çabalarını yoğunlaştırmıştır. Siber alanda en başarılı girişim 95 yasal madde ve 282 sayfa içeren Tallinn El Kitabı'nda sunulan girişimdir. Talinn El Kitabı, uluslararası insancıl hukukun elektronik savaş için geçerli olduğunu ve uluslararası insancıl hukuk kurallarının bu alanda oynayacağı rolü tanımlar(Jensen 2016).

Elektronik savaşlar ve çevrimiçi katılım kurallarının düzenlenmesinde geçerli olan uluslararası yasaları içeren bu rehber iki bölüme ayrılmıştır: birincisi elektronik güvenlikle, ikincisi elektronik uyuşmazlıklarla ilgilidir.

Tallinn Rehberi, elektronik işlemlerin koşullara göre, özellikle de bu işlemlerin zararlı etkilerine bağlı olarak silahlı çatışma oluşturabileceğini kabul etmektedir. Siber uzayda silah kullanma süreci, atakları çoğaltma kolaylığı ve hayati altyapı ve ekonomik, finansal, siyasi ve askeri kurumlar gibi hazır hedefleri elektronik olarak etkileme yeteneği ile karakterizedir.

Elektronik savaşlar aracılık/vasıtalar yoluyla ortaya çıkabilir: örneğin, askeri eylemlerde uzmanlaşmış kuruluşlar bilgi ve güvenlik hizmetlerini bazı kurum ve devletlere satmaktadır(Schmitt and Vihul 2014). Savaşta siber alan kullanımı, silahlı

çatışma yasalarını altüst etmiştir. Çünkü internet çoğunlukla askeri bir ağ olarak kullanılmamaktadır, sivil bir ağdır ve yalnızca askeri güçleri değil, sivil nüfusu da etkileyecek ve geleneksel sınırları tanımayacaktır.

Siber uzay, ulusal sınırları geçersiz/düşünsel kılmaktadır, çünkü ağlar arasındaki etkileşimler, sivilleri ciddi tehlikelere maruz bırakan çok sayıda elektronik silahın geliştirilmesi ve ortaya çıkması ışığında sınırları siber saldırıları önleyememiştir. Genel olarak, sanal alanın düzenlenmesinde devletin kontrolünü kaybetmesi şaşırtıcı değildir.

Modern tarih boyunca, silahlı çatışmaların uluslararası yasaları, savaşların dehşetine ve onların yeni yollarına yanıt olarak güncellenmiştir, yenilenmeye daimi/acil bir ihtiyaç vardır. Çünkü elektronik harp eylemleri muhtemelen mevcut silahlı çatışma yasalarının birçok hükmünün ihlaline yol açmaktadır, bu yasaların kapsamı dışında kalmaktadır(Maogoto and Freeland 2007).

2.3.6. Siber Savaşın Hukuki Niteliği ve Elektronik Savaşların Uluslararası Hukuka Tabiiyeti:

Uluslararası insancıl hukuk kurallarını siber savaşa uygulama olasılığının araştırılması, bu konunun savaşın meşruiyeti ve gayri meşruiyeti açısından değerlendirilmesi, hukuka uyarlanması gerektirmektedir. Dolayısıyla uluslararası ilişkilerde güç kullanımı ışığında siber gücün etkisinin araştırılmasına ihtiyaç bulunmaktadır.

Çağdaş uluslararası hukuk normları, devletlerin veya grupların kendilerini savunma hakkı dışında veya Güvenlik Konseyi tarafından alınan kolluk tedbirlerinin uygulanması haricinde güç kullanımını yasaklamaktadır. Savaş yasası, askeri operasyonların yürütülmesine açık kısıtlamalar getirmekte ve onun gereklerini insanlık yasalarıyla bağdaştırmayı amaçlamaktadır.

Uluslararası ilişkilerde güç kullanımı, Birleşmiş Milletler Antlaşmasına göre, yasadışı bir eylemdir: “Tüm üyeler, uluslararası ilişkilerinde gerek herhangi bir başka devletin toprak bütünlüğüne ya da siyasal bağımsızlığa karşı, gerek Birleşmiş Milletler’in Amaçları ile bağdaşmayacak herhangi bir biçimde kuvvet kullanma tehdidine

ya da kuvvet kullanılmasına başvurmaktan kaçınırlar."(Schmitt 1998) Güç terimiyle devletlerin saldırganlık veya silahlı saldırı çerçevesinde yalnızca silahlı kuvvetlere başvurması mı yoksa ekonomik abluka, siyasi baskı ve hatta siber saldırılar gibi diğer türleri de içerip içermediği ele alınmalıdır.

Gerçek şu ki, teknolojik gelişme nedeniyle devletin tüm bu olasılıklara sahip olması durumunda saldırıya uğrayan devletin "bu tür bir saldırı ile başa çıkmak için elektronik yasal seçenekleri" olup olmadığı tartışılmaktadır. Bu soruyu cevaplamanın önemi, elektronik saldırının kendisinin ayrı bir nitelikte olmasından ve alışılmış hareketliliğin dışında olmak ile karakterize edilmesinden kaynaklanmaktadır.

Uluslararası hukuk kuralları ışığında elektronik saldırılardan kaynaklanan kendini savunma hakkı, ilgili uluslararası anlaşmalar imzaladıklarında devletlerin algısı dışındaydı. Özellikle, Birleşmiş Milletler Antlaşması 51. Maddede ve Kuzey Atlantik Paktı Antlaşması'nın 5. Maddesinde kendini savunma hakkında bu konu değerlendirilmemiştir. Birleşmiş Antlaşması'nın 2/4 ve 51. (Jackson 2016)Maddelerinin elektronik saldırılara uygulanabilirliği tartışılmalıdır:

1) Birleşmiş Milletler Antlaşması'nın 2/4 ve 51. Maddelerinin elektronik saldırılara uygulanabilirliğini ortaya koymak amacıyla iki temel soruya cevap verilmelidir:

Birincisi: Elektronik saldırılar, Birleşmiş Milletler Anlaşması'nın "başka bir ülkenin toprak bütünlüğüne karşı güç kullanımı veya tehdidi belirten" Madde 2/4 'ü ihlal edebilir mi?

İkincisi: Bir elektronik saldırının Birleşmiş Milletler Antlaşması'nın 51. Maddesinde öngörülen (silahlı saldırı) seviyesine ulaşması mümkün müdür? Askeri agresif devlete uygulanmasında olduğu gibi, ülkeye saldırı kendini savunma hakkı verir mi? Uluslararası antlaşmaların veya normların içeriğinde bu sorulara net bir cevap olmaması dikkat çekicidir. Uluslararası Adalet Divanı'nın kararlarını incelerken, uluslararası hukukta devletin egemenliği ile ilgili bazı hükümler bulunduğu görülmektedir. Tallinn El Kitabında sunulan bazı maddeler yoluyla, elektronik saldırılar konusundaki uluslararası hukukun konumunu bilmek ve anlamak mümkündür.

Örneğin, Uluslararası Adalet Divanı, 1986 yılında Uluslararası Adalet Divanı'na getirilen ABD aleyhindeki Nikaragua Davası'nı ele almıştır, Nikaragua'daki limanları bombalayarak Nikaragua hükümetine karşı savaşta silahlı muhalefeti destekleyen ABD'nin tavrının uluslararası hukuka aykırı olduğunu kabul etmiştir. Mahkeme, kararında Birleşmiş Milletler Şartı'nın 2/4 maddesinin uygulanmasına iki açıdan atıfta bulunmuştur. İlk açı maddenin niteliğine ilişkindir, kararının 187. paragrafında, güç kullanımını veya kullanım tehdidini yasaklama ilkesinin tüm devletlerin uyması gereken uluslararası bir kural olduğunu belirtmiştir(Kahn 1987).

İkinci açı ise şudur: Mahkeme kararında kapsayıcılık ilkesini kabul etmiştir ve güç kullanımını yasaklama ilkesi, devlet sınırları dışında ordu kullanımı ile temsil edilen geleneksel güçle sınırlı değildir. Düzenli veya düzensiz gruplar ya da diğer araçlar olması fark etmeksizin devlet tarafından ya da devlet adına kuvvetler göndermenin, Bireşmiş Milletler Antlaşması'nın 2/4 maddesine aykırı/muhalif olduğunu teyit etmiştir(Lieverman 1986).

Bu tür bir davranışla karşılaşan ülke, kuvvet kullanımının boyutuna ve etkisine dayanarak Antlaşma'nın 51. Maddesi hükümlerine göre silahlı saldırı hazırlayabilir. Burada mahkeme, üye ülkeler arasında güç kullanımının Uluslararası Antlaşma'nın ihlali olduğunu açıklamıştır. Mahkeme kararı, devletin, kendi toprakları dışındaki diğer üyelere zarar verebilecek doğrudan ve dolaylı suiistimal ve uygulamalara karşı sorumluluğunu vurgulamıştır.

Mahkemenin ilgili kararı siber saldırılara dair bir hüküm olmasa da, bir ülkenin geleneksel güç modellerinin kullanımından kaynaklanan hasara benzeyen bir kayba yol açan etkili siber saldırılara maruz kaldığını iddia etmesi durumunda çeşitli davalara uygulanabilecek bir temel anlamındadır.

Tallinn Rehberi'nde 11. maddede böylesi bir çıkarımı desteklemektedir:

"Elektronik işlemlerin, seviyeleri ve etkileri elektronik olmayan işlemlere yakın olduğunda güç kullanımı olarak kabul edilir."

Bu kılavuzu/rehberi hazırlayan kanun uzmanları ve hukukçular grubu, elektronik saldırının, Birleşmiş Milletler Antlaşması'nın 2/4 Maddesi bakımından gereksiz/ bir silahlı saldırı veya yasa dışı bir güç kullanımı anlamına gelip gelmeyeceğine ilişkin Ölçek ve Etki (Scale and Effect) kriterine dayandıklarını söylemektedir(Williams 2012).

Bahsedilenler, saldırıya uğramış devletin Antlaşma'nın 51. maddesi uyarınca kendisini savunmasını haklı çıkarmaktadır. Ancak bir tür güç kullanımı olarak kabul edilen (daha tehlikeli) eylemler ile bu hakkın uygulanmasına izin vermeyen (daha az tehlikeli) eylemler arasında ayrım yaptığı için, mahkeme tarafından kararını verirken kabul edilen ölçütü (boyut ve etki) açıklığa kavuşturmak zorundayız. Daha tehlikeli ve daha az tehlikeli fiiller arasında kesin bir sınır olmadığı dile getirilmektedir. Bu madde, meydana gelen bazı orta düzey siber suçlarla ilgili davalarda uluslararası tahkim sorununu karmaşıklaştırabilir. Daha az tehlikeli ve daha tehlikeli işlerin niteliğini tespit etmeyi zorlaştırabilir(Pax 1985).

2.3.7. Uluslararası Hukuk Kuralları Işığında Siber Savaşlar:

Savaş zamanlarında uygulanan yasa olan uluslararası insancıl hukuk, bu çatışmaların uluslararası veya uluslararası olmayan nitelikte olup olmadığı, uluslararası insancıl hukukun ilke ve kurallarının siber işlemlere ne ölçüde uygulanabileceği ve bu yasa kurallarının tutarlılığının ve siber operasyonlara uygulanabilirliğinin ne kadar yaygın olduğu hakkında bilgi gerektirir. Bu hukukun ilkeleri siber saldırılara ne kadar uygulanabilir olduğunu açıklığa kavuşturmamızı sağlar. Söz konusu ilkelerin en önemlileri şunlardır:

1. Kapsayıcılık:

Uluslararası insancıl hukuk kurallarının özellikle siber operasyonlara atıfta bulunmadığını kabul edersek, bu yasada belirli referansların bulunmaması, bahsedilen operasyonların, tüm savaş yöntemlerini ve yöntemlerini düzenleyen genel kuralları aracılığıyla uluslararası insancıl hukuk kurallarına tabi olmadığı anlamına gelmez. Çünkü silahların kullanımını barındırmaktadır. Bu hususta dört sözleşme olan Cenevre Sözleşmeleri'nin 1977 tarihli 1. Ek Protokolün içeriğine başvurulabilir.

“Herhangi bir yüksek sözleşmeci taraf, yeni bir silahı veya savaş aracını incelerken, geliştirirken veya edinirken veya yeni bir savaş yöntemi benimserken, bunun tüm durumlarda veya bazı durumlarda bu ek nedeniyle yasaklandığını araştırmakla yükümlüdür.” Yüksek Sözleşmeci Taraf, yeni silahın bağlı olduğu diğer uluslararası hukuk kurallarına uyup uymadığını soruşturmakla yükümlüdür(Kellenberger 2011).

Yukarıdaki metne göre, eğer teknolojik bir savaş silahı, bir araç ya da yöntem olarak uyarlanmışsa, taraflar kullanımlarının yasallığını protokolün kurallarına ya da herhangi bir uluslararası hukuk kuralına uygun olarak doğrulanmalıdır.

Ayrıca siber savaş için ne kadar sürede uygulanabileceği uluslararası insancıl hukukun temel ilkeleri esas alınmalıdır. Bu ilkelerin belki de en önemlisi Martenz/Martens koşuludur. 1899 ve 1907 tarihli 4. Lahey Sözleşmesinin önsözünde yer alan ve daha sonra 1977’nin ilk ek protokolünün metnine ve II. Protokolün önsözüne giren bu madde, şunları öngörmektedir: “Belirli bir antlaşma hukuku kuralının yokluğunda, savaşçılar, geleneksel hukuka, insanlığın ilkeleri ve kamu vicdanının emirlerine tabidir(Ticehurst 1997).”

Önceki metinde geçen (insanlığın ilkeleri ve kamu vicdanının belirlediği şey) ifadesi, tartışmalı bir konuyu gündeme getirmekte midir? Yoksa yalnızca bağlayıcı olmayan ahlaki ilkeler mi kastedilmektedir? Bu bağlamda Uluslararası Adalet Divanı tarafından nükleer silahların tehdidi veya kullanımının yasallığı konusunda yayınlanan karara atıfta bulunmak yerinde olacaktır. Çünkü mahkeme, devam eden varlığı ve uygulanabilirliği hakkında şüphe edilemeyen Martenz maddesinin önemini ve onun askeri teknolojinin hızlı gelişimine karşı etkili bir yol olduğunu vurgulamıştır.

1948’deki Krupp davasındaki Birleşik Devletler Askeri Mahkemesi’nin kararında belirtilenler Martens/Martenz koşulunun yasal bir ilkenin açıklanmasından daha fazlası olduğunu göstermektedir. İlgili koşul, uygar ulusların istikrarlı alışkanlıklarını kamu vicdanının belirlediği, (yasal standartların) veya (yasal dayanağın) bir parçası olan kılmasıdır. Anlaşma hükümlerinin belirli davaları kapsamadığı durumlarda bu koşul tatbik edilmelidir. Burada, insani standartların ihlaline eşlik eden hu-

susların Martenz şartların oluşturulduğu zamankinden daha ileri düzeyde olabileceğini belirtmek isteriz.

Bu koşulu savunanlar, uluslararası antlaşma ve örfte/geleneklerde yasaklanmayan hususların insanilik ilkesi ve kamu vicdanına aykırı olması halinde serbest olmayacağını belirtmişlerdir. Martenz ilkesi, kanuni kısıtlama içermektedir, kanun boşluklarından kaynaklanan suiistimallerin önüne geçilmesi için başvurulan bir esastır(Meron 2006).

2- Rastgele Yapılan Saldırıları Yasaklama İlkesi:

Rastgele saldırılar: Belirli bir askeri hedefe yönelik olmayan ya da bir mücadele yöntemi ya da ayrım gözetmeyen saldırılar biçiminde tanımlanabilir. Etkileri uluslararası insancıl hukukun gerektirdiği şekilde belirlenemediğinden, belirli bir askeri hedefe yönlendirilemez. Böylesi bir atak, her bir durumda, ayrımcılık yapmadan askeri veya sivil hedeflere ve sivillere zarar vermektedir.

Beklenen biçimde ya da tesadüfen sivil hayatın kaybına, kendilerine zarar vermesine ya da sivil tesis ve yapıların zarar görmesine neden olabilecek her saldırıyı yasaklar ya da bu kayıp ve zararların bir kombinasyonuna neden olabilir. Algılanan faydayı veya doğrudan askeri avantajı büyük ölçüde aşar ve buna orantılılık ilkesi denir. Bu ilke, temelini uluslararası ve uluslararası olmayan silahlı çatışmalarda uygulanan geleneksel uluslararası insancıl hukuk kurallarında da bulur(Tanizawa, et al. 2005).

3- Askeri gereklilik ilkesi: Yalnızca düşmanın tamamen veya kısmen boyun eğdirilmesi için silahlı çatışmanın amaçlanan meşru hedefine ulaşmak üzere gerekli olan güç türünün ve derecesinin kullanılmasına izin verir. Bu ilkeye göre, savaşın gerekleri büyük bir yıkımı ve ele geçirmeyi dayatmadıkça, bu bağlamda düşmana ait varlıkları tamamen imha etme ya da ele geçirme politikası güdülmemelidir. “Askeri gereklilik, bir devletin, savaş hukuku kurallarına uymak kaydıyla, düşmanının teslim olmasını sağlamasıdır. Bunu yaparken can, mal, zaman ve para kaybını minimum seviyede tutulmasını ön görmektedir(Carnahan 1998).”

4- İnsancıllık/ İnsanilik ilkesi: Gereksiz acı veya zarara yol açmayı yasaklandığı için askeri zorunluluk ilkesini tamamlayıcı unsur olarak değerlendirilmektedir ve ona dâhil edildiği için genel bir ilkedir. Bu ilke, başka bir uluslararası hukuk kuralı tarafından kullanılması menedilmemiş savaş araçlarına veya yöntemlerine başvurmayı yasaklamaktadır.

İnsanların, herhangi bir silahlı çatışmaya taraf olmalarının, savaş yöntemlerini ve araçlarını seçme hakkının, kısıtlı olmayan bir hak olmadığını ifade etmektedir. Gereksiz zayiat veya acıya neden olacak silah, mermi, malzeme ve savaş araçlarının kullanımının yasaklanmasının zorunlu olduğunu belirtmektedir. Yukarıdaki bilgiler aracılığıyla söz konusu ilke ve kuralların sadece teknik ve teknolojik yönüyle mevcut savaş araç ve yöntemleriyle sınırlı olmadığı, gelecekte yeni bir silahın veya yeni savaş yöntemlerinin veya savaş yöntemlerinin geliştirilmesi, edinilmesi veya benimsenmesi için geçerli oldukları söylenebilir.

Uluslararası insancıl hukukun ilke ve kurallarının evrenselliği siber saldırıların özgünlüğü ve uluslararası insancıl hukukun ilke ve kurallarının onun üzerindeki etkisi, yaklaşık yüz elli yıl önce orijinal Cenevre Konvansiyonu'nun benimsenmesinden bu yana savaşların doğasında meydana gelen değişiklikleri göz ardı ederek değerlendirilemez. Savaş araçları ve yöntemleri, bu anlaşmanın çerçevelerinin hayal bile edemeyeceği derecede geliştirilmiştir. Belki de siber uzayın askeri amaçlarla kullanımı, silahlı çatışmaların yürütülmesini düzenleyen kuralları gözden geçirmek ve bu kullanımların doğası ile orantılı bir şekilde formüle etmek için en önemli nedenlerden biri olabilir(Hathaway, et al. 2012).

Siber Saldırılardan Kaynaklanan Uluslararası Sorumluluklar:

Başlangıçta, söz konusu ülkeye atfedilen yanlış fiilden bağımsız olarak, İngilizce dışındaki dillerde "devlet sorumluluğu" ve "uluslararası sorumluluk" arasında ayrım yapmada dilsel bir eksiklik olduğunu belirtmeliyiz.

"Devlet sorumluluğu" genel olarak uluslararası hukuk kapsamında bir ülkenin sorumluluğunu, "uluslararası sorumluluk" ise "medeni/sivil sorumluluk" veya yükümlülüğü ifade eder. Devlet tarafından kendi kontrolü dâhilindeki veya altındaki

faaliyetler nedeniyle ulusal sınırlarının dışında kalan vatandaş olmayan kişilere tazminat ödenebilmektedir. Dolayısıyla bu iki kavram arasındaki bağ, uluslararası hukuk kapsamındaki yargılama veya kontrol çerçevesindeki faaliyetlerin diğer ülkeleri veya onların vatandaşlarını etkileyen zararlı sonuçları hakkında bir ülkenin devlet sorumluluğu ile devletlerin uluslararası sorumluluğu arasındaki ilişkiyi yansıtmaktadır (Sucharitkul, 1995).

Son zamanlarda, bir devlete veya siber saldırı suçlamalarının atfedildiği bir grup devlet dışı aktöre karşı uluslararası sorumluluğu yöneltme olasılığını tartışmak için birçok özel yasal çalışması yapılmıştır.

Siber saldırılardan kaynaklanan uluslararası sorumluluğun boyutlarını belirlemek için, uluslararası sorumluluk kavramını, uluslararası mahkemelerin kararları gibi çağdaş uluslararası mercilerin yanı sıra genel uluslararası hukuk uzmanlarının görüş ve yorumları ışığında irdelemek lazımdır.

Uluslararası hukukta uluslararası sorumluluğun kurucu unsurlarında olduğu kadar, hiçbir şey üzerinde bu kadar farklı görüş bildirilmemiştir, bazı hukukçular, uluslararası sorumluluğu oluşturan unsurlar da dâhil olmak üzere, uluslararası sorumluluk bağlamında özgün bir terminoloji geliştirmişlerdir.

Uluslararası hukukta sorumluluğun temel dayanaklarının sayısı konusunda ittifak yoktur, iki veya üç oldukları söylenmektedir. Onları zararlı eylemle ve zararlı eylemin uluslararası hukuktaki bir kişiye atfedilmesi ile sınırlayanlar bulunmaktadır(Shackelford and Andres 2010).

Bu bağlamda, uluslararası sorumluluğun temel dayanakları ve etkileri şu şekilde ele alınabilir:

Uluslararası yasal sorumluluk unsurlarının bir sonucu olarak, uluslararası sorumluluğun varlığını belirtmek gerekir. Bu noktada üç unsur vardır: İlk unsur: uluslararası hukukun “zararlı fiil” sorumluluğunu verdiği bir fiil, İkinci unsur: fiilin uluslararası veya örgütlü uluslararası kamu hukuku açısından değerlendirilmesi, Üçüncü

unsur: uluslararası hukuka aykırı davranan bir kimsenin/failin haksız fiil sonucu zararı

Uluslararası sorumluluk konusu, hata teorilerinin yanı sıra nesnel/realist teorinin sunulmasından başlayarak ve Uluslararası Hukuk Komisyonu'nun yanlış eylemler için uluslararası sorumluluk taslağı hazırlamasıyla temsil edilen çağdaş uluslararası organizasyonun katkılarıyla sona eren çeşitli değişkenlere ve gelişmelere maruz kalmıştır(Amador, et al. 1974).

Siber saldırılar konusunda uluslararası sorumluluk kavramını açıklığa kavuşturan 2001 tarihli Yasadışı Hareketlere Karşı Uluslararası Sorumluluk Taslağı ve özellikle de 1. maddesi incelenmelidir: "Uluslararası düzeyde yanlış sayılan her fiilden devletin sorumluluğu doğmaktadır."

Davranışın teamül veya antlaşma yasasına aykırı olduğu tespit edilmedikçe, uluslararası sorumluluğun tesis edilemeyeceğini söylemek doğrudur. Ancak bir davranışın zararlı ya da faydalı olarak belirtilmesi önem kazanmaktadır.

2001 yılında yasadışı durumlar için hazırlanan Uluslararası Sorumluluk taslağının 1. Maddesinin gözden geçirilmesi neticesinde, uluslararası sorumluluğun yüklenmesi için bir zararın ortaya çıkması koşulunun gerekmediği anlaşılmaktadır. Madde- 1. 'de bahsedilen kavram, uluslararası hukukun oluşturulmasında zarar unsurunun elde edilmesini öngören yaklaşımdan farklıdır.

Uluslararası beşeri hukuk, siber saldırılardan kaynaklanan uluslararası sorumluluğu şu şekilde ele almaktadır:

Uluslararası geleneksel anlaşma ve kuralların hükümlerinin, eylemin/fiilin resmi ya da yarı resmi devlet kurumları tarafından işlenip işlenmediğini gözeterek, devletlerin 3. Maddede atıfta bulunulan eylemleri kontrol edebilmeleri koşuluyla, devlete ait olan sorumluluğu açıkça tanımladığı bilinmektedir. 1907'de değiştirildiği şekliyle 1899 Kara Savaşı ile ilgili Lahey Konvansiyonu şöyle demektedir:

Yukarıda bahsi geçen yönetmelik hükümlerini ihlal eden savaşan tarafı, ihtiyaç duyulması halinde tazminat ödemekle yükümlü tutar ve ayrıca silahlı kuvvetlerine mensup kişilerin yaptığı tüm suç unsurlarından da sorumlu tutar(Bos 2005).

Siber saldırılardan kaynaklanan uluslararası sorumluluğa yakından bakıldığında, bunların bir koşuldan diğerine farklılık gösterdiği kavranmaktadır. Siber saldırı, silahlı çatışma sırasında askeri veya sivil iletişim araçlarını aksatmaya odaklanmışsa, konu sadece uluslararası insancıl hukuk hükümlerine ve özellikle savaşçıların eylemlerini kontrol eden hükümlere tabidir. Askeri operasyon yöntemleri ve uluslararası normlar/teamüller düşmanlıkların ortaya çıkmasından önce savaş ilan etme zorunluluğunu benimsediğinden, bu operasyonların deklare edilmeden gerçekleşmesi, koşullar bunu elverirse bir savaş durumu yaratabilir. “

Yukarıdakilerden hareketle, siber saldırılar silahlı çatışma sırasında bir antlaşmayı veya geleneksel bir uluslararası kuralı ihlal ettiğinde, bu etki için uluslararası sorumluluğun düşmanlıkların/saldırıların yürütülmesini düzenleyen uluslararası ilkeler kapsamında olacağı sonucuna ulaşılmaktadır. Uluslararası insancıl hukuk kuralları yalnızca silahlı çatışmalar bağlamında geçerlidir ve çatışmanın taraflarına belirli kısıtlamalar getirir. Bu nedenle, "siber savaş" terimi, yalnızca UST anlamında bir silahlı çatışma bağlamında gerçekleştirilen veya bununla ilgili siber operasyonlardan oluşan savaş araçlarına ve yöntemlerine atıfta bulunacaktır(Droege 2012).

Bir çatışmaya taraf olanların savaş araçlarını ve yöntemlerini seçme hakkının mutlak bir hak olmadığı, diğer uluslararası ilkelerin da devrede tutulmasının zorunlu olduğu anlaşılmaktadır:

- Sivillerin ve savaşçıların ayırt edilmesi ilkesi,
- Gereksiz yaralanma, rastgele etkiler veya haksız acı ilkesi,
- Askeri gereklilik ilkesi,
- Kuvvet kullanımında orantılılık ilkesi,
- Martenz Koşulu Prensibi.

İkinci hal, başka devletlerin içindeki silahlı gruplarla casusluk yapmak ve iletişim kurmak gibi yollarda bir barış durumunda siber saldırılar yapmaktır. Bu durum-

da, uluslararası sorumluluk, devletlerin iç işlerine karışmanın kabul edilemezliği ilkesinin ihlaline dayanmaktadır. Müdahaledeki rolünden ötürü devletin sorumluluğunun belirlenmesi iki yasa tarafından düzenlenmektedir: Bunlardan birincisi, Uluslararası Hukuk Komisyonu Taslağı'nda 4. Maddesi'dir, devletin hatalı uluslararası eylemler için sorumluluğuna değinmektedir, ikincisi unsur, 8. Maddesi'dir, devletin eylemleri ve onun kontrol ettiği grupların çalışmaları ile ilgili sorumluluğuna temas etmektedir (Shackelford and Andres 2010).

Yukarıda bahsedilen maddelerin analizinden şu husus anlaşılmaktadır: Sorumluluk, devletin yürütme, yasama veya yargı organlarından birine yanlış davranış atfedildiğinde ve başka bir ülkenin çıkarlarına veya vatandaşlarından birine karşı zarar verildiğinde belirlenir. Kontrol ölçütü ve devlet kurumlarının, çalışanlarından birinin veya desteklediği silahlı grupların eylemlerini kontrol etme yeteneği, uluslararası sorumluluğun mobilize edilebileceği temeli temsil eder. Ancak, kontrol ölçütlerine ulaşılıp ulaşılmadığını araştırmak ve doğrulamak yetkili mahkemelere bırakılmıştır.

Toplu ve bireysel güvenlik operasyonlarıyla kısmen alınan tedbirler de dâhil olmak üzere belirli durumlar haricinde uluslararası ilişkilerde güç kullanılması ile ilgili alınan tedbirler, devletlerin ulusal güvenliğine karşı olası saldırı durumunda kendilerini savunma aracı olarak kabul edilmektedir. Siber saldırılar konusu ve zorluklarla mücadele, yasal listelerde ele alınmamıştır. Bu kanun maddesi, bir takım göze çarpan sorunların alternatif çözümlerini içeren ana sorunları tartışmasına rağmen, sonunda belirlenmesi gereken açık ve yasal yönergeler sunamamıştır.

Bu nedenle, elektronik saldırılara karşı mücadele ile ilgili düzenleme içeren yasal usul ve ilkelerin, taraf devletlerin uluslararası ilişkilerinde, Birleşmiş Milletler' in amaç ve ilkeleri dışına çıkarak farklı bir tutumla bir ülkenin toprak bütünlüğüne ve siyasi bağımsızlığına karşı güç kullanılmasını engellemesi gerektiğini görmekteyiz (Hathaway, et al. 2012).

Devletin herhangi bir alanda istikrarını tehdit eden her durum, devlete karşı yapılan bir silahlı saldırı olarak görülmelidir. Bu şekilde görüldüğü takdirde o zaman

siber saldırıların sadece bir ülkenin değil, tüm dünya ülkelerinin güvenlik ve istikrarı için bir tehdit unsuru olduğunu görebiliriz.

Siber saldırılar, sıradan bir saldırganlık olarak düşünülebilir. Ancak konunun önemini Birleşmiş Milletler sözleşmesinin 39. Maddesinde daha açıkça görebiliyoruz. Söz konusu maddede; "Güvenlik Konseyi, barış ve güvenliğe yönelik bir tehdit veya ihlal olup olmadığına ya da suçun bir saldırı eylemi olup olmadığına karar vererek bu konudaki tavsiyelerini yapar ve 41. ve 42. Maddelerin hükümleri uyarınca Uluslararası barış ve güvenliği korumak adına hangi önlemlerin alınması gerektiğine karar verir." (Happold 2003).

Siber saldırılar konusu, silahla yapılan saldırılardan daha tehlikeli olduğuna dair değerlendirilmeye başlanmıştır.

Bu nedenle, NATO siber saldırı tehdidini askeri saldırganlık düzeyine yükselterek siber saldırıları gerçek bir saldırı eylemi olarak görmektedir. Buna mukabil, Güvenlik Konseyi'nin uluslararası bir siber saldırıya karşı tedbirler almasını sağlayacak uluslararası pratik emsallerinin henüz olmadığını görüyoruz. Güvenlik Konseyi, kendisine sunulan gerçekleri uyarlarken izlenecek pratik bir kontrol mekanizması ya da belirli bir standart belirlememiş, takdir yetkilerine kısıtlamalar getirmekten de kaçınmıştır.

Güvenlik Konseyi'nin aldığı kararlar ışığında baktığımızda, en tehlikeli konunun (siber tehditlerin) uluslararası barışa ve güvenliğe karşı kaçınılmaz bir tehdit olduğunu görüyoruz. Bu durum belki şimdilik doğrudan siber saldırılarla uyuşmayabilir. Ancak uluslararası barış ve güvenliği ihlal etmekten bahsetmek istiyorsak, Siber saldırıların, başka bir uluslararası tarafın ilan ettiği uluslararası bir siber saldırının gerçekleşmesi yoluyla uluslararası barış ve güvenliği ihlal ettiği sonucuna bizi götüren bazı bağlantılar olduğunu görebiliriz. Bu tür saldırıların tehlikesi, özellikle bir uluslararası organizasyonu veya kuruluşu birkaç saniye içinde felce uğratması ve tahrip kapasitesinin devletlerin stratejik çıkarlarına saldırabilme boyutuna ulaşması ile ortaya çıkmaktadır(Hathaway, et al. 2012).

Siber saldırılarda yeni ve net bir saldırganlık eğilimini belirginleştirebilmemiz için, bu tür saldırılarda ortaya çıkan saldırganlığa daha fazla ışık tutmalıyız. Saldırı eyleminin bir siber saldırı olarak gerçekleştiğini gösteren bazı örnekler üzerinden gitmemiz gerekecektir. Örneğin, "Stuxnet" programı ile İran'a karşı yapılan bilgisayarın alt yapısını tahrip etme saldırısı, İran'ın siber saldırılara hedef ülkeler arasında ön planda olduğunu göstermektedir. İran'ın bilgisayar ağlarına yapılan saldırıda % 60 oranında hasar ve zarar tespit edilmiştir. İran örneğiyle, bir ülkenin son derece hassas ve tehlikeli olan bir saldırı türüyle, stratejik ve ekonomik açıdan önemli bir mekanizmayı hedefleyen ve önceden kurgulanmış bir siber saldırıya maruz kaldığını görmekteyiz(Farwell and Rohozinski 2011).

Bu örneği ele alıp değerlendirdiğimizde bir saldırganlık eylemiyle ilişkilendirmek istersek, uluslararası barış ve güvenliğin açıkça ihlal edildiğini görürüz. Bir tek kurşunun bile atılmadığı bir insani felakete ya da soykırıma yol açmasının hiçte uzak bir tehdit olmadığı anlaşılacaktır. Bu nedenle Güvenlik Konseyi'nde buna benzer tehlikeli saldırıların önlenmesini amaçlayan, acil müdahale ve uygun tedbirlerin alınması gerekmektedir.

Estonya devlet kurumlarının, gazetelerinin ve bankalarının web sitelerinin yok edildiği Estonya saldırıları buna bir örnektir. Gruplar halinde gerçekleştirilen siber saldırılar üç hafta sürmüş ve Estonya'yı kelimenin tam anlamıyla felç etmiştir. İnternet korsanları, hedef aldıkları web sitelerine aynı anda büyük miktarda bilgi göndererek, web sitelerinin aşırı yüklenmesine ve nihayetinde durdurulmasına neden olmuştur.

Bu örnekle, yine siber saldırılarla hedef tahtasına oturtulan bir devlete karşı yapılan saldırının şekli sanal da olsa, bilfiil savaş saldırısı gibi, belki daha da tehlikeli boyutta amacına ulaşabildiği sonucuna varıyoruz. Nitekim devletlerin alt yapısını, stratejik çıkarlarını bozmakta ve varlıklarını önemli ölçüde zayıflatmaktadır. Bu tür bir saldırganlık fiili, her ne kadar ülke topraklarını işgal edip siyasi bağımsızlığına son vermese de, yıkıcı boyutları ve zararları onu bazı durumlarda silahlı saldırıdan daha kötü hale getirmektedir (Shackelford 2009).

İkinci Bölümün Özeti:

Çalışmalarımızın bu bölümünde, siber tehditlerin değişen güç, savaş ve barış algıları üzerinde önemli bir etkisi olduğu sonucuna vardık. Küreselleşme çağının siber tehditlerin artışındaki etkileri ile bağlantılı olarak, siber tehditlerin uluslararası ilişkiler üzerindeki etkisinin yanı sıra, çoğu ülkenin yeni değişime uyum sağlamada güvenlik doktrinini geliştirmesine neden olan siber uzayın tehdit türlerine değindik. Öte yandan siber suçlar, terörizm ve siber uzayda güç yarışı, devletlerin karşı karşıya olduğu yeni güvenlik sorunları arasında yer aldığından, bütün bunların, hızla artan ve gelişen siber tehditlerle mücadele etme gerekliliğini ortaya koyduğunu vurguladık.

Bu nedenle ülkelerin ulusal güvenliklerini korumak ve siber tehditlerle mücadele etmek için iki yol üzerinde çalışmaları gerektiğine işaret ettik. Birincisi; teknik, siber orduların geliştirilmesi ve siber güvenlik organlarının oluşturulmasıdır. İkincisi ise siber suçlar ve siber terörizmle etkin bir mücadele için; ulusal, bölgesel ve uluslararası yasal mevzuatın çıkarılması gerektiğine değindik.

Çalışmamızın bu bölümünde bir dizi önemli sonuca ulaşılmıştır. Örneğin, çağımızda modern teknolojik mekanizmaların gelişimi ışığında elektronik tehditler, çeşitli alanlarda küresel güvenliğin karşı karşıya olduğu geleneksel güvenlik tehditlerinden daha az tehlikeli olmadığı vurgulanmıştır. Öte yandan güç dengesindeki değişimin bir sonucu olarak, yeni uluslararası çatışma modellerini vurgulamada, siber saldırıların etkisi üzerinde durmanın yanı sıra, siber uzayda caydırıcı stratejiler belirlenerek karşılaşılan zorluklara, tehdit ve tehlikelerin boyutuna değinerek siber saldırıları azaltmak için gerekli önlemlerin alınmasına değinilmiştir.

ÜÇÜNCÜ BÖLÜM

3. SİBER UZAYDA TERÖR VE RADİKALİZM

3.1. Terör Örgütlerinin Siber Terörünü Kullanmaları ve Gelişimi - Siber Terörizm (Cyberterrorism)

Yaşadığımız çağa kısaca "siber çağı" diyebiliriz. Küresel elektronik ağının gelişmesiyle dünyanın her yerinden geniş bir izleyici kitlesinin takibiyle iletişim ve diyaloğun kolay ve mümkün hale gelmesi, çağımızın çok önemli bir devrimi sayılmıştır.

İnternet, günlük yaşamda neredeyse bireyler, gruplar ve hatta devletler düzeyinde tüm faaliyetlerin belkemiğini oluşturmuştur. İnternet kullanımının kolay ve ucuz olması, çağımız insanının bireysel ve toplumsal temelde her kesimin, resmi ve gayrı resmi kurum ve kuruluşların internete etkin bir şekilde bağlı olmasına paralel, uluslararası güvenlik her düzeyde tehdit altında olmuştur. Terör örgütleri, dijital alanı, tehlikeli yasadışı veya saldırgan eylemleriyle etkileme ve kutuplaşma alanı olarak kullanmaya başlamıştır. Elektronik terör, internetteki en önemli yeni ve ciddi güvenlik tehdidi olarak gündeme oturmuştur (Askari, 2018: 275).

İnternet kullanımında büyük gelişmelerin yaşanması, savaş alanının elektronik ortama kaymasına ve sivillerin yüreğinde terör ve korku yaymada kullanılmasına neden olmuştur. Bilişim teknolojilerinin çok işlevli doğası nedeniyle, gelecekteki savaşlarda e-savaşın baskın yön olması beklenmektedir. Günümüzde terörist gruplar internet üzerinden siber saldırılar düzenlemektedir. Siber Terörizmin, terörist gruplar için giderek daha arzulanan bir taktik haline gelebileceği ve bu alanda her devletin hedef olabileceği endişesi ortaya çıkmıştır (Yusuf 2018).

Bugün siber saldırıların sayısında tanık olunan artışın, çoğu ülkenin temel altyapısındaki bilgisayar ve internet ağlarının sağlam bir koruma altına kaynaklandığı bir gerçektir. Sosyal iletişim ağlarının programlarına bilerek ya da bilmeyerek, kişisel ve kurumsal ağ bilgilerine erişim hakkının verilmesi ya da bu şirketlerin yasal zeminden çıkıp özel bilgileri üçüncü kişilerle paylaşıma açması, kişi, kurum veya

devletleri, hacker denilen bilgisayar korsanlarının siber saldırılarına açık hale getirmiştir.

Terörist saldırılar hedeften binlerce kilometre uzaktan başlatılabildiğinden, izlenebilmesi ve engellenebilmesi oldukça zor olmaktadır: Siber terörizmin potansiyel hedefleri, başta ülke ekonomisi, bankacılık endüstrisi, askeri tesisler, elektrik santralleri, hava trafik kontrol sistemleri, su sistemleri ve hedef ülkelerdeki vatandaşların yaşam seyrini etkili biçimde çökertebilen diğer hayati hedeflerdir. (Mallik 2004).

Siber Alanın Terörizm için Kullanımı ve Gelişimi - Siber Terörizm (Cyberterrorism)

Terör örgütlerinin Siber terörünü kendi emelleri doğrultusunda nasıl kullandıkları konusunu açıklığa kavuşturmak istiyorsak, bu konuyu net ve doğru bir şekilde anlayabilmek, analiz edebilmek ve anlayabilmek için öncelikle Elektronik Terörizm ya da Siber Terörizm kavramının tanımına atıfta bulunmamız gerekir.

Siber Terörizm terimi ilk olarak 1980'lerde Barry Collin tarafından tanıtılmıştır. Ancak zamanla sürekli şekil ve kapsam değişikliği nedeniyle kapsamlı bir tanım getirebilmenin zor olduğu sonucuna varmıştır. Bununla beraber tanımı çerçevesinde şunların altını çizmektedir: Hedef aldıkları devletleri, politik, dini veya ideolojik amaçların peşinde tehdit etmeye veya saldırmaya yöneliktir. Bir elektronik saldırının, siber terörü olarak değerlendirilebilmesi, terörizmin maddi eylemlerine eşdeğer yıkıcı ve tahrip etme etkisine sahip olması gerekir (Polse, 2009: 279).

ama Bu tanime terörizm salt bir aktöre haz bir eylem olarak kabul edilmiş ve hedef olarak da devlet gösterilmiştir. Oysa terör eylemleri bütün akörler tarafından kullanılmakta ve hedef genelde toplumdur. Toplumda korku yaratmaktadır.

Siber terörü tanımı ile ilgili belirli bir formül üzerinde bir fikir birliği olmadığı açıktır, ancak bu konuda belirli açıklamalar getiren tüm uzmanlar arasında ortak yaklaşımlar olduğu da bir gerçektir. Dorothy Denningg**,** siber terörizmin "bilgisayar saldırısına dayanan bir saldırı" olduğunu ve tehdidin siyasi, dini veya ideolojik hedeflere ulaşmaları için hükümetleri veya toplumları korkutmayı veya zorlamayı hedefle-

diğini savunmaktadır. Ona göre de saldırının terörizmin maddi eylemlerine benzer bir korku yaratması, yıkıcı ve tahrip edici olması lazımdır (Theohary, 2015: 280). **James Lewiss,** "Bir devletin enerji, ulaştırma, devlet işlemleri gibi önemli ulusal altyapılarını yok etmek veya bozmak, bir hükümeti indirmek veya sivillerin içine korku salmak için bilgisayar ağ araçlarının kullanılması" olarak tanımlamaktadır (Lewis 2002). Buna göre, Barış dönemlerinde Kritik altyapılara yönrlik saldırıar terör eylemi kabul edilir.

Siber güvenlik konusunda uzman bir Arap araştırmacı olan Dr. Adel Abdel-Sadiq ise, "Devletler, gruplar veya bireyler tarafından elektronik araçların kullanılmasıyla gerçekleştirilen ve soyut ya da somut sonuçlar getiren her türlü saldırganlık, tehdit, korku veya boyun eğdirilmek için böyle bir saldırganlığın hedefi olmaktır". Şeklinde yaklaşımda bulunmaktadır (Abdul Sadiq 2009).

ABD Savunma Bakanlığı, bu kavramın tanımını veren en önemli kurumlardan biri olmuştur. Elektronik terörizmi; "belirli bir politik, sosyal veya entelektüel çıkar için herhangi bir hükümeti veya milleti ciddi bir karışıklık ve belirsizliğe yol açacak şekilde etkilemek amacıyla, bilgisayar teknolojisi ve sosyal iletişim ağları kullanılarak hazırlanan, şiddet, korku ve yıkım eylemlerinin gerçekleştirildiği bir suç mekanizması" olarak tanımlamıştır. NATO da aynı doğrultuda bir tanımla; "Bilgisayar ağları veya iletişim araçları kullanılarak, ideolojik bir amaç doğrultusunda bir toplumu terörize edecek, korku yaratacak ve yıkımlara neden olacak her tür internet saldırısıdır." şeklinde konunun önemine dikkat çekmiştir(Gordon, 2002: 267).

Vermiş olduğumuz tanımlamalar ışığında "elektronik terörizmi" kısaca, "yasadışı saldırılar "şeklinde tanımlamak mümkündür. Başka bir ifadeyle, "hükümetleri, halkları ve hatta tüm uluslararası toplumu elektronik araçlarla siyasi, dini veya sosyal hedeflere ulaşmak için misilleme ve şantaj yöntemiyle zorlama ya da etki altına alarak bilgisayarlara, ağlara ve depolanan bilgilere yönelik saldırı ve tehditlerdir."

Bir kişinin terörist olarak kabul edilebilmesi için, başlattığı saldırıların kişilere, toplumlara veya belirli kurumlara yönelik şiddete yol açması gerekir. Bu bağlamda siber uzayı kötüye kullanarak birbirlerini veya belirli toplumları hedef alan tüm

aktörlerin, terör eylemlerini gerçekleştirebileceği ihtimali de göz ardı edilmemelidir. Nitekim elektronik terörizme işaret edilerek, terörü insanların ruhuna yaymaya çalışan ve toplumları hedef alan her türlü terörizmin önlenmesi gerektiği vurgulanmıştır.(Najeeb bin Omar 2017)

3.1.1. Siber Uzayın Terör amaçlı Kullanım Alanları

Terörizm modern bir terimdir. Uluslararası toplumda bir zorlama aracı olarak kabul edilmiştir. Terörist eylemler, ne evrensel olarak ne de yasal olarak çerçevesi çizilmiş belirli hedeflere sahiptir. Ancak terörizmin genel tanımlarına ek olarak ceza hukuku kapsamında şekillenen suçlar çerçevesinde kendini göstermiştir. Buna göre; belirli bir dinin mensuplarına ya da bir ülkeye veya topluma topyekûn ya da toplum içerisindeki etnik gruplara karşı politik ya da ideolojik hedefler taşıyan, korku atmosferi yaratmaya yönelik şiddet eylemleri içeren hareketlerdir. Bu amaçla güvenliğin kasıtlı olarak hedeflenmesi veya göz ardı edilmesi söz konusudur. Günümüzde son olarak yapılan bazı tanımlarda ise, "yasadışı şiddet ve savaş eylemleri" kapsamında değerlendirilmiş ve altı çizilmiştir (Merari, 1993: 288).

Siyasi ve dini karmaşıklıklar nedeniyle, bu kavramın tanımı kimi zaman belirsiz ve farklı hale gelmiştir. Hristiyanların aşırılık yanlısı bazı grupların hedefi olmaları nedeniyle zaman zaman mağdur oldukları, İslam âlemi de günümüzde uluslararası politik nedenlerden dolayı, bölgesel çatışmalarla boy gösteren çalkantılar sonucu maalesef bu terimden nasibini almıştır. Filistin'de, İsrail güvenlik servislerinden elde edilen verilere göre, Yahudi terörist çetelerin "Siyonist Telâl Gençlik Örgütü" son yıllarda işlediği nefret suçlarında önemli bir artış göstermiştir. 2018'de işgal altındaki Batı Şeria'da önce Duabsha ailesinin evini yakıp ailesini yangında ölüme terk etmişlerdir. Aynı radikal Siyonist örgütü, 16 Haziran 2014 tarihinde Taberiye (Tiberias) Gölü'nün kuzeyinde Galile (Celile) kenti yakınlarında bulunan "Multiplication of the Loaves and Fishes" (Somun ve Balık Çoğalımı) kilisesini ateşe vererek kundaklamış ve duvarlara "Hristiyanlık karşıtı" grafiti yazmıştır. Bu terör örgütünün ana hedefi, yerleşik Arapları topraklarından kovmak ve olası barışa engel olmaktır. Temel ideoloji olarak (Kach ve Kahane Chai) denilen Yahudi egemenliğini hâkim kılmaktır. Örgüt, Yahudi şeriatı olan Halakha yasalarına göre Yahudiliğin yaşanması gerektiği-

ni, buna göre Aksa mescidinin yıkılması, ezilmiş Yahudilerin, yabancıların ve özellikle de Arapların esaretinden kurtulması gerektiğine inanmaktadır. Bu nedenle kilise ve camii gibi ibadet haneleri hedef almakta, her türlü terör eylemlerini meşru görerek "Büyük İsrail" hedeflerinin gerçekleşmesi için geniş ideolojik ve askeri anlamda destek görmektedir (Pascovich, 2017: 292).

Şebîbetü't-Telâl (Tepe Gençliği/Hilltop Youth) diye adlandırılan Yahudi terör örgütü ideolojik olarak yaşlı önderlerin öğretileri ile İsrail'deki hahamların liderleri tarafından formüle edilen aşırı dini bir görüşü benimsemişlerdir. Örgütün üyeleri, ikinci nesil yerleşimcilerden oluşmaktadır. Çoğunlukla "1948 yılı toprakları" denilen bölgede doğmuş, resmi ve gayrı resmi okullarda okumuş ve İsrail hükümeti tarafından bazılarının kanun dışı hareket ettiklerine dair adları kayıtlara geçmiş olan gençlerdir.

Örgüt üyeleri, laik ideolojiye mensup kişiler ve aşırılık taraftarı Yahudi dini inanışına sahip militanlardır. Filistin topraklarından Arapları çıkarma ve "Büyük İsrail" ideallerini gerçekleştirme hedefleri üzerinde birleşmektedir. Bazı istatistiklere göre Kudüs ve Batı Şeria yerleşim bölgelerinde konuşlandırılmış ve örgüt tarafından eğitilen silahlı savaşçı sayısı sekiz yüzü aşmaktadır.(Chernofsky, 2009: 293).

Din eksenli terörden Hristiyanlık da nasibini almıştır. Dini gerekçeler başta olmak üzere renk ve ırk temelinde terör eylemleri düzenleyen aşırılık yanlısı Hristiyan sağcı örgütlerin militanları, yabancılara suikast düzenlemekte ya da camileri kundaklamaktadır. Birleşik Devletlerde benzer bir hareketin bir uzantısı olan ve Avrupa'da, 2000'li yılların başından bu yana yeniden ortaya çıkan aşırı sağ örgütler, günümüzde daha fazla öne çıkmaya başlamış olup hatta Avrupa başkentlerinde bile alenen radikal söylemler içeren mitingler düzenleyebilmektedir.

Bir Afrika ülkesi olan Ruanda'da 1994'te bir grup rahip ve din adamının önderlik ettiği soykırım da temelde din ve etnik ayrışma ekseninde cereyan etmiştir. 6 Nisan 1994 yılında başlamış olan katliam, iktidardaki **Hutu** (Abahutu)'ların başta Fransa gibi batılı ülkelerin silah desteği ile sistematik bir biçimde **Tutsi** azınlığın yaklaşık %75'ini katletmesi ile sonuçlanmıştır. (Simonsson, 2019: 294).

Hristiyan âleminde ortaya çıkan din temelli teröre başka bir örnek de, Bosna Hersek'te işlenmiştir. Radovan Karadziç ve Ratko Mladiç liderliğindeki Sırp ordusunun Temmuz 1995'te Bosna-Hersek'teki Müslüman toplumun yaşadığı Srebrenitsa kasabası kasıtlı ve sistematik bir etnik temizlik vakasına maruz kalmıştır. Aralarında kadınlar, çocuklar ve yaşlıların bulunduğu 8.000'den fazla insan katledilmiştir. Kuşkusuz bu katliam, modern Avrupa tarihinde Hıristiyan milislerin Müslüman bir toplumu hedeflediği en büyük terör eylemi olmuştur. 1990 yılında Sovyetler Birliği'nin çöküşünden ve Doğu Blokunun yıkılmasından etkilenen Yugoslavya Federasyonu, dağılma sürecine girmiştir. Nisan 1992 yılında Bosna Hersek'in kontrolünü ele geçirmek için Sırp milisleri büyük bir askeri operasyon başlatarak saldırıya geçmiştir (Brunborg, 2003: 295).

Srebrenitsa kenti, coğrafik konumu itibariyle bir kesitinin doğudan Sırbistan topraklarına sınır olması ve güneyden Sırbistan'ın iç kısımlarına doğru bir cep şeklinde uzanmasıyla, Bosna Hersek için stratejik açıdan çok önemli bir toprak parçası olmuştur. Sırplar ise, bu kasabanın Doğu ve Kuzey Doğu'daki tüm bölgeleri Bosna'nın geri kalanından izole ederek kontrol altına almayı hedeflemiştir. Sırp ordusu tarafından gerçekleştirilen Srebrenitsa katliamı, II. Dünya Savaşı'ndan sonra meydana gelen Avrupa tarihindeki en büyük katliam olarak tarihe geçmiştir (M. Kaplan, 2003: 297).

Yugoslavya Uluslararası Ceza Mahkemesi, Srebrenitsa katliamını "Etnik Soykırım" kararıyla Sırbistan'ı mahkûm etmesine rağmen 2006'da Sırp devletini bu soykırımdan sorumlu tutmak yerine, soykırımın önlenmesindeki gevşeklikle itham etmeyi yeterli görmüştür. Öte yandan Mahkeme ne yazık ki bu toplu katliama karşılık, soykırım suçu ve insanlığa karşı alenen ve cebren işlenen suçlar nedeniyle Radovan Karadziç ve Ratko Mladiç'i sadece kınamakla yetinerek müebbet hapis cezası vermiştir (Sprinzak, 1995: 298).

Etnik temele dayalı terör açısından, Avrupa ve Amerika Birleşik Devletleri'ndeki aşırı sağ parti ve ırkçı akımlarca desteklenen ve sözde sağcı-ulusalcı düşünce etrafında kenetlenen ve milliyetçilikle de hiç bağdaşmayan, ekseriyeti yasaklı birçok terör guruplarının var olduğunu söyleyebiliriz. Siyasi sürece katılmak istemeyen ve

çoğunlukla resmi taraflarca da temsil edilmeyen bu terör gurupları; "Neo-Naziler, Dazlaklar, Aşırı Sağcı Kuruluşlar ve Irkçı Gruplar" şeklinde sayabiliriz.

Aşırı sağcı terörün yayılmasının en önemli etkenlerinden biri, Avrupa ülkelerinde hızlı ve aşırı göç sonucu oluşan yabancı unsurların entegrasyonu sürecinde "ulusal ve yerel hassasiyetlerin aşağılandığı" korkusu etkili olmuştur. Bu durum, ister istemez politik ve ekonomik faktörlere de yansımıştır. Örneğin; Avrupalı gençlerin yeniden ortaya çıkan Yahudi ve Siyonist kampanyalara verdiği tepki, "Naziler" denilen gurubun yeniden canlanmasını doğurmuştur. Öte yandan ekonomik nedenler, sağcı terör ideolojisinin ortaya çıkmasını tetiklemiştir. Avrupa'daki yabancı nüfus oranlarının yüksek düzeylere ulaşmasıyla istihdam sorunu ortaya çıkmıştır. Bir taraftan maliyeti düşük kaçak işçi çalıştırmakla iş ortamları kıskaca alınmış, diğer taraftan ülke vatandaşlarının iş bulamamasına ve daha az ücretle çalışmak zorunda bırakılmasına neden olmuştur. Bu sosyoekonomik dengesizlik de yabancı düşmanlığı ve ırkçı duyguların büyümesinde önemli rol oynamıştır.

Aşırı sağ terörün gerçekleştirdiği en önemli eylemlerden biri, ABD'de Pennsylvania'nın Pittsburgh kentinde bulunan Yahudi "Hayat Ağacı" sinagoguna yapılan saldırıdır. 48 yaşındaki Robert Bowers adlı bir terör militanının "Yahudilere Ölüm!" sloganıyla sinagoga saldırarak 8 kişiyi öldürüp 12 kişiyi yaraladığı eylemdir. İbrani Göçmenleri Yardım Derneği HIAS'ın yaptığı açıklamaya göre, Robert Bowers adındaki şahıs, saldırıdan bir saat önce, sosyal medyada anti-Semitik paylaşımlar yapmıştır. Terör elemanı, Powers, "Gab" adlı sosyal medya platformunda, "One Dingo" başlığı altında; "İşgalciler halkımızı öldürmek için yanlarına çekmeyi seviyor" sloganını paylaşmıştır. Heavy.com web sitesine göre, aşırı terör örgütü mensubu bu şahıs, Gab Sosyal iletişim Platformunda kendisinin oluşturduğu özgür düşünce formuna; "Oturup insanların katledildiğini izleyemem, ben gidiyorum" sloganını paylaşmıştır. Aynı şahsın, Twitter ve diğer bazı web sitelerinden taraftar topladığı ve birçok beyaz fanatiğin kendisine katılıp çeşitli yorumlarla desteklediği tespit edilmiştir (Freivogel, 2018: 299).

2001'den sonra Neo-Naziler, beyazların üstünlüğünü savunan aşırı sağ veya antisemitiz gruplar, hükümet karşıtı militanlar ve benzeri terör grupları tarafından

yapılan eylemler, Amerika Birleşik Devletleri ve Avrupa'da, yaygın bir nefret diliyle kınanmaya başlanmıştır (Jones, 2018: 300).

"Gösteri Karşıtı Derneği" adındaki Anti-Semitizm ve kâr amacı gütmeyen sol görüşlü bir derneğin yıllık raporundaki analizinde; ABD'de beyaz ırkçı militanların işlediği cinayetlerin sayısının 2016'ya kıyasla 2017 de 20 kişi fazlasıyla iki katına çıktığını duyurmuştur (Astor, 2018: 301).

Yine Hükümet Sorumluluk Ofisinin 2017 yılı raporunda, Aşırı Sağcı Terör saldırılarının, Radikal İslamcı Terör saldırılarından (23'e karşılık 62 vakıa ile) yaklaşık üç katından fazlasıyla sorumlu tutulduğu deklare edilmiştir. Raporda, ABD'de Sağcı Terör saldırılarda 106 kişinin, Radikal İslamcı Terör saldırılarında ise, 119 kişinin ölümüyle sonuçlandığı açıklanmıştır (G.A.O, 2017: 302).

Trump idaresi, 2018'de yayınlanan yeni Ulusal Terörle Mücadele Stratejisi'nde ABD'de yerel terörizmin yükseldiğini kabul etmiştir. 34 Sayfalık belgede; Amerika'nın, Radikal İslami İdeoloji tarafından motive edilmeyen ancak aşırı ırkçılar, aşırı hayvan hakları savunucuları, radikal çevreciler, aşırı özgürlükçüler ve radikal milisçiler gibi diğer şiddet yanlısı yerel terör odaklarından kaynaklanan bir "Güvenlik Tehdidi" ile karşı karşıya olduğu ve her geçen gün bu tehdidin hızla arttığı vurgulanmıştır. Ayrıca belgede, "bu tehditlere karşı mücadelenin başarıya ulaşabilmesi için yegâne şartın, terör ideolojisinin internet üzerinden yaptığı faaliyetlerin durdurulmasına bağlıdır." ifadesi önemle vurgulanmıştır (Stigall, et al. 2018).

Avrupa'da Aşırı Sağcı Hıristiyan ve Laik, Milliyetçi veya Irkçı Terör grupları ile DAİŞ gibi bazı radikal İslami terör örgütleri arasında, ideolojiler arasındaki keskin çelişkiye rağmen, bazılarının bariz bir şekilde bazılarının da dolaylı olarak çok açık benzerliklerin var olduğunu vurgulamamız gerekir.

Birçok beyaz fanatik terör grupları ile kendilerini "İslamcı" olarak tanıtan aşırılık yanlısı terör örgütlerinin, diğer görüşlere karşı körü körüne bir nefret içinde oldukları ve fanatizmin pençesine düşmüş dar bir dünyada yaşama eğiliminde oldukları yapılan analizlerde ortaya çıkmıştır. Örneğin; DAİŞ, sadece Müslüman olmayanları değil, Şiileri de düşman görmekte ve hatta hiçbir ideolojinin etkisinde olmayıp kendi

halinde yaşayan Müslümanları da kendileri gibi düşünmedikleri için düşman olarak görmektedir. Sünni anlayışa sahip Müslümanları ise, "Tekfir" kavramı altında, "Mürted" iddiasıyla hedeflerine oturtmakta ve saldırılarına bahane uydurmaktadır (Gardner, 2019: 305).

Bu taassup ve dar görüşlülük, El-Kâide ve DAİŞ gibi terör örgütlerinin ellerinde bir maşa olarak kullandığı, başta İslam coğrafyasında olmak üzere tüm dünyada sebepsiz yere sayısızca masum insanın katledilmesine zemin hazırlamıştır.

İngiltere ve diğer Avrupa ülkelerinde Aşırı Sağcı terör yanlılarının, Asya ve Afrika'dan gelen göçmenlerin akışına izin verenleri ve onlara yardım edenleri düşman ilan etmeleri de, aynı ideolojik bağnazlığın terör örgütleri arasındaki benzerliğini ortaya koyma açısından dikkat çekicidir. Örneğin, 2011'de Norveçli Anders Behring Breivik adındaki aşırı terör örgütü üyesi, Oslo'da gerçekleştirdiği ölümcül saldırısını doğrudan Müslüman veya göçmen unsurlara değil, Norveç halkını, yabancı etnik nüfusun karışımına maruz bıraktıkları gerekçesiyle suçladığı bir siyasi partinin genç üyelerini hedef alarak gerçekleştirmiştir (de Graaf, 2013: 307).

Yeni Zelanda'da iki camiye yaptığı terör saldırısında 49 kişiyi öldüren Avustralyalı 28 yaşındaki Brenton Tarrant adındaki terörist, saldırısını gerçekleştirmek için iki yıl boyunca hedefteki camiye gittiğini ve uygun bir zaman kolladığını ifadesinde belirtti. Gözü dönmüş teröristin, Twitter hesabında "Büyük Değişim" başlığıyla 74 sayfalık aşırı ırkçı bir açıklama yayınladığı tespit edildi. Ayrıca yapılan araştırmalarda teröristin, sosyal paylaşım siteleri ve çeşitli internet forumlarında beyaz ırkın üstünlüğü hakkında yazılar yazdığı, Müslüman ve diğer azınlıklara yönelik şiddeti öven sloganlar yayınladığı ve aşırı sağa mesajlar göndererek yapacağı saldırılarla ilgili kin ve nefret uyandırıcı paylaşımlarda bulunduğu tespit edildi (Macklin, 2019: 314).

Teröristin Yeni Zelanda'nın Christchurch kentindeki iki camide gerçekleştirdiği bu katliamı facebook hesabı üzerinden kamerayla canlı olarak yayınlaması ve bilahare kullandığı silahın fotoğraflarının yayınlanmasıyla silah üzerindeki mesajların haçlı zihniyetini körükleyici, kin ve nefrete çağrı, Türk ve İslam düşmanlığı gibi ideolojik mesajlar verdiği açıkça ortaya konulmuştur.

Bir başka ayrıntı ise şahsın kullandığı silahın üzerindeki mesajlarda, Birleşmiş Milletlerin göçmenlerle nasıl başa çıkılacağı konusunda hazırladığı el broşürüyle alay edilmesiydi. Yine bir takım tarihler yazılarak, etnik veya dini gerekçelerle çeşitli cinayetlere karışmış olan ya da tarihte Müslümanlara karşı yapılan savaşlarda Müslümanları yendiği iddia edilen Slav, Ermeni ve Gürcü gibi Hristiyan âleminde tarihe mal olmuş kişilerin isimlerine övgüyle yer vermesiydi. Bu tipik eylem, aşırı ırkçı terör eylemlerinin ne kadar tehlikeli boyutlara ulaşabildiğini göstermiştir (Peacock, 2019: 315).

İslam dünyasında ise Selefi-Cihatçı hareketlerin ortaya çıkması 70'li yılların sonlarına dayanmaktadır. Özellikle o yıllar Mısır'da Arap dünyasındaki rejimleri devirmek için cihatçı grupların ortaya çıktığına rastlamaktayız.

O dönemdeki cihatçılar bir hareketten ziyade, darbe modelini temsil ediyorlardı. Nitekim 1981'de doğrudan darbe kastıyla zamanın Mısır Cumhurbaşkanı Enver Sedat'a bir suikast düzenlemiş ve katletmişlerdir.

Aradan geçen zamanla El-Kaide'nin Afganistan'da ortaya çıkması ile cihatçı örgütler daha bariz bir şekilde eyleme geçmişlerdir. El-Kaide'nin ismi, Abdullah Azzam'ın Afganistan'da "El-Kâide tü's-Salbe" (Sert Temel) adıyla yayınlanan bir dergide yazdığı bir makaleye dayanıyordu.

Azzam, makalesinde Afganistan'da bir cihat üssünün kurulması çağrısında bulunuyordu. Sovyetlerin Afganistan'dan çekilmesinden ve Soğuk Savaş'ın sona ermesinden sonra, anavatanlarına dönen Afgan göçmenlerin tanıştığı yeni ve cazip bir fikir olarak ortaya çıkmıştır. Onlara göre bu mücadele Rusları topraklarından atmaya güç yetirebildiyse artık bu cihat ruhu bölgesel değil küresel düzleme taşınmalıydı. Bu fikirlerin fiiliyata geçmesinde ise, El-Kâide için büyük bir fırsat doğurmuştur. Nitekim El-Kâide, 1998 yılında Yahudilerle ve Haçlılarla Mücadele için "Uluslararası İslami Cephenin" kuruluşunu ilan etmiştir (Azzam, 1992: 317).

Aynı yıl El-Kâide militanları, Kenya ve Tanzanya'daki ABD elçiliklerine saldırmış, Ardından yaklaşık üç yıl sonra, güya "Küresel Yayılma ve Cihadı Destekle-

me" amacıyla 2002 yılında Yemen sahilinde bulunan ABD'ye ait (USS Cole) askeri üssünü havaya uçurmuştu (Kerry, 2010: 320).

Birleşik Devletler 'in Afganistan'da Sovyetler Birliği'ne karşı El-Kâide 'ye maddi ve askeri destek sağladıkları sırada ordular arasındaki teknolojik açığın test edilmesine olanak tanımıştır. Bu dirsek teması, Afganistan'da bulunan cihatçı örgütlerin fikirlerini yayabilmesi, üyeleri arasındaki iletişimi kolaylaştırabilmesi ve silahlanmadaki açığı doldurabilmesi için teknolojiyi kullanmanın önemini hissettikleri bir başlangıç olmuştur.

Her ne kadar bu destek bazı basit iletişim teknolojisinden öteye geçmemiş olsa da Afganistan ve El-Kâide için teknolojiyle tanışmış olmaları bakımından önem arz etmiştir. Ancak örgütün elektronik yetenekleri 1990'ların sonunda bilgi teknoloji devriminin ortaya çıkması, Sovyetler Birliği'nin çöküşü, Soğuk Savaş'ın sona ermesi ve Amerika Birleşik Devletleri lehine meydana gelen tek kutuplu sistemin ortaya çıkmasıyla hızla gelişen olayların gölgesinde sınırlı kalmıştır. Tek kutuplu yenidünya düzeni çerçevesinde dünyanın farklı bölgelerinde meydana gelen çıkar ittifakları, bölgesel güç dengelerinin yeniden şekillenmesine ve ABD'nin bazı rejimleri ortadan kaldırma stratejisinin ortaya çıkmasına neden olmuştur.

El-Kâide örgütünün bilişim teknolojisi kullandığı ve internet ağları üzerinde etkin propaganda ve eylemsel faaliyetler gerçekleştirdiği 11 Eylül 2001 tarihinde ABD'nin New York kentindeki Manhattan bölgesinde bulunan dünyaca ünlü ikiz kule saldırılarının örgütçe üstlenilmesiyle anlaşılmıştır. (Sadek, 2019: 321).

ABD yönetimleri, ABD askeri gücünü daha da güçlendirmek ve aradığı jeopolitik hedeflere ulaşmak için terör sahnelerini gündemde tutarak teröre maruz kalmış bölgeleri terörden arındırmak ve oralara "demokrasi!" götürmek vaadiyle kullandı. Amerika Birleşik Devletleri'ndeki başlıca medya kuruluşları, "Medeniyetler Çatışması" adı altında terörizm ile İslam arasında paralel bir bağ olduğu algısı yarattı. Küresel terör sorununa bir çözüm sağlamak yerine, artık krizi daha da kötüleştirebilecek askeri müdahalelere destek veren savaş çığırtkanlıkları yükselmeye başlamıştı. El-Kâide de aynı şekilde medyanın kendilerini desteklemedeki önemin farkındaydı.

Nitekim el-Cezire gibi bir takım medya kanalları aracılığıyla yayınladığı ses kayıtlarıyla, radikal cihatçı fikirlerini tanıtmaya başlamış ve savaşı Müslümanlar ile Hıristiyanlar arasında gerçekleşen dini bir savaş olarak tanımlamaya çalışmıştır (Pesto, 2010: 319).

11 Eylül saldırısı, ABD ordusunun Afganistan'a yaptığı askeri operasyonlarının en önemli sonuçlarından biri olmuştur. El-Kâide açısından ise, sadece fiziksel eğitimin yeterli olmadığı ve güvenli bir organizasyona sahip olabilmenin internet teknolojisini kullanmanın vaz geçilemez olduğunu ortaya koymuştur. Güçlü silahlarla baş edemeyen El-Kâide artık bu tecrübeden sonra yoğun olarak bilgi iletişim teknolojisine yönelmiş ve militanlarıyla çeşitli sosyal ağlar üzerinden iletişime geçmiştir.

Ortaçağ düşüncesiyle 21. yüzyıl teknolojisini kucaklayan bir organizasyon oluşturan El-Kâide, henüz o dönemler siber terörizmini kullanma kapasitesine sahip olmamakla beraber internet ortamında bilgi aktarabiliyor ve iletişimler sağlayabiliyordu. El-Kâide terör örgütü, İnternet teknolojisini kullanarak öncelikle liderleri Bin Ladin ve diğer militanların mesajlarını dünyadaki milyonlarca kişiye iletmenin yanı sıra, böylesine küçük bir grubun sesini daha geniş bir dünyaya ulaştırabilme olanağına sahip olmak için var gücüyle çalışmıştır (Jacobson, 2010: 322).

2000 yılı İnternetin dünyaya yayılmasına tanıklık etti. İnternetin altyapısı istikrarlı kurumlara dayanıyordu. İnternetin sunduğu yazılım ve hizmetler düzeyindeki gelişmeler süratle daha belirgin hale geldi. "Adeta yeni nesillerin ortaya çıkmasına zemin hazırlayan teknolojideki bu gelişmeler çerçevesinde, internette farklı programlama dillerine dayanan dinamik sayfalarla statik web sayfaları geliştirdi. Facebook, Twitter, Google Plus ve diğer birçok hizmetler ve sosyal ağ sitelerinin gelişip çoğalması, bu teknolojik devrimle beraber ortaya çıkan savaşlar, devrimler, darbeler vb. karmaşık olaylar hakkında internet, en iyi bilgi kaynağı haline gelmiştir" (Kellner, 2004).

11 Eylül saldırıları sırasında el-Kaide militanı operatörler, uçaklara ait uçuş saatleri gibi bilgileri toplamak, saldırı saatlerini belirlemek ve aralarında güvenli bir

koordinasyon sağlamak için 24 saat boyunca Internet teknolojisinden yararlandıkları tespit edilmiştir.

El-Kâide militanı iki hava korsanının yine bu teknolojiden yararlanarak Florida'da kaldıkları bir otelin odasında dizüstü bilgisayarları üzerinden yoğun bir şekilde bilgi alışverişinde bulunarak uçak biletleri aldıkları, sosyal güvenlik numaralarını çaldıkları ve sahte ehliyet çıkardıkları tespit edilmiştir. 11 Eylül saldırılarının lideri Mohammed Atta, Almanya'nın Hamburg kentinde çevrimiçi olduğu ve ABD havacılık okulları hakkında bilgi topladığı da ortaya çıkmıştır (States and Gale, 2004) .

El-Kâide terör örgütünün 2002'de Afganistan'da ve 2003'te Irak'ta İnternet üzerinden dünyanın her yerinden gençleri uzaktan motive ederek ve yüksek maddi imkânlar vadederek nasıl saflarına çektiğini anlamak için gerçekleştirdiği saldırılara bakmak yeterli olacaktır. Ayrıca 2002'de Bali ve Endonezya'da, 2003'te Kazablanka 'da 2004'te Madrid'de, 2005'te Londra ve Amman'da gerçekleştirdiği saldırılarda olduğu gibi, "Küresel Cihat" emelleri doğrultusunda dünyanın önemli merkezlerine bombalama olaylarında kullandıkları yöntemleri, internet üzerindeki ağları deşifre ederek gözlemlemek mümkündür (Jazeera 2014).

El-Kaide ve beraberindeki terör guruplarının uluslararası koalisyona kaşı koyamayarak Afganistan'dan ayrılmasının ardından, internete yönelmesi, bu alanı daha da geliştirmesine neden olmuştur. El-Kâide, kurmuş olduğu Alneda.com, Jehad.net, alsaha.com ve islammemo.com gibi web siteleri aracılığıyla finansman ve eleman devşirme, elektronik iletişim ve propaganda ile bilgi toplama ve yayma faaliyetlerini (maalesef) çok rahat bir şekilde yürütmüştür.

Aralık 2004'te, geçmişte olduğu gibi al-Jazeera'ye bir kopyasını göndermek yerine, Bin Ladin'den olduğu iddia edilen bir sesli mesajı direk kendi web sitesi üzerinden yayınlamıştır. Suudi kraliyet ailesini hedef alan eleştirel açıklamalarını, al-Jazeera program editörlerinin silme veya düzenleme riskini ortadan kaldırmak için yine özellikle bu tarihten sonra yoğun olarak kendi web sitelerini kullanmıştır (Thomas, 2003: 323).

El- Kâide ‘nin Irak’taki liderlerinden **Ebu Ayyub el- Masri**’ye ait, intihar bombacılarını öven kısa videoların yayınlaması, yine eski liderinden **Ebu Musab el-Zarqawi’**nin ölümünden önce ve sonra, Mücahitlerin Şura Konseyi (Meclis’üş Şura el-Mucahidin) adıyla bilinen El-Kaide’nin Irak’taki şemsiye örgütü, internet ortamında düzenli olarak varlığını sürdürmüştür. Gerilla eğitimi, intihar bombacılarının “şehadetlerini” övme ve cihada katılma çağrılarını içeren videolar, internet siteleri üzerinden sistematik bir şekilde yayınlanmıştır.(Elnassery, 2010: 324).

2014 yılının başlarında Irak ve Suriye’deki cihatçı terör örgütleri, Irak ve Şam İslam Devleti (DAİŞ) adıyla sözde bir İslami hilafet devleti kurma girişimiyle yeni bir aşamaya geçmiş, daha fazla kitleye ulaşmak amacıyla Afrika ve Avrupa sınırlarına doğru genişleme politikası benimsemiştir. Yoğun ve karmaşık bilgileri kolay ve hızlı anlaşılır bir şekilde sunmak amacıyla kullanılan infografik yayınlar ve küçük boyuttaki el broşürleri dağıtarak taraftar kazanmaya çalışmıştır. DAİŞ ve destekçisi yapılar, arzu edilen hedeflerini gerçekleştirmek için birden fazla web sitesi açmışlardır. Arapça dergilerine ek olarak İngilizce, Fransızca, Türkçe ve Rusça dillerinde dergiler yayınlayıp piyasaya sürmüşlerdir. El-Hayat, el-Furkan ve el-İtisam gibi yayın organlarıyla Rusya, Afrika ve Filipinler’de çeşitli faaliyetler yürüterek, Irak ve Suriye toprakları üzerinde kurmuş oldukları devletin, vatandaşlarına hizmet ve güvenlik sağlayan bir yapı olduğunu savunarak başarı sağlandıkları propagandası yapmışlardır.

Öte yandan sivil vatandaşlara yönelik katliamlar, cinayetler ve şiddet sahnelerine odaklanan ikinci bir propaganda türüne de etkin olarak başvuran DAİŞ, kontrol altına almak istediği şehirlerde korku ve panik yaratarak düşman kategorisinde gördüğü her yeri etkileme amacı gütmüştür. Bu politika ilk başlarda kısmen başarılı olmuştur. Bölge halkı can korkusuyla büyük endişelere kapılmış, yaşadıkları şehir ve köyleri acil olarak DAİŞ’e bırakmak zorunda bırakmıştır.

Örgütün Irak ve Suriye ordularına karşı kaydettiği birtakım başarılar ile bölgedeki diğer silahlı güçlere karşı giriştikleri saldırılara ait kamera kayıtlarının web siteleri aracılığıyla yayınlanması, cesaret ve kahramanlık sahneleriyle baskın gücünü kanıtlamaya dönüktür.

DAİŞ, Fransa, Finlandiya, Kanada ve Birleşik Krallık gibi ülkelerden gelen 30.000 kadar yabancı savaşçıyı kendi saflarına katılmaları için Suriye ve Irak'a çekmeyi başarmıştır. Bu rakam kesinlikle küçümsenemeyecek derecededir. Terör örgütleri arasında şimdiye dek bu kadar kısa bir sürede bu boyuttaki eleman sayısını kendi saflarına katmış başka bir örgütün olmadığını söylemek mümkündür. (Tuck, 2016: 325).

3.1.2. Terörizmin İleri Teknoloji Kullanımı Üzerindeki Olumsuz Etkileri

İnternet ve telekomünikasyon teknolojilerinde yaşanan hızlı ve şaşırtıcı gelişmeler, "Yenidünya düzeninin" farklı bir biçimde şekillenmesine yol açmış, birtakım beklenmedik değişimleri doğurmuştur. Öte yandan teknolojinin getirdiği ilerlemelerden yararlanan terör örgütleri de geniş siber alandan sınırsız yararlanmak üzere çeşitli stratejiler belirlemiştir, sahadaki yenilgileri ve maddi hasarları elektronik ortamda telafi etmeyi hedeflemiştir. Aşırılık yanlısı gruplar ideolojik söylemlerini birbirine devrederek ideolojilerini sürekli tutma olanağı bulmuşlardır.

Bu gerçeklerin farkında olan çoğu devlet, önümüzdeki yıllarda, çeşitli radikal terörist grupların siber saldırılarına daha fazla hedef olma olasılığına karşın yeni ve köklü tedbirler alacaktır. Modern teknolojinin kullanımıyla ilgili getirilecek yeni mevzuat ve düzenlemelerin (güvenlik nedenleriyle elektronik kısıtlamalarının arttırılması) toplum huzuru açısından olumsuz yansımaları olacaktır. Ülkedeki etnik ve dini azınlıkların yönelimlerini izleme, elektronik gözetim ve istihbarat denetimlerinin artırılması bağlamında Amerika Birleşik Devletleri gibi gelişmiş ülkelerde alınan sıkı önlemler bahsedilen tahmini güçlendirmektedir (Edward Joseph Snowden).

ABD Ulusal Güvenlik Ajansı (NSA) eski çalışanlarından elektronik gözetim konusunda uzmanın bir görevlinin, yabancı şahıslara ve hükümetlere ait gizli bilgileri elde edebilen büyük bir casus programını bulduğunu açıklamıştır. PRISM adıyla bilinen ve Ulusal Güvenlik Ajansı tarafından yüksek düzeyde geliştirilmiş bu dijital program 2007'den beri çok gizli istihbarat sırlarını deşifre etmede kullanılmaktadır. Resmi adı, "US-984XN" olan bu program, canlı iletişimin ve depolanan bilgilerin derinlemesine izlenmesini sağlamaktadır. Program, herhangi bir müşteriyi dünyanın

neresinde olursa olsun ya da ABD vatandaşı olup olmadığına bakmaksızın, şirkete hedefleyebilmekte ve katılım sağlayabilmektedir. PRISM'in alabileceği veriler arasında e-posta, video ve sesli görüşmeler, görüntüler, İnternet üzerinden sesli iletişim, dosya aktarımı, erişim bildirimleri ve sosyal ağlardaki gezinti detayları bulunmaktadır. (Kelion, 2014: 326).

CIA, ülkelerinin uluslararası terörizmden ve diğer tehditlerden korunabilmesinde hayati önem taşıyan bir talepte bulunmuştur. Kongre'den "yabancı istihbarat kanallarının gizli gözetimi" kanununda yapılacak değişikliklerle, kendilerine ABD vatandaşlarını sürekli elektronik izleme ve gözetim hakkı verilmesini istedi. Ancak bu talep, istihbarat teşkilatlarının, sıradan Amerikan vatandaşlarının kişisel elektronik verilerine erişme potansiyeline sahip olduğuna inanan, ABD'deki bazı politikacılar ve insan hakları aktivistleri, "bu durumun ABD'yi sivil hak ve özgürlüklerin açıkça ihlal edildiği bir ülke konumuna getireceği" düşüncesiyle sert bir şekilde eleştirmişlerdir (Sinha, 2013: 327).

İngiltere'de ise, 2015 yılının Kasım ayı başlarında, Birleşik Krallık, Ulusal Siber Güvenlik Merkezi (The National Cyber Security Centre), "NCSC" aracılığıyla e-planlar dâhilinde yeni stratejiler geliştirdiğini ilan etmiştir. Geliştirilen bu yeni siber teknolojisi, sadece bilinen tarzdaki olağan savunma tekniği alanında değil, aksine "Aktif Siber Savunma" (Active Cyber Defence) olarak adlandırılan hassa istihbarat alanlarını da kapsamaktadır.

İngiltere devlet politikası olarak, İnternet kullanıcılarına karşı yapılan saldırıları zorlaştırmak için telekomünikasyon servis sağlayıcıları ile birlikte hareket ederek, hükümet tarafından alınan bir dizi teknik önlemlerle önemli tedbirler almaktadır. İngiltere, bu çalışma sayesinde silah teçhizatını oluşturan her türlü somut araçlar ile siber alandaki elektronik saldırıları bertaraf etme potansiyelini birbirine senkronize etmenin yanı sıra, yeni ve sıra dışı kodlama yeteneklerini geliştirerek siber alandaki hayati çıkarlarını savunma konusunda bir koruma ağı oluşturmuştur. Böylece ulusal bağımsızlığını her türlü saldırılardan korumak için, bizzat devletin şifreleme yetenekleri üzerindeki tam egemenliğini güvence altına almayı hedeflemiştir (Dewar, 2014: 241).

2016'da İngiltere, siber tehditlerle mücadele için hükümet tarafından finanse edilen 1,9 milyar sterlin (2,7 milyar dolar) hacminde, 5 yıllık bir plan açıklamıştır. Ardından kamu kurumlarına ve ticari sektörlere yönelik siber saldırı ve dolandırıcılıktan toplumu korumak ve daha güvenli bir şekilde yararlanmalarını sağlamak amacıyla hizmete soktukları ve kısa adı ACD olan Aktif Siber Savunma (Active Cyber Defence) programını hayata geçirdiğini duyurmuştur.

Aktif Siber Savunma (ACD), kamu sektöründe sınandıktan sonra özel sektörün ve sivil toplumun siber saldırılarına karşı güvenliğin arttırılması amacıyla kullanılmaktadır. Bu da doğal olarak özel sektör ve sivil vatandaşlar üzerinde devlet müdahalesi olup olmadığı soruları ile karşı karşıya kalınmasına neden olmaktadır (Taddeo, 2018: 242) .

Özellikle 1994 İstihbarat Hizmetleri Kanunu uyarınca, İngiltere İletişim Bürolarına, (GCHQ) Ulusal güvenlik amaçlı istihbarat sinyallerinin bir parçası olarak, ulusal ekonomik refahın sağlanabilmesi, ciddi suçların önlenebilmesi veya tespit edilebilmesi, elektronik cihazlar üzerinden bilgi akışının izlenmesi ve müdahale edilmesi hakkı tanınmıştır. Aynı yasa uyarınca GCHQ ayrıca devlet daireleri ve özel kurumlar gibi kuruluşlar arası bilgi güvenliği ve güvence tavsiyesi verebilir.

Bu hükümler 2016 yılı Soruşturma Yetkileri Yasası uyarınca değiştirilmiştir. GCHQ'nın sakıncalı ya da gizli materyallerden "yararlanabilmesi" ve nitelikli olmayan kuruluşlar ile kamuoyu gibi çeşitli taraflara tavsiyelerde bulunması karara bağlanmıştır. Gizli istihbarat bilgisi ile dâhili iletişim üzerinde kontrol sistemi bir nevi toplum özgürlük alanına müdahale anlamına de gelmektedir (Tim Stevens, 2019: 240).

Haziran 2015 sonunda, David Cameron İngiltere parlamentosundaki konuşmasında şifrelere erişim yasağı istemiştir. İngiliz İçişleri Bakanı Amber Rudd, konuşmacıya cevaben yaptığı açıklamada; hükümetin bir yönden bir yöne şifrelemeyi tamamen engellemek gibi bir niyetinin olmadığını ancak aynı zamanda, E2E şifreli mesajlaşma sağlayıcılarının şifrelerin çözülmesi için anahtarlara erişim yolu sağlanması taleplerini göz ardı etmediklerini ifade etmiştir. Zira telekomünikasyon opera-

törlerine itirazda bulunma hakkını içeren 2000 yılı Soruşturma Yetkileri Yasasında olduğu gibi, 2016'nın yeni soruşturma yetkileri kapsamında da kolluk kuvvetlerinin gerektiğinde bunları okuyabilmeleri, mesaj sahibinin şifresini çözerek suçluyu tutuklama konusunda kolaylık sağlayacağı için bunun ulusal güvenlik açısından önemli olduğunu vurgulamıştır (Smith, 2017: 252).

Almanya'da 30 Mayıs 2018'de Alman yargısı tarafından onaylanan karara göre; Alman istihbarat servisinin, ulusal güvenlik nedenlerinden ötürü büyük İnternet servis sağlayıcılarını gözetleme hakkı tanımıştır. Federal İdare Mahkemesi, yıllardır yabancı istihbarat servislerini sansürün meşruiyetini savundukları için protesto eden Alman Do-Six firmasının davasını reddettiğini açıklamıştır.

Bu araç ve gereçler, çok sayıdaki uluslararası Telekom operatörü ve servis sağlayıcısı ile ilişkisi olan Do-Six dev internet ağı üzerinden geçen uluslararası bilgi akışını kontrol altında tutmaktadır. Ayrıca Almanya'da kısa adı **BfV** olan (Bundesamt für Verfassungsschutz) adında bir Alman istihbarat servisi kurulmuştur. Bu özel birim, özgür demokratik rejime yönelik siber saldırıları ve casusluk eylemleri hakkında bilgi toplama ve analiz etme faaliyeti yürütmektedir. Bu ofis gizli bilgileri toplamak için kendisine özgü çeşitli yöntemler, araç ve gereçler kullanmaktadır (Dietrich, 2016: 3280).

Federal Bilgi Güvenliği Bürosu (BSI) Bonn kenti merkezli ve İçişleri Bakanlığına bağlı bir kurum olarak, devlet yapısı için çok önemli BT güvenlik konularından sorumludur. "Ulusal siber güvenlik otoritesi olan BSI, devlet, ekonomi ve toplum için önleme, tespit etme ve müdahale etme yoluyla dijitalleştirmede bilgi güvenliğini tasarlar. BSI, Siber alanda devleti, ekonomiyi ve toplumu tahrip edecek saldırıları önleme, tespit etme ve müdahale etme yoluyla dijital alanda güvenliği sağlamaktadır. Özetle ifade edecek olursak devlet mekanizmasının işleyişi için yetkililere düzenli olarak uyarı mesajları ve raporları sunmaktadır.

Siber saldırılarının tehlikesine karşı mücadeleye katkıda bulunmak amacıyla birçok otorite ulusal ve uluslararası düzeyde birlikte çalışmaktadır. Bu işbirliğini da-

ha iyi koordine etmek için, 2011 yılında Almanya'da bir "Ulusal Savunma Merkezi" kurulmuştur (Guitton, 2013: 329).

Terörizmle mücadele ile güvenlik ve özgürlüklerin korunması arasındaki denge:

Dijital güvenlik konusunda alınan sert politikalar kimi zaman insan hakları ihlaline yol açmaktadır. Bazı devletlerin terör saldırısı kaygısıyla yüksek güvenlik alarmına geçme durumu, gelişmiş elektronik ve dijital araç ve gereçlerle alınan aşırı tedbir uygulamaları, insan hak ve özgürlüklerini tehdit etmesine neden olmuştur. Bu durum birçok araştırma merkezinde tartışma platformlarında ve hatta uluslararası konferans ve seminerlerde işlenmiştir.

Siber tehditlerle mücadele konusunda, Dijital güvenlik politikaları ile insan hakları arasında bir denge ve fikir birliği oluşturmak elbette kolay bir durum değildir. Ancak insan hak ve hürriyetleri güvence altına almak da bir ülkenin vatandaşlarına karşı temel görevlerindendir. Örneğin Çin Hükümeti, web sayfaları ve arama motorlarında bazı anahtar kelimeleri filtreleyerek "Çin Büyük Güvenlik Duvarı" olarak adlandırılan web sitesinin kara listesi aracılığıyla ülkede faaliyet gösteren tüm İnternet kaynakları üzerinde tam kontrol sağlamaya çalışmaktadır. Bu nedenle Çin gibi, sürekli insan hakları ihlallerine dair kayıtlara sahip olduğu bilinen baskıcı rejimlerin, özgürlüklere karşı daha dikkatli, dengeli ve şeffaf bir çizgiye gelmeleri gerekmektedir(Joyce 2015).

İnsan hakları savunucuları, politikacılar ve bazı insan hakları örgütlerinin çoğuna göre, bu noktada asıl sorunun terörle mücadele yasalarında olmadığı, buna karşılık "zaruretlerin yasaklara izin verdiği" bahanesiyle özgürlükleri kısıtlamayı meşru çerçevede görmekten kaynaklanmaktadır. Aşırı derecede uygulanan bir kontrol, İnternet kullanma özgürlüğünün kısıtlanmasına yol açmaktadır. Bu durum, siyasi kargaşadan bir türlü kurtulamayan çoğu Arap rejimlerinde de açıkça ortaya çıkmıştır. Irak hükümeti Ekim 2019'daki gösteriler sırasında İnternet hizmetini sıklıkla kesmiştir. Aynı şekilde Mısır hükümeti 2011'de Mısır devriminin yaşandığı günlerde sosyal ağ sitelerinin kullanımını kısıtlamaya gitmiştir.

Bazı uzmanlara göre bunun çaresi, insan haklarının belirli bir süre etkisiz hale getirilmesini gerektiriyor. Ancak insan haklarını savunma gerekçesi ve özgürlüklerle ilgili endişe bahanesiyle bir takım insan hakları savunucularını, politikacıları ve ideologları saflarına çekme peşinde olan terörizm de bu mantığı dayatmaktadır(Brophy and Halpin 1999).

İnsan hakları savunucuları arasında, devletin caydırıcı rolünü iyi oynaması ve yasal yaptırımları uygulaması gerektiğine dair yaygın bir kanaat vardır. Bu düşünce bazı akademik araştırmacıların bakış açısından farklı olarak tezahür etmektedir. Şöyle ki; devlet, ulusal güvenliği söz konusu olduğunda özgürlükleri kısmen sınırlamakla şüpheli ya da terör riski taşıyan unsurları engelleme ve vatandaşların güvenliğini sağlamakla yükümlüdür. Dolayısıyla eğer terör riski varsa, bir takım geçici kısıtlamalar, insan hakları ve özgürlüklerine karşı bir hak ihlali olarak algılanmamalıdır.

Ulusal güvenlik söz konusu olduğunda İnternet ve iletişim kanallarının izlenmesi ile ilgili katı önlemler talep edenler, insan haklarının ihlal edildiğine dair yapılan çağrıların yersiz olduğunu ve devletin demokratik kazanımlarına yönelik bir tehdit veya önyargı anlamına gelmediğini vurgulamaktadır. Çünkü herkese açık bir dijital dünyada internetteki sosyal medya programlarının ve telefon iletişiminin dikkatlice izlenmesini, terörizmin yaratacağı riskler açısından proaktif bir izleme eylemi olarak gerekli kılmaktadır(Meserve and Pemstein 2020).

3.1.3. Terör Örgütlerinin İnternet Hizmetlerini Kullanma Yolları

İnternet devrimi terörist grupların operasyonlarını yeni yollarla gizlemelerine olanak tanımıştır. Terör grupları İnternet teknolojisinden yararlanarak gizli iletişim ve bilgi alış verişi başta olmak üzere siber alanı kullanarak eylemlerini gerçekleştirebilmektedirler. Terörist gruplar, güvenilir iletişim hizmetleri, gizlenme açısından uygun koşullara sahip olma, sanal kimlikler, takma isimler kullanma ve bu hizmetlerden ücretsiz ve sınırsız yararlanma gibi interneti kullanmanın en önemli yöntemlerini keşfetmiştir.

Reklam:

Aşağıdaki amaçlar için her türlü reklam ve tanıtım aracı kullanılmıştır:

a) İş İmkânı Sağlama Bahanesiyle Örgüte Eleman Kazandırmak:

Terör örgütleri, İnternet üzerinden daha hızlı ve tespit edilmesi zor karmaşık şifreler kullanarak açtıkları sahte hesaplar üzerinden sosyal iletişim ağları aracılığıyla terör örgütlerine katılım sağlamak için, işe alım bahanesiyle fikirlerini benimsemeye ikna ederek kıtalar ötesindeki meyilli elemanlarla dirsek sağlayabilmekte, saflarına katabilmekte ve onları yerlerinden alıp savaş alanlarına sevk edebilmektedir. Geçmişte bu etkileşim ve iletişim zaman açısından aylar alırken, geldiğimiz noktada artık dakikalar hatta saniyeler bile önem kazanmış durumdadır. Dahası bu terör örgütlerinin, sosyal medyayı gayrı resmi bir araç olarak kullanmanın yanı sıra bir nevi yaşam tarzı haline getirmiş olması, konunun vahametini ortaya koyma açısından büyük önem arz etmektedir (Kartal, 2018: 330).

Bu örgütler, Twitter, Tumblr, Facebook, Skype gibi programları kullanarak, birçok sosyal ağ uygulaması ve diğer mesajlarla beraber profesyonelce çekilen videolar ve diğer işitsel ve görsel dokümanları yayınlamalarıyla, özel çabaların haricinde adeta daha resmi bir desteğe sahip olmuşlardır. Bunun en bariz örneği, kendisini diğer terör örgütlerinden ayıran bu özelliğiyle dünyanın her bölgesinden internet aracılığıyla etkin bir şekilde eleman toplayıp hedef yerlere yönlendirebilen ve akıl almaz boyutta eylemler gerçekleştirebilen DAİŞ terör örgütüdür(Ristori, 2016: 237).

b) Aşırılığa Teşvik ve Tahrik Etmek:

Örgütün, sosyal paylaşım sitelerinin kötüye kullanılması yoluyla şiddeti teşvik etmesinin ve aşırılık yanlısı söylemlerini yaymanın en önemli yollarından biri olan internet, çeşitli sosyal sınıflar ve özellikle de fakirler ve işsizler üzerinde etkinliğini kolaylaştırmıştır. Örneğin Taliban, Afganistan'daki ABD işgal kuvvetlerine karşı başlattığı operasyonları gerçekleştirmek ve intihar bombacılarına talimat vermek için bir yılı aşkın bir süre bir web sitesi aracılığıyla iletişim ağı oluşturmuştur. Ayda 70 dolara kiraladıkları ve yaklaşık 16 milyon kullanıcı hesaba sahip olan bu web site,

Teksas'taki bir ABD şirketine aitti ve aylık kira ödentileri kredi kartıyla yapılmıştı (Jones, 2008: 331).

Finansman:

Terör eylemlerini finanse etmek için, fikirlerini benimseyen destekçilerden ve varlıklı finansörlerden doğrudan talep etmenin yanı sıra İnternet üzerinden elektronik iletişim yoluyla bir takım şirketler, kurum ve kuruluşlardan maddi destek sağlanmıştır. Şüphesiz bu nevi terör örgütleri, bir takım yardım kuruluşlarını kendilerine aracı olarak kullanmıştır. Görünürde dini veya insani hayır faaliyetleri gerçekleştirmek üzere kurulmuş, ancak gerçekte kurgusal olan bu oluşumlar üzerinden duygu sömürüsü yaparak toplumun her kesiminden bağış toplatmış, kredi kartlarıyla ve elektronik para transferleriyle elde ettikleri paraları eylem sahalarına, yasadışı terörizme ya da örgütün idari mekanizmalarına aktarmıştır (Keatinge, 2019: 332).

Eğitim:

İnternet, terör örgütlerinin elemanlarına patlayıcıların nasıl üretileceğine ilişkin talimatlar yayınlayabilecekleri ve elektronik broşürler veya çeşitli kayıt araçlarıyla kendi web siteleri üzerinden eğitebilecekleri açık bir alan haline gelmiştir. Yine ne yazık ki İnternet, teröristler tarafından güvenli ve risksiz olarak değerlendirilmekte ve sanal bir eğitim kampı olarak görülmektedir.

Terör örgütleri, bilgiyi yeni ve modern yollarla paylaşabilmektedir. Güvenlik uzmanları kısaltması TTPS olarak adlandırılan Taktik, teknik ve prosedürler (Tactics, Techniques, and Procedures) formülünü belirli bir tehdidi karakterize etmek için bir araç olarak kullanabilmektedir. Taktik, rakibin saldırılarını baştan sona nasıl yapmayı planladığını ve planladığı eylemi hangi yöntemlerle gerçekleştireceğini belirlemeyi amaçlarken, Teknik, saldırganın saldırı esnasında teknik açıdan kullanacağı araç ve gereçleri içermemektedir. Prosedürler ise, saldırının örgütsel yaklaşımını, vermek istediği mesajı ve tehdit ile alınmak istenen sonucu elde etme sürecinde takip edilecek işlemleri kapsamaktadır. Bu yüzden bir terör örgütünü anlamak ve onunla mücadele etmek için, saldırganın bir eylemde kullandığı taktik ve teknikleri (TTP) çok iyi anlamak gerekir. Zira bir düşmanın taktiklerini bilmek, gelecekteki olası saldırıları

erken aşamada tahmin etmeye ve tespit etmeye yardımcı olacaktır (Shetret, 2011: 334).

Teröristler İnternet üzerinden, dijital ortamda bulunan patlayıcılarla ilgili görsel- işitsel bilgi ve dokümanlar sayesinde adeta bilfiil sahada verilen eğitim gibi önemli bir fırsata sahip olabilmektedir. Bağlantı kurdukları siteler aracılığıyla eylem sahasındaymış gibi alıştırmalar yaparak her türlü saldırı ve patlayıcı araç ve gereçleri sanal âlemde kullanıp tecrübe sahibi olabilmektedir.

Bu nedenle İnternet, İnsansız Hava Araçlarının, terör örgütlerine ait açık kampları bombalamasından koruyacak sanal eğitim alanları sağlamış bulunmaktadır (Rogan, 2006: 181).

Planlama:

Çağımızda Ceza Mahkemelerinde soruşturulması yapılan terör davalarının çoğunda Suçluların İnternette planlarını geliştirerek, saldırı için ihtiyaç duydukları her türlü bilgiye erişebildikleri, yaptıkları paylaşım ve yorumların eylemleriyle örtüştüğü ve web sitelerine giriş çıkışları ile yapılan saldırının tarih ve saatleri arasındaki yakın paralellik karşılaştırılmış ve terör örgütünün internet ağlarını profesyonelce kullanıldığını kanıtlamıştır. Çünkü İnternet, terör gruplarına hedefleri hakkında istihbarat toplamada, uçtan uca en hızlı iletişim sağlamada güvenirliği yüksek ve maliyeti düşük bir kaynak olmuştur. Örneğin, Pakistan'daki Lashkar-e-Taiba'nın 2008'de Mumbai saldırısını, Google Earth programı üzerinden planladığı tespit edilmiştir (Mahadevan, 2019: 335).

Uygulama:

İnternet, aktörlerin kimliklerini gizleme özelliğinden dolayı, masum insanların yüreğinde panik yaratma tehditleri gibi terör eylemlerini gerçekleştirmede sıklıkla kullanılmaktadır. Bir İnternet şebekesinin satın alınması ya da bir web sitenin kurulmasıyla terör örgütlerinin suç araçlarını temin etme ve suç mahalline güvenli erişim sağlama gibi önemli kolaylıklar tanımaktadır.

2007 yılında bir grup ABD askeri, Irak'taki askeri üssünde fotoğraf karelerine helikopterleri alarak önlerinde bir hatıra fotoğrafı çektirmişti. Ardından fotoğrafta helikopter tiplerinin anlaşılmaması için tedbir amacıyla üzerlerine karalama yaptıktan sonra internette yayınlamışlardı. Güya silahlı gruplara her hangi bir ipucu verilmemesi adına hassa hareket edilmişti. Ancak bazı silahlı gruplar, söz konusu askeri üssü Geotag (Konum etiketi) yardımıyla yer tespitini yapmayı başarmış ve yoğun havan saldırısıyla dört ABD helikopterini imha etmeyi başarabilmiştir (Staff, 2012: 336).

3.2. Siber Dünyada Terörizmin Haritası:

Siber dünya, engin ve sınırsız bir sanal dünyadan ibarettir. Farklı şekil ve yönelimleri ile terör örgütlerinin varlık alanlarını belirleyen bir harita oluşturmak neredeyse imkânsızdır. Ancak bu örgütlerin muhtelif gündemlerini belirlemek ve aralarındaki kontağı sağlamak için kullandıkları önemli program ve uygulamaları belirlemek mümkündür. Bahsedilen araçlar, çoğunlukla bu örgütlerin iletişim yollarını içermektedir.

"Operasyon Güvenliği" (Operational Security) kavramı, terör örgütlerinin geçtiğimiz yıllarda elektronik dünya ile alışveriş/etkileşim biçimini anlamanın en önemli giriş noktası sayılmaktadır. Ellen Zhang'a göre Operasyon Güvenliği; (tüm terör örgütleri dâhil olmak üzere), bir örgütün operasyonlarını analiz etmeye ve önemli bilgileri koruyup düşman cephenin eline geçmesini engellemek için düşmanın bakış açısından değerlendirmesine iten risk yönetim süreci mesabesindedir. Tasnif edilmemiş bazı hassas bilgiler doğru bir şekilde ele alındığında düşman için hâlihazırda veya gelecekteki operasyonlara dair kıymetli bilgilere kolayca dönüşebilir (Basyouni 2018).

Örgütlerin büyük çoğunluğu, güvenlik birimleri karşısında deşifre olmayı engellemek için bahsedilen yapıların temel niteliklerinden biri olan şifreleme (encryption) fikrini hayata geçirmeye çalışmaktadır. 11 Eylül 2001 saldırılarını takip eden yıllarda Batılı istihbarat birimleri, 2006 yılında Londra'dan hareket edip Atlas Okyanusu üzerinden Amerika Birleşik Devletleri ve Kanada'ya giden uçağın patlatılması

planını boşa çıkardıkları gibi El-Kâide terör örgütünün bazı saldırılarını engellemeyi başarmıştır. Örgütün bu başarısızlığı, kendisini çeşitli program ve iletişim yöntemlerini kullanmaya sevk etmiştir (Williams, 1999).

3.2.1. Terörizm AMaçlı Kullanılan Programlar/Uygulamalar:

a) Telegram Programı:

Telegram programı, son derece gizli bir alanın bulunması, şifrelenme ve gizli sohbet odaları içermesi nedeniyle, terör örgütlerinin lider kadroları ve elemanları tarafından birinci derecede tercih edilen bir program olarak değerlendirilmektedir. Teröristlerce emellerini gerçekleştirmek açısından başvurulan ideal bir araç sayılan ve aynı zamanda çok kolay bir ara yüze sahip olan bu program, şiddet yanlısı grupların rahat bir şekilde fikir alışverişinde bulunmalarına, bir tuşa yardımıyla anlık propagandalarını yapabilmelerine, bunun yanında kimlik ve gizli bilgilerini koruyabilmelerine imkân tanımaktadır. Terör örgütlerine bağlı unsurların Telegram ve diğer şifreli platformlardan başarılı bir şekilde yararlanmaları, bu uygulamaların sağladığı belli özelliklerle de irtibatlıdır. Bu özelliklerin belki de en önemlisi, bir uygulamanın diğer uygulamalara kıyasla gönderileri daha güvenli hale getiren ve güvenlik birimleri tarafından çözülmesini zorlaştıran özel bir şifreleme sistemine sahip olmasıdır. Terör tarafından hedef kitle olarak görülen toplumların saptanmasını da kolaylaştırmaktadır.

Telegram uygulaması kullanıcılara iletişim hizmeti sunarken, kayıt dışı bir biçimde detaylı etkileşim ve iletişim imkânı tanımaktadır. Terör örgütleri, şifreli gizli görüşme odalarının işlevselliğinden rahatça yararlanmaktadır. Ayrıca program, birbirleriyle iletişim kuran tarafların kendi isteklerine göre, gönderilen mesajların iki saniyeden bir haftaya kadar belirlenen zaman dilimi içerisinde kendiliğinden yok olması veya silinmesini sağlayan bir özellik de sunmaktadır. Bu durum mesajların kontrolü konusunu imkânsız hale getirmektedir. Üstelik kullanıcılar da programın saklama tarihi dolmuş olan ve silinen eski mesajlarını yeniden yükleyememektedir (Shehabat, et al. 2017).

Terör analistleri, hangi programın terör guruplarına göre daha güvenli olduğu konusunda en fazla tercih edilen programın Telegram uygulaması olduğunun altını çizmişlerdir. Analistler, kısmen de olsa Telegram'a rakip şirketlerin teröristleri kendi kanallarından uzak tutmak için bir takım güvenlik tedbirlerini oluşturmakta daha dikkatli olmaları ve buna karşılık Telegram'ın gerekli tedbirleri almada başarı olmamasını ilgili durumun sebepleri arasında saymışlardır (Warrick 2016).

DAİŞ terör örgütü, 2014 yılının Mayıs ayında Telegram üzerinden sözde İslam Devleti Basın Bürosuna bağlı Merkez el-Hayat el-İslami adlı adresini kurmuştur. Bu merkezde, örgütsel doküman olarak kullanılan birtakım kitap, video görüntüleri ve marşlar üretmektedir. Örgüt, hitap edilecek hedef kitlenin Batı ülkelerinde yaşayan genç nüfus olduğundan, yayınlarının büyük çoğunluğunu aralarında İngilizce, Almanca, Fransızca ve Rusçanın da bulunduğu 10'dan fazla yabancı dilde hazırlamış ve propaganda malzemesi olarak kullanmıştır. 2015 yılının eylül ayının sonlarında DAİŞ, Telegram üzerinde oluşturulan Channels uygulamasından yararlanmış ve kendisine "Nashir" adında bir kanal kurmuştur. Bu isim İngilizce' ye "yayıncı/dağıtıcı" şeklinde tercüme edilmektedir. Kanal bir tür bilgi akışını bozma ve asker edinme aracı olarak kullanılmaktadır. Ancak Telegramda bu tür bilgiler tek yönden hareket etmesinden ötürü cihat propagandalarına karşı koymak ya da engellemek çok zordur (Irwin And Milad 2016).

Teröristlerin Telegram programını kullanması, Amerika ve Avrupa'daki terörle mücadele kurumlarının endişelerini artırmıştır. Bu durum Alman merkezli şirkete yönelik çok sayıda soruşturmaya ve şikâyete temel teşkil etmiştir. Şirketin kurucusu Pavel Durov ise istihbarat birimlerinin hassas çalışmalarını desteklediklerini vurgulamakta ve bu doğrultuda 13 Kasım 2015'teki Paris terör saldırılarının akabinde şirketlerinin, DAİŞ'e ait 78 kanalı kapattığını ifade etmektedir. Ayrıca terör gruplarının Telegram'daki sohbet odalarında çoğunluğu oluşturduğunu ve bu durumun çok ürkütücü olduğunu belirterek terör yayılımını önlemek için her türlü çabayı gösterdiklerini ve daha fazlasını yapmaya devam edeceklerini açıklamıştır. Buna rağmen Durov, 100 milyondan fazla kullanıcı sayısı olan Telegram programının sunduğu şifreli iletişim hizmetinden terör örgütlerinin yararlanmasını tamamen engellenebilmesinin, dü-

şünce ve ifade özgürlüğünün bulunduğu ülkelerde yaşayan milyonlarca kişinin de katıldığı küresel bir ağ olması sebebiyle imkânsız olduğunu vurgulamıştır.

b) Whatsapp Uygulaması:

Bu uygulama ses, görüntü, bilgi paylaşımı, fotoğraf ve belge gönderilerini, iletişim esnasında bilgi ve dokümanları güvenli ve dikkatli bir şekilde ulaştırmaktadır, cep telefonu ve bilgisayar aracılığıyla kullanılabilmektedir. Bu nedenle 2009 yılında kurulduğundan bu yana dünyanın birçok farklı bölgesinde geniş bir alana yayılmıştır. Farklı özelliklerinden ötürü kullanıcı sayısı 180 ülkede bir milyar kişiyi aşmıştır. Onu ayrıcalıklı kılan en önemli özellik, programın farklı mobil cihazlar ve bilgisayarlarda kolayca kullanılabilmesi ve üst düzey şifreleme sisteminin bulunmasıdır. Uygulama 2014 yılının Şubat ayında Facebook şirketi tarafından 19 milyar dolar karşılığında satın alınmıştır.

WhatsApp uygulaması kullanıcılarına görüntülü arama, video ve ses dosyalarını gönderme imkânı sağlamaktadır. Programın sağladığı kapsamlı ve gelişmiş şifreleme sistemi, bilgilerin ulaşım güvenliğini garanti etmekte ve iletişim kuranların kimliğini korumaktadır. Uygulama tarafından kullanılan "End To End Encryption" programı hakkında üretici şirketin yetkilileri, kendi teknisyenlerinin bile kişisel mesajları okuyamadığını, gönderilen iletileri kimin gönderdiğini ve ne yazıldığını bilmediklerini belirtmişlerdir. Bu nedenle terör örgütleri tarafından cazip uygulamalardan biri olarak kabul edilmiştir. Çünkü terör hücrelerine destek ve finansman ağları temini için muhtelif kesimlerle iletişim kurma imkânı tanırken, aşırıcılığın oluşabileceği gizli bir ortam da sağlayabilmektedir. Bu durum birtakım terör gruplarının aşırı ideolojik fikirlerinin nispeten de olsa denetimsiz bir şekilde yayılmasına imkân tanımaktadır. Cihatçı terör gurupları WhatsApp uygulamasını dört ana amaçla kullanmaktadır:

- **Terör Hücreleriyle Komuta Merkezinde Bulunan Lider Kadro Arasında Güvenli İletişim Platformu:** Bu şekilde destek ağları oluşturularak, yerel unsurların bağlılığı sürdürülmekte ve uluslararası düzeyde faaliyetler koordine edilebilmektedir.

Uzak bölgelerden katılmak isteyen bireylerin planları tartışılmakta ve örgüte eleman kazandırılması için uygun zeminler oluşturulmaktadır.

- **Silahlandırma Platformu:** Örgüte katılımı gerçekleştirilmiş olan potansiyel genç militan unsurlara farklı saldırı türlerinin icrası için eğitim materyallerinin dağıtımını sağlayarak, başta patlayıcı olmak üzere her türlü silah kullanım becerisini kazandırmak amaçlanmaktadır.

- **Radikal İdeolojilerinin Yayılmasını Artıracak Tartışma Forumları:** Militanların haber ve olayları kendi aralarında tahlil etmesi, sonuç çıkarması ve görüş paylaşımı, forumlardaki tartışmalarla yapılmaktadır.

- **Yardım Toplama ve Satış Platformu:** Örgüte ait bayrak, flama, sırt çantası, askeri elbiseler ve savaş zırhları gibi eşyanın yanı sıra, "savaşçı donatma" kampanyası gibi yardım kampanyalarıyla bağış toplanmakta ve silah satışı yapılmaktadır. Bazı raporlara göre, militanların Amerika Birleşik Devletleri'nin 41 vilayeti ve 73 ülkenin anahtar numaralarını kullanmıştır. **WhatsApp** bu rakamlar vasıtasıyla kullanıcılarının coğrafi konumlarını tespit etse de numaraların çoğunlukla sanal ya da geçici numaralar olduğu tespit edilmiştir. (Sosnow, 2017: 250) .

Mesajlara şifreli koruma sağlayan WhatsApp hızlı mesajlaşma programının, terörist guruplar, çocuk tacirleri ve cinayet suçluları için bir araç haline gelmiş olması, devlet yönetimleri ve hükümetler tarafından eleştiri konusu olmuştur. Bu konuda bazı hükümetlerce WhatsApp şirketi suçlanırken, bazıları Afrika, Güney Amerika ve Güneydoğu Asya ülkelerinde kargaşa, iç karışıklık vb. talihsiz olayların yaşanması nedeniyle uygulama sahibi şirketi kınanmıştır. WhatsApp uygulaması birtakım ülkelerin demokratik seçimlerinde de belirsizlik ve kargaşanın temel aracı haline gelmiştir. Örneğin, Uganda'da Whatsapp, yalan, sansasyonel haber ve söylentilerin yayılma vesilesi olmuştur. Söylentilerle savaş bağlamında daha önce yaşanan şiddetli protestoların tekrarlanmaması için şifrelenmiş özel mesajları vergilendirmek gibi girişimler ortaya konmuştur. Hindistan'da gelişen olaylarda, Devlet Bakanı WhatsApp şirketini yalan haber ve söylentilerin yayılması konusunda sorumluluğunu üstlenmeye davet etmiştir. Hükümetlerinin bu uygulamanın kötüye kullanılmasıyla yalan haberlerin

yayılmasına asla izin vermeyeceğini, WhatsApp ve benzeri programların uyuşturucu tacirlerinin iletişim kanalına dönüştüğünü açıklamış ve uyarılarda bulunmuştur. Öte yandan aynı programın öğrenci grupları ile teröristlerin irtibat adresi olduğunu dile getirmiştir. Alınacak bu tür tedbirlere rağmen uzmanlar gizliliği koruyan şifreli uygulamalardan birinin kapatılması veya yasaklanması durumunda, kullanıcıların diğer uygulamalara geçeceklerini düşünmektedir.(Mutsvairo, 2016: 343).

c) Wickr Uygulaması:

Wickr uygulaması da terör örgütlerinin kullandığı önemli programlardan biri sayılmaktadır. Bu programda, mesaj şifreleme işlemlerinin içeriğine ulaşılması son derece zor ve bazen de imkânsızdır. Çünkü kullanıcıya ait şifre anahtarının güvenli bir şekilde dağıtılması başlı başına bir temel engel olarak karşımıza çıkmaktadır. Mesaj içeriğindeki bilgileri okunamaz metinlere dönüştüren şifreleme anahtarıdır. Böyle bir şifreyi çözmek pek olası değildir. Zira uygulamada kullanıcı sürekli bir veya iki anahtarı değil, gönderdiği her mesajda 5 farklı şifre anahtarı kullanır. Böylece sadece mesajı şifrelemek açısından değil, başka yönlerden de sınırlar zorlanmaktadır. Kullanıcı gönderdiği mesajın şifresini açabilecek tek kişinin mesajın alıcısı olduğunu bilir. Böyle bir şifreleme ile yapılan mesaj gönderimine, "ideal güvenlikli" gönderim denilmektedir. Bu yöntemle gönderilen mesajları artık ne FBI, ne NSA hatta Wickr'in kendisi bile denetleyemez. (Heidi Shey with Stephanie Balaouras, 2019: 344).

d) Gmail e-Posta Gönderme Uygulaması:

Gmail her ne kadar kullanıcı kimliğini deşifre etmese de, elektronik postaların gönderildiği sitelerin takip edilmesi günümüzde artık mümkün hale gelmiştir. Lansman sırasında Gmail, kullanıcı başına 1 GB'lık bir başlangıç depolama teklifi sunarken, o sırada sunulan rakiplerden çok daha yüksek. Bugün, hizmet 15 GB depolama alanı ile birlikte geliyor ve saklanan dosyaları uzun süre saklıyor ve uygulamada kullanıcı hesabından gerektiğinde geri yüklenebiliyor. Kullanıcılar ekleri de dâhil olmak üzere 50 MB'a kadar e-posta mesajı alabilirken 25 MB'ye kadar e-posta mesajı gönderebilir. Daha büyük dosyalar göndermek için kullanıcılar, Google Drive'dan mesaja dosya ekleyebilir. Bu nedenle, bu uygulama terör örgütleri tarafından veri ve bilgi-

lerin aktarılması ve korunmasında ve üyeleri arasında, özellikle de büyük dosyalar arasında kullanılan önemli uygulamalardan biridir (Miller, 2004: 345).

e) Amaq Uygulaması, Amaq Haber Ajansı:

DAİŞ örgütü tarafından Twitter üzerinden örgütün ana propaganda platformu olarak tanıtımı yapılmıştır. Örgütün propagandasını yaptığı platformdur. Sri Lanka'daki üç kiliseye DAİŞ tarafından yapılan saldırılarda 310 kişinin hayatını kaybettiği eylem ve haberler Amaq uygulamasıyla duyurulmuştur (Amarasingham, 2019: 350).

2014 yılında İslam Devleti (ISIS) tarafından kurulan en önemli medyalardan biridir ve kuruluşun resmi haber ajansıdır ve kuruluşun resmi olarak en ünlü sitelerinden biridir ve misyonu günün her saati siyasi ve askeri haberleri yayınlamak ve savaşların haber ve videolarını yayınlamaktır. Alandaki "başarılarını" gösteren haber ve infografiklerle uğraşırken, örgütün diğer ülkelerdeki saldırıları benimsediğini onayladı veya reddetti. Android cihazlara indirilebilen, ilk olarak Google Mağazasına yüklenen ve daha sonra silinebilen bir uygulaması vardır. Sahih-i Müslim'deki hadis adından sonra ismini almıştır: «Roma derinliklerine - veya Bdabk'a - kadar saat inmiyor (Winter, 2018: 348).

f) Alrawi apk veya The Alrawi App uygulaması:

Terör örgütü DAİŞ, Amaq programına benzeyen bu programı tasarlamakta başarılı olmuştur. Ancak örgüt üyelerinin kullandığı metin mesajları açısından bu program çok daha güvenlidir. Son olarak elektronik terörizm ile savaşan gruplardan biri olan Ghost Security Group, DAİŞ terör örgütü tarafından propaganda ve siyasi yayınlarını yaymada ve bunları güvenli bir şekilde halka iletmekte kullanılan özel uygulamalar hakkında yeni bilgilere ulaşmıştır. Yazılı mesaj özelliklerinin yeni bir versiyonu sayılan, ancak gizlilik ve koruma düzeyi noktasında Whatsapp ve Telegram uygulamalarına büyük ölçüde benzeyen yeni bir uygulama tespit edilmiştir. Bunun anlamı, DAİŞ üyelerinin kendi aralarında normal kullanıcıların kullandığı uygulamalardan başka bir takım güvenli ve gizli iletişim kanalları ile iletişim kuruyor demektir. Tespit edilebilen bazı uygulamaların sözde İslam devletinin hedef ve ilkelerinin

propagandasını daha fazla sayıda insana ulaştırmak ve cihat saflarına katılmasını sağlamayı amaçladıkları gözlenmiştir. Bu uygulamaların kullanımı, DAİŞ terör örgütünün baş döndürücü propaganda çalışmalarının bir parçası olmuştur (Tucker, 2016: 251).

Öte yandan bu uygulama örgüt üyeleri arasında maksimum 15 metre mesafeden bluetooth üzerinden mesajlaşma imkânı da tanımaktadır. Raporda ayrıca programın şekil itibarıyla ilkel göründüğü, ancak DAİŞ'in elektronik buluşlarından biri olduğundan bahsedilmekte, bu gibi uygulamaların kullanımının, büyük platformlar tarafından sınırsız sayıda radikal hesabın yasaklanması veya askıya alınması neticesinde, terör yapılanmalarının kendi aralarında güvenli bir ortam oluşturma sonucu doğuracağı da belirtilmiştir (Staff, 2016: 352).

g) Signal Uygulaması:

Bu uygulama da aynı şekilde DAİŞ ve diğer terör örgütleri için güçlü bir platform olarak kullanılmaktadır. EFF kurumunun raporuna göre, DAİŞ tamamen elektronik sınırların ve elektronik cephelerin örgütüdür. Signal uygulaması, kullanıcıları tarafından ayarlanabilen en güvenli program sayılmakta ve şifreleme açısından güvenlik özellikleri (kullanıcıların metin, fotoğraf, şifreli grup ve video mesajları göndermelerini ve birbirleri arasında şifreli telefon görüşmeleri yapmalarını) sağlayan açık kaynak kodlu bir yazılım olmasıyla whatsapp programından daha iyi görülmektedir (Graham, 2016: 353).

h) Silent Phone, Silent Circle (software) Uygulaması:

Le Grand-Saconnex, İsviçre merkezli şifreli bir iletişim şirketidir. Özel güvenlik standartlarına göre tüm dereceleri elde etmiş olan bu uygulama da aynı şekilde terör örgütleri tarafından aktif olarak kullanılmaktadır. Sessiz Telefon, kurumsal düzeyde şifreli ses, video ve mesajlaşma sağlar. Uçtan uca güvenliğimiz, işinizi, itibarınızı ve değerli fikri mülkiyetlerini casusluktan korur. Bu program birden fazla özellik ve en önemlisi ile karakterize edilir (Ungerleider, 2012: 354).

- Dünyanın her yerindeki işletmelerin ve hükümetlerin güvendiği gizlilik ve güvenlik
- Kuruluşunuzda basit "sıfır dokunuşlu" dağıtım
- Silent Manager ile entegre kurumsal kullanıcı yönetim
- Eşsiz Güvenlik Sözleriyle güvenli sesli ve görüntülü aramalar
- Güvenli yüksek tanımlı konferans görüşmesi ve grup mesajlaşması
- Yazma komutları gönderilen mesajların tüm kopyalarını imha eder
- Yanma zamanlayıcıları eski mesajları otomatik olarak yeniden düzenler
- Sesli notlar iletişimi hızlandırır ve güvensiz sesli postayı değiştirir
- Makbuzları oku ve makbuzları ekiplerine durumsal farkındalık kazandır
- Belgeleri, videoları, resimleri ve diğer dosyaları güvenle gönderin
- Silent World, daha fazla güvenlik ile geleneksel telefon numaralarına / dan arama olanağı sunar (Tsukayama, 2013: 355).

ı) Cryptocat Uygulaması:

EFF Kurumu tarafından yüksek güvenlikli değerlendirmesini elde eden uygulamalardan biridir. Uygulama Facebook üzerinden giriş yapılması aracılığıyla şifreli konuşma seçeneği üzerinden uygulamayı kullanan kullanıcılar arasında toplu bir şekilde mesajlaşma, fotoğraf ve dosya gönderme olanağı sunmaktadır. (Matonis, 2012: 356).

i) Threema Uygulaması:

Kullanıcılara arkadaşlarıyla sesli ve yazılı mesajlaşma, fotoğraf, video ve dosya gönderme, toplu konuşmalar oluşturma ve oy kullanma imkânı tanımaktadır. Uygulama, kullanıcılara ait yedi farklı gizlilik koruma standardından altı tanesini gerçekleştirmesiyle, programı teröristler için doğru bir tercih haline getirmektedir. (Siebelts, 2017: 357).

j) Tox Uygulaması:

Tox, uçtan uca şifreleme sunan bir eşler arası anlık mesajlaşma ve görüntülü görüşme protokolüdür. Projenin belirtilen amacı herkes için güvenli ancak kolay erişilebilir iletişim sağlamaktır. Protokolün referans uygulaması, GNU Genel Kamu Lisansı koşulları altında ücretsiz ve açık kaynaklı yazılım olarak yayınlanmaktadır. Teröristlerin kullandığı uygulamalar sınıfına katılmıştır. Yazılı metin ses ve görsel mesajların gönderimine imkân sağlayan ve tüm iletişimleri tamamen şifreli bir şekilde gerçekleştiren bir uygulamadır (Wikipedia, 2019: 358).

k) Linphone Uygulaması:

IP softphone, SIP istemcisi ve servis üzerinden ücretsiz bir ses. Herhangi bir VoIP yumuşak anahtar veya IP-PBX üzerinden doğrudan sesli ve görüntülü aramalar ve çağrılar için kullanılabilir. Ayrıca Linphone anlık mesajlaşma imkânı sunar. GUI için GTK + tabanlı basit birçoklu dil arayüzüne sahiptir ve Linux'ta konsol modu uygulaması olarak da çalıştırılabilir.

Yazılım telefonu şu anda Fransa'daki Belledonne Communications tarafından geliştirilmiştir. Linphone başlangıçta Linux [9] [10] için geliştirildi, ancak şimdi Microsoft Windows, Mac OS X ve Windows Phone, [11] iOS [12] veya Android kullanan cep telefonları dâhil olmak üzere pek çok ek platformu destekliyor. Uçtan uca şifreli ses ve video iletişimi için ZRTP'yi destekler (Wikipedia, 2019: 358). Tüm iletişim süreçlerinde yüksek güvenlikli şifreleme özelliklerine sahip bir program olup, teröristlerin kullandığı uygulamalar listesinde yer almaktadır (Project, 2019: 360).

l) Surespot Uygulaması:

Teröristler bu uygulamayla tamamen şifreli bir şekilde görsel iletişim kurma imkânına sahiptirler. Bu şifreler sadece hesap sahibi tarafından kırılmaktadır. Örgüt liderleri ile yeni örgüt militanları arasındaki görüşmeler bu uygulama ile yapılmaktadır.

Öte yandan DAİŞ örgütü, bir takım uygulamaları şifreleme teknikleri ile daha güvenli hale getirmeyi de başarabilmiştir. Örneğin elektronik mesajları şifreleyen Mojahedeen Secrets, Yahoo, Msn, Google Talk ve Aım hesapları üzerinden yaptığı konuşmaları şifreleyerek "gizli sohbet odaları" gibi kullanabilmektedir. 2013 yılında Küresel İslami Basın Cephesi isimli grup, cep telefonlarını şifreleyebilen mobil şifreleme adlı bir uygulama geliştirmiştir (News, 2015: 361).

3.2.2. İnternet Sitelerinin Terör Örgütleri Tarafından Kullanılması:

Belirtilen uygulamalara ek olarak terör örgütleri bir takım internet sitelerini de kullanmaktadır. İnternet siteleri terör örgütleri için propaganda aracı olarak görülmekte ve fikirlerini ulaştırmak adına önemli platformlar teşkil etmektedir. Militanlar arasında mesaj iletişimi, örgüte yeni eleman kazandırma, farklı mekânlara para sevkiyatı ve silah satışı noktasında örgüt üyeleri arasında önemli bilgi transferleri oluşturma gibi faaliyetler gerçekleştirilmektedir. Ayrıca örgüt, birtakım internet siteleri aracılığıyla çökertmeye çalıştıkları devlet sitelerini kolayca ele geçirmekte, ülke ekonomilerine zarar verme olanağı bulmaktadır.

Terör örgütü, bilgi güvenliğini sağlamak, istediği hızda bilgi transferleri gerçekleştirmek ve kendisine bağlı unsurların kimliklerini gizleyebilmek için binlerce sunucu (Servers) kullanabilmektedir. Bu serverler, kullanıcı konumu veya kullanılan cihazla ilgili bilgilerin tespit edilmesini zorlaştırmaktadır. Terörle mücadele eden hükümetler ve ilgili güvenlik kurumlarının işini son derece zora sokmaktadır.

Terör Yapılanmaları tercih edilen internet sitelerinin en önemlileri şunlardır:

a) Dark web sitesi:

Diğer adlarıyla "Karanlık İnternet" ya da "Kara Ağ" olarak bilinen İnternet sitesi, terör örgütünün önemli bir aracı sayılmaktadır. Site, yayınlayıcı kimliğini veya konumunu deşifre etmeksizin internet sitesi kurmaya ve bilgi paylaşımına izin vermektedir. Arama motorları üzerinden kullanılmayan, ancak **tor** servisi gibi internet kullanıcılarının ifade özgürlüğü ve gizlilik niteliği bulunan bilgilere ulaşmak ve irti-

bat kurmak için belirli motorlar tarafından kullanılabilmektedir. Bu sistem veya tor arama motoru Amerika deniz kuvvetleri tarafından önemli ve tehlikeli bilgileri elde etmek aynı zamanda devlete ait gizli bilgilere ulaşımı engellemek için kurulmuş olup, önceleri askeri bir kurumun internet sitesi olarak hizmete başlamıştır. Akabinde 2003 yılında halkın kullanımına açılmıştır (Staff, 2014: 362).

Yerel hükümetler tor kullanıcılarını takip etmekte zorlanmaktadırlar. Zira normalde kullanıcıların konumu ya da cihaz bilgileri diğer programlarla takip edilebilmekteyken, tor programı kesinlikle buna engel olmaktadır. Bu nedenle terörist grupların büyük çoğunluğu kişisel konum veya IP adreslerinin devletlerin takip birimlerinin eline geçmesini engellemek için cihaz bilgilerini paylaşmayan bu **tor** programını kullanma yoluna gitmektedir.

Bu program, Facebook, Yahoo, Youtube ve Gmail gibi uluslararası şirketler tarafından yasaklı program olarak tanıtılmış ve rejimlere karşı savaşan terör grupları tarafından kullanılan en tehlikeli arama motorları arasında sayılmıştır. Tüm iletişim bilgilerini gizleyebilen Tor programı arama motorunda 5000'den fazla serverin dolaşım kapasitesine sahiptir (Overlier, 2006: 365).

Öte yandan bu sunucu üzerinden finansal işlemler hükümetlerin gözünden uzak tutulmaktadır. Özellikle de Bitcoin gibi özel bir finansal para birimine sahip olduğu için başta DAİŞ olmak üzere çoğu terör örgütü, hükümetlerin elektronik saldırısından kurtulmak için bu sunucuyu tercih etmektedirler.

Terör örgütü "Kara İnternet" sitesi üzerinden hilafet yayınları sitesi kurmuş, site kullanıcılar arasında anlık iletişim yapabilecek ve dolayısıyla operasyonları hızlandıracak şekilde geliştirilmiştir. Avrupa birliği bu sayfayı takibe alacak elektronik suçlarla mücadele merkezi kurmayı planlamış ancak henüz başaramamıştır (Weimann, 2016: 364).

b) Online Oyun Siteleri:

Elektronik oyunlar farklı şekillere sahip radikal örgütlerin kullanabileceği en iyi iletişim yöntemlerinden biri sayılmaktadır. Çünkü dünyanın her bölgesinde inter-

netin bulunduğu her yerden giriş sağlanabilmektedir. Ayrıca terör unsurları, çocuk ve gençlerin kendilerine katılımı için özellikle bu sitelerden yararlanmaktadır. Batı menşeli birçok raporda, radikal örgüt unsurlarının özellikle de çevrimiçi elektronik oyunları "Online Oyunlar" güvenlik takibatından uzak bir iletişim aracı olarak kullandıkları tespit edilmiştir. Teröristler Saint-denis ve Fransa Uluslararası Stadyumu'nda gerçekleştirdikleri bombalı saldırılarda bu yöntemi kullanmıştır. Bu tür internet oyunlarının, "görünürde masumane bir çocuk oyunu algısı vermesi açısından" İstihbarat birimlerinin tespitinden uzak olması, son derece tehlikeli sonuçlar doğurduğunu kanıtlamıştır. Zira bir oyun sitesinin asıl amacı eğlence olması gerekirken, terör militanlarınca fırsat alanlarına dönüştürülebilmektedir. Yine elektronik posta veya sosyal paylaşım sitelerine göre çok daha kamuflajlı ve daha rahat gezilebilir olması nedeniyle bu siteler tercih edilmektedir. Bu nedenle her geçen gün terör örgütleri tarafından bir takım oyun siteleri açılmakta veya kurulmuş siteler ele geçirilmekte ve hem özel parolalar kullanarak kendi aralarındaki iletişimler sağlanmakta hem de oyun oynamak için giren masum gençleri kirli emellerine çekmek için uğraşmaktadırlar (Gercke, 2012: 368).

Bu oyunlar üzerinden teröristler, gençlerin aklını çelerek örgüte katmak, onları yaşadıkları toplum içerisinde kendi adlarına şiddet eylemleri gerçekleştirmeye sevk etmek ve her türlü saldırıya hazır hale getirme stratejisi gütmektedir.

Bu oyunların içerisinde bulunan şiddet sahneleri, çocuklarda bir tür favori haline gelebilmektedir. Gençler, çocuklar ve ergen yaştaki delikanlılar sanal savaşlara katılabilmekte ve neredeyse gerçeğe yakın bir psikolojik şiddet hayatı yaşayabilmektedir. Zaten bu tür oyunlar aslında gerçek hayatlarında ulaşamayacakları şeyleri yapmak isteyenler için tasarlanmıştır. Radikal örgütlerin militanlarıyla uzun süreli görüşmelere izin veren bu oyunların tüm dünyaya serbestçe oynanması için dağıtılmış olması ve oyun taktiklerinde verilen tüyeler, teröristlere planlı bir saldırı için senaryolar geliştirilebilmeyi adeta altın tasla sunmaktadır. Çünkü örgütler bu oyunlarda işlenen bombalama ve cinayet sahnelerini kandırdıkları ve militan olarak seçtikleri gençlerin, psikolojileri açısından her türlü şiddete hazırlama yönüyle de faydalan-

maktadır. Sosyal paylaşım sitelerinden farklı olarak bu sitelerin izlenmesi de oldukça zordur (Al-Rawi, 2018: 369).

Asıl tehlike ise, terör örgütlerinin sanal âlemde avladıkları gençleri, gerçek âlemde cinayet, bombalama saldırı ve intihar eylemleri gerçekleştirmeleri için hazırlayıp talimat vermesinde gizlidir. Eylül 2014'te DAİŞ örgütü, sosyal paylaşım siteleri, iletişim forumları ve Youtube gibi programlar üzerinden meşhur Grand Theft Auto oyununu taklit ederek Sallil Swarm adında bir elektronik oyun geliştirmiş ve bu oyun batıya "Cihat Simülatörü" adıyla sunulmuştur. Oyun, kullanıcılarına bombalama, keskin nişancılık ve taarruz operasyonları yapma imkânı tanırken oyunun başkahramanlarını; DAİŞ unsurlarını, düşmanları ise; Arap Ordularını ve Koalisyon Güçlerini temsil edecek şekilde uyarlanmıştır.

İngiliz BBC kanalının DAİŞ örgütünde faaliyet gösteren Ebu Sümeyye adındaki bir İngiliz vatandaşı ile yaptığı röportajda; kendisinin küresel Call Of Duty oyunundaki bir etabı geçmek veya oyundaki görevini yerine getirmek için kendisine yapılan çağrı nedeniyle örgüte dâhil olduğunu dile getirmiştir. Aynı röportajda, bir şahıs, üç çocuğunun DAİŞ örgütüne katıldığını övünçle bahsederek, Suriye ve Irak'ın bir bölümünü elinde tuttuklarını, savaşmanın onlar için Call Of Duty oyunundan çok daha iyi olduğunu dile getirmesi, terör örgütünün söz konusu oyun üzerinden insanları nasıl kandırıp saflarına çektiğini açıkça ortaya koymaktadır (Crompton, 2014: 370).

Suudi Arabistan Krallığı İslami İşler Bakanlığı tarafından radikal fikir sahipleri ve terörist faaliyetlere meyilli bir takım kişilerle bazı elektronik ropörtajlar yapılmıştır. Alınan bilgilere göre, "diyalog için sükûnet" kampanyası çerçevesinde DAİŞ örgütünün sesli ve yazılı sohbet ortamları gibi farklı yöntemler kullanarak oyuncularla görüştüğü, kendilerini saptırma girişimlerinde bulunduğu ve Roblox çocuk oyunu gibi oyunlar üzerinden Amerika Birleşik Devletlerindeki çocukları örgüte katarak Amerika'da terörist eylemler gerçekleştirmeye çalıştığı tespit edilmiştir (East, 2017: 371)

Öte yandan örgüt, Grand Theft Auto 5 gibi şiddet oyunları hakkında videolar oluşturarak oyunculara, karakterlerin başına gelenleri oyun dünyasında olduğu gibi gerçek dünyada kendilerinin de bizzat yapabileceklerini, ancak bunun örgüte katılmakla mümkün olabileceğini telkin ettikleri kayda geçmiştir. Örgüt oyuna Arma 3 adı altında ücretsiz bir savaş yaması getirmiş olup, bu yama silahların anlatımı ve savaş sistemleri noktasında gerçekçiliği ile bilinmektedir. Gerçekten ilham alan senaryolarıyla militanlarını eğitmeyi hedeflemekte, saflarına katılmaları için çocukları ve gençleri etkilemeye çalışmaktadır. Örgütün kollarından biri olan "himmet kütüphanesi" grubunun 10 Mayıs 2016 tarihinde çıkardığı bir uygulama da bulunmaktadır. Söz konusu uygulama Android sistemi üzerinden çalışmakta ve çocuklara Arap harflerini şiddet ve ölümle alakalı fotoğrafları kullanarak öğretmektedir. Burada Arap harflerini öğrencinin ezberleyebileceği örnekler üzerinden ve silah türlerinin isimleri ile irtibatlandırarak vermektedir (kadrosu, 2016.05.13: 372).

c) Deep web:

Bilinen herhangi bir arama motoru tarafından erişilemeyen, tamamen gizli bir internet ağıdır. Koşulsuz ve sansürsüz, gizli bir dünyadır. İzlenemez ve denetlenemez, genellikle gizli yollarla, sahte adlarla ve doğal internet ağına doğrudan bağlanamayan bilgisayarlarda kullanılır. Bu ağ, tehlikeli mesajların iletilmesine dayanır ve site dışındaki kişilerin siteye girmesini engelleyen milyonlarca virüsle doludur. Bunun yanı sıra kullanıcıların grup bilgisine virüs bulaştırmasını ve böylece özel bilgileri otomatik olarak şifrelemelerini sağlar. Bu sitelere veya Deep Web dünyasına sadece özel programlar ve örümcek ağında çalışan ilgili protokollere tabii özel tarayıcılar tarafından erişilebilir.

Deep Web'te kamuya açık bilgilerin, şu anda küresel ağdan 400 ila 550 kat daha fazla olduğu bilinmektedir.

Deep Web, 19 terabaytlık yüzeysel internet bilgisi karşısında 7500 terabayt bilgi içermektedir. Normal yüzeysel internet ağı bir milyar kişisel belge içerirken, Deep Web yaklaşık 550 milyar kişisel belge içermektedir. Şu anda kurulu 200.000 Deep Web internet sitesi bulunmaktadır (Bergman, 2001: 254).

Altmış büyük Deep Web internet sitesi toplamda 750 terabayt civarında bilgiyi içermekte olup bu bile tek başına yüzeysel internetin boyutunu 40 katını aşmaktadır.

Deep Web'e Girebilen En Önemli Tarayıcılar Şunlardır:

1. Tor tarayıcısı: web sitelerinde özgürce gezinirken bilgilerinizin şifrelendiği en popüler ve güvenli tarayıcılardan biridir.

2. P12 tarayıcısı.

3. Freenet tarayıcısı.

4 Techxtra: Öğrenciler için çok önemli bir arama motorudur. Techxtra; mühendislik, matematik ve bilgisayar alanlarında içerik bulmasına olanak sağlar. Önemli endüstri haberleri, iş duyuruları, teknik raporlar, teknik veriler, tam metinler ve öğretme ve öğrenme kaynakları ile ilgili konularda yardımcı olabilecek web siteleri Techxtra'dan öğrenilebilir (Raghavan, 2000: 375).

5. Infomine: İnternetteki birçok ABD Kütüphanesi tarafından geliştirilen İnfomine, öğrencilerin kitap, makale, not, soru formu, çözüm vb. materyalleri bulabileceği harika bir alternatif arama motorudur. Arama motoru, California Üniversitesi Kütüphanesi, Wake Forest Üniversitesi, California Eyalet Üniversitesi ve Detroit Üniversitesi'nin veri tabanlarını içermektedir. Veri tabanlarından, e-dergilerden, e-kitaplardan, bülten panolarından, posta listelerinden, elektronik kütüphane kart kataloglarından, makalelerden, araştırma kılavuzlarından ve diğer pek çok kaynaktan bilgi elde edilebilir.

6. Infoplease: İnternette çok sayıda ansiklopedi, takvim, atlas, biyografi arama linkleri ve çocuklara yönelik sayfalara ulaşabilme imkânı tanıyan alternatif bir derin arama motorudur.

7. Internet Archive: Film, canlı müzik, ses ve basılı materyallere erişim sağlayan muhteşem bir veri tabanıdır. Bunun yanında, internette oluşturulan hemen hemen her sitenin en eski kaydedilmiş sürümlerini ve şu ana kadar kayda geçmiş 391 milyardan fazla dosyaya buradan ulaşılabilir.

8. Deep Web Tech: Deep Web Sadece bir arama motoru değildir. Aynı zamanda belirli konular için toplam 5 arama motoru (ve tarayıcı uzantısı) sağlar. Genellikle bilim, tıp ve işletme konularını içerir. Böylece bu konulardaki temel haberlere, ayrıntılı bilgilere, web sitelerine, dergi vb. dokümanlara kolayca erişilebilir (Hamilton, 2003: 377).

9. Deeppeep: Bilgi edinmek için veri tabanlarını ve web servislerini sorgulayan formlar üzerinden Deep Web'e erişim sağlar. Her hangi bir sorgulama yapıldığında, normal arama motorları tarafından listelenemeyen, dinamik ve kısa ömürlü bir sonuç sayfası açılır (Barbosa, :378).

10. www.virtual.library: Web'in mucidi Tim Berners-Lee tarafından başlatılan en eski web kataloğudur. Sanal kütüphane, son derece düzenli bir şekilde tertip edilen birçok konuyla ilgili çok sayıda kaynağı listeler. Konular alfabetik bir şekilde sıralanmış olup, kullanıcıların göz atmasını kolaylaştırmaktadır.

11. Intute: İngiltere'de kurulmuş merkezi bir arama motorudur. İngiltere'deki saygın üniversitelerin çoğuyla birlikte araştırma ve çalışmalar için temel kaynaklar sağlamaktadır. Arama motoru, tarım, veterinerlik ve diğer ilgili konular hakkında birçok kaynak içermektedir. Sonuç almak için sadece anahtar kelime girilmesi yeterlidir. İlgili konularda siteleri inceleyen ve dizine ekleme yapan site uzmanları belirlenir. Intute ayrıca etkili internet arama becerilerini öğretmek için 60'tan fazla ücretsiz çevrimiçi ders sunar. Eğitim programları adım adım rehberlik sunmakta olup, belirli konular çerçevesinde sıralanmaktadır (Watkins, 2009: 379).

12. Complete Planet: Deep Web veri tabanlarındaki bağlantılara ücretsiz erişim sağlayan bir arama motorudur. Bu site, büyük bir dinamik veri tabanı bloğuna erişmeyi kolaylaştıran önemli bir kaynak ve iyi tasarlanmış ücretsiz bir dizindir. Site, Deeb Web'de bulunan, yiyecek, askeriye, uyuşturucu, içecek vb. materyal aramalarını kolaylaştıran 70.000'den fazla veri tabanı içermektedir. Uzmanlar, buradaki herhangi bir usulsüz web sitesinin kapatılmasının imkânsız olduğunu, belirli bir sitedeki faaliyetleri ne olursa olsun yerel bir hükümet birimlerinin bu sitelere girişi engelleyemeyeceğini, zira her bir internet sitesinin binlerce

sunucusunun bulunduğunu söylemektedirler. Buna delil olarak çoğu ülkenin karanlık web sitelerine erişimi yasaklamış olmasına rağmen, dünyanın hemen her yerinden bu sitelerin kullanılması ve terörist grupların iletişimlerini devam ettirmesi ileri sürülmektedir.

Bu sitelerin kullanıcıları genellikle gerçek isimlerini ve internete bağlı kendi kişisel bilgisayarlarını kullanmazlar, aksine sadece Deeb Web hesaplarına bağlı bilgisayarları kullanırlar. Yine kullanıcılar asıl e-postalarını da kullanmazlar. Gerçekte bu gibi ağlar, her türlü yasa dışı bilgi transferi ve iletişim olanağı sağlamaktadır. Öte yandan kişilerin tek başına ulaşamayacağı birçok istihbarat ve devlet bilgisi sunmaktadır. Bu tür bilgiler, genellikle FBI gibi istihbarat kuruluşları tarafından depolanmaktadır. Bunun gibi hukuk dışı ve tehlikeli birçok internet sitesi bulunabilir. Uyuşturucu, silah, insan ve organ ticareti siteleri, elektronik korsanlık eğitim ve silah/ patlayıcı yapımını öğreten siteler, gösterimi yasaklanan kitaplar ve filmler, farklı iletişim siteleri ve birçok yasaklı yazılım buna örnek olarak verilebilir.

Uzmanlar, terör örgütlerinin Deeb Web'i, silah ticareti, eleman kazanma, banka ve hükümet binalarını soyma gibi eylem ve faaliyetlerde kullandıklarını ifade etmektedir. Amerikan istihbaratının elektronik birimleri bu sitelere girmeye çalışmış, ancak bu sitelerin yöneticileri Amerikan istihbarat sitelerine erişmeyi, onları elektronik olarak hacklemeyi ve eski Başkan George Bush yönetimi dönemine ait bilgilere ulaşmayı başarmışlardır. (Fisher, 2019: 380).

3.2.3. Sosyal Ağlar Aracılığıyla Ortaya Çıkan Terörizm ve Radikalizm:

Sosyal ağların yayılma süreci henüz 20 yılı aşmamış olmasına rağmen kısa dönemde modern yaşamın birçok yönünü yeniden şekillendirmiştir. Bu siteler, modern tasarımları, her kullanıcının ilgisini çeken gelişmiş yazılımları sayesinde küresel ölçekteki birçok olayda etkili siteler haline gelmeyi başarmıştır. Örneğin 2016 yılındaki ABD başkanlık seçimlerinde başkan Donald Trump'ın seçim kampanyası esasen Facebook sitesine dayanmaktadır. Trump, düşük maliyetli bir çalışmayla seçmenlere ulaşmayı başararak hedefini gerçekleştirmiştir. Sosyal paylaşım araçları esasen, internet üzerinden insanların kendi aralarında işitsel, yazılı ve görsel mesajlarını

paylaşabildikleri, etkileşim içine girebildikleri modern teknolojik uygulamalardan ibarettir. Bu araçlar yeryüzünde canlı toplumları oluşturmaya ve etkinleştirmeye çalışmaktadır. İnsanlar bu uygulamalar üzerinden ilgi alanlarını ve faaliyetlerini paylaşmaktadırlar. En popüler sosyal iletişim araçları ise şunlardır:

Twitter: 2006 yılında Amerika Birleşik Devletleri merkezli olarak Evan Williams, Noah Glass, Jack Dorsy ve Pease Stone tarafından kurulmuştur. Yüz kırk karakteri aşmayan ve tweet adıyla bilinen tek mesajlık blog yazılarla hizmet sağlamaktadır.(Bilton, 2013: 381).

Facebook: 2004 yılında yine Amerika Birleşik Devletleri merkezli olarak Mark Zuckerberg, Chris Hughes, Andrew Mccollum, Eduardo Saffrin ve Daston Moskowitz tarafından kurulmuş olup, alt dallarında Messenger ve İnstagram uygulaması yer almaktadır. Çok iyi bir program olma özelliğine sahip olan Facebook, 70'ten fazla dile hitap etmektedir (Hempel, 2009: 382).

viber: 2010 yılında kurulmuştur. Ücretsiz olarak anlık mesajlaşma konuşma video fotoğraf yazı ve ses mesajları gönderme hizmeti sunmaktadır. Farklı platformlarda işletim sistemi özelliğine sahiptir (Sutikno, 2016: 384).

Mixi: 2004 yılında Japonya merkezli olarak kurulmuş olup sadece Japonca hizmet vermektedir. Flickr: 2004 yılında kurulmuştur. Yahoo şirketine aittir. Birkaç farklı özelliklere sahip olup İngilizce, İtalyanca, Fransızca, Korece, Çince, Portekizce, İspanyolca ve Almanca dillerinde hizmet vermektedir. Video ve fotoğraf paylaşımı, saklama ve düzenleme hizmeti sunmaktadır (Takahashi, 2010: 385).

Tumblr: 2007 yılında David Carp tarafından kurulmuştur. Kullanıcılarına görüntülü video metin aktarımı ve sesli konuşma bağlantıları gibi birçok olanak sunan bir sosyal paylaşım blog uygulamasından ibarettir. Basit tasarımı, kullanıcılar arası yardımlaşma olanağı, sosyal ağ olarak iletişim sağlaması, ürün ve hizmet pazarlamada kullanılması ve kullanıcı gizliliğini koruması gibi özelliklerle öne çıkmaktadır (Jackson, 2014: 386).

Plurk: 2008 yılında kurulmuş olup, mikro blog hizmeti sunmaktadır. Kullanım kolaylığı ve İngilizce dil desteğine sahip olan program, tüm kullanıcılara en fazla 140 karakter ile durum gönderme olanağı sağlamaktadır (Russell, 2013: 387).

Orkut: 2004 yılında kurulmuş olup mülkiyeti Google'a aittir. 48 dilde hizmet verme özelliğine sahiptir (Chen, 2009: 388).

Myspace: 2003 yılında Thomas Anderson tarafından kurulmuş olup, sadece siteye kayıtlı üyeler arasında etkileşimli bir ağdan ibarettir. Kullanıcılara fotoğraf, müzik ve video gibi materyaller yayınlama, bloklara yorum yazma ve birbirlerine mesaj göndermelerine imkân sağlamaktadır. Öte yandan birçok sosyal paylaşım sitesi de bulunmaktadır. Bunlar;

Blog oluşturma siteleri: bilgi paylaşım ve iletişim siteleridir. Ayrıca, önemli konularla ilgili yardım toplama siteleri de vardır. Wiki sitesi buna bir örnektir. Etkinlik siteleri; Twitter ve Meetup sitesi gibi siteleri saymak mümkündür (Thelwall, 2009: 389).

Hi5: Kullanıcılar arasında doğrudan iletişim kurulan, arkadaş arama, kullanıcıların hayatında meydana gelen yenilikleri öğrenme gibi kullanıcılarının etkinlik ve ilgi alanlarını paylaştıkları sosyal paylaşım siteleridir. Good reads gibi web siteleri buna örnektir (Arrington, 2007: 391).

Bilgi toplama siteleri: Waze sitesi buna örnek olarak verilebilir. İlgi alanı paylaşma siteleridir ki, takım oluşturma, sosyal gezinme ve işbirliği sağlama siteleri gibi sitelerdir.

Newsvine: En önemli sosyal haber sitelerinden biridir. Örneğini, Google kitaplar ve google dokümanlar gibi siteler metin düzenleme ve yönetme siteleridir.

Multimedya siteleri: Bu siteler de canlı yayın ve video paylaşımı siteleridir. "Video Sharing" buna örnek olarak verilebilir.

Sanat ve fotoğrafçılık siteleri: Örneğin, "flickr sitesi" Müzik ve ses paylaşım sitesidir.

Video yayın ve depolama siteleri: Youtube sitesi örnek olarak verilebilir. Her türlü ses görüntü ve kayıt olanağı sunmaktadır.

İnceleme ve görüş bildirme siteleri: Toplu yarışma, soru ve cevap siteleri bu türden sitelerdir.

Ürün inceleme siteleri: Sosyal iletişim ve eğlence siteleridir. İnternette çevrimiçi olarak oynanabilen sosyal oyun siteleridir (Boer, 2008: 366).

3.2.4. Şiddet ve Nefret Söylemlerinin Yayılmasında Sosyal Medya Araçlarının Etkisi:

Birçok olumlu yönlerinin yanı sıra her yeni teknolojide daima olumsuz bir takım sorunlar da bulunmaktadır. Sosyal paylaşım araçları da bundan istisna değildir. Sosyal paylaşım araçları da bir takım nedenlerden dolayı terör ve aşırılık söylemlerinin yayılmasına uygun ortam oluşturmuştur. Bu nedenleri şöyle sıralayabiliriz:

1) Sosyal paylaşım siteleri, geleneksel medya sitelerine göre ses kayıtları ve yazılı yayınlarıyla teröristler tarafından iletişim kurma ve fikirlerini geniş bir şekilde yayma noktasında olumsuz yönde kullanılabilmektedir. Örneğin bugün Facebook, Twitter, Instagram ve Youtube gibi sosyal paylaşım platformları kişilerin mesajlarını anında dünyanın her yerindeki kullanıcıların video ya da sesli mesaj şeklinde yayılmasını sağlamakta ve tüm hizmetler ücretsiz olduğu gibi kişi kimliğini izleme imkânı da bulunmaktadır. Bu da terör guruplarının hızlı paylaşım olanağından yararlanmasına olanak tanımaktadır (Theohary, 2011: 367).

Sosyal paylaşım siteleri, Avm software şirketine sahip olduğu Paltalk odaları gibi sohbet odalarına sahiptir. Bu şirket 1998 yılında New York şehrinde kurulmuş özel bir şirkettir. Şirket dört milyondan fazla abonenin bu hizmetten yararlandığını iddia etmektedir. Öte yandan sosyal paylaşım siteleri, kullanıcılara grup oluşturma imkânı verilmektedir. Bu özellik benzer ideolojiye sahip kişilerin özel gruplar kurarak gizli bir şekilde haber, fikir ve bilgi paylaşımı yapmalarına imkân tanımaktadır. Bu nedenle terör odakları, nefret ve şiddet içerikli sohbet odaları veya web siteleri üzerinden iletişim kurabilme imkânı sağlamaktadır.

Facebook Youtube ve Twitter gibi sosyal paylaşım sitelerinin ortaya çıkması, aynı zamanda nefret söylemlerinin daha fazla yayılmasına neden olmuştur. Üzerinde akıllı telefon cihazı bulunan her insanın bunlara anında ve kolayca ulaşabilmesine neden olmuştur. Yeni Zelanda'daki iki camiye yapılan saldırılar buna bir örnektir. Bu saldırılar Facebook üzerinden canlı yayınlanmış, ardından 8chan ve Youtube üzerinden de yayınlanmış, Reddit üzerinden yorumlar yapılmış ve teknoloji şirketleri tarafından yayılmasını engelleyecek işlemler yapılamadan dünyanın her yerine yayılmıştır. Böylece sosyal paylaşım siteleri nefret hislerinin yükselmesine neden olmuş ve beyaz ırk terörünü Müslümanlara, diğer dinlere, ırklara ve toplumlara karşı âdeta desteklemiştir. Yeni Zelanda saldırganının 87 sayfalık bildirisi de kendilerini diğer gruplara karşı üstün gören beyaz ırk propagandası ile dolu olup, bu bildiri de aynı şekilde internet üzerinden paylaşılmıştır.

2) Sosyal medya üzerinden yayılan medya şiddeti, toplumlarda suça karışma oranında önemli artışlara yol açabilmektedir. Bu nedenle internet üzerinden kullanılan tekniklere ve ödül sistemlerine odaklanmak gerekir. Aslında basit ve önemsiz gibi görünen bu programlar, toplum zihninde yer bulmakta ve daha büyük saldırılara zemin hazırlamaktadır. Çünkü sosyal medya platformlarının büyük çoğunluğu, performans suçlarını teşvik eden prim veren ve ortaya çıkaran çerçevelere sahiptir. Öte yandan yeni basın çevresi birtakım yeni "performans suçluları" ortaya çıkarmıştır ki, bunlar izleyiciler tarafından izlenme rekoru kırma hevesi ile başlayan ve daha sonra izleyicilerden en çok beğeni almak için işlenen yasa dışı eylemlerdir. Suç işleyen kişi veya bir başkası suçun videosunu kaydeder, ardından video Facebook, Youtube ve Twitter gibi sosyal paylaşım sitelerinde video kaydını yayınlar. Yaptığı işin yanlış veya yasak bir fiil olduğunu düşünmeden, izleyici sayısının fazlalığı ve ne kadar kişinin beğenisini aldığıyla kendisini avutur. Şiddet ve nefret suçu gösterimlerinin 2005 yılında İngiltere'de ortaya çıkan bir sapkınlık olan "Mutlu Tokat" video kesitleriyle birlikte arttığı görülmüştür. Bunlar belirli bir kurban hedef alınarak saldırının telefon kamerası veya normal kamerayla kaydedildiği basit dereceden şiddet suçlarından ibaretti. Ancak zamanla gençler arasında yayılmış olan bu tür suçlar sıradan davranışlar gibi görülmüş, bir takım dayak ve cinsel saldırıları normal hale getirmiştir (Jewkes, 2013: 258).

3) Ne gariptir ki zamanımızda elektronik suçların eğlence ve avuntu aracı olarak kullanılması gibi yeni bir tarz ortaya çıkmıştır. Saygın toplumun kontrolünden çıkan teknoloji korkuyu doğurmuştur. Sırf ilgi arayan birçok suçlu bulunmakta olup, bu kimseler herhangi birilerinin dikkatini çekmek için suç işlemektedirler. Dolayısıyla suç, çok geniş bir kitlenin önünde belgelenmekte ve sosyal medya aracılığıyla yayılmaktadır. Performans suçunun gelişmesine neden olan en önemli faktörlerden biri de 20. yüzyılda "şöhret olma" kültürünün ortaya çıkması ve birçok kimsenin özellikle de sosyal medya araçları yayıldıktan sonra can revan çalışmasına neden olmuştur. Surette'ye göre cani, performans suçu izleyicisinin kendisini yasal olarak meşrulaştırıldığını düşünmekte ve toplumsal olarak kabul edilebilir kıldığını iddia etmektedir (Surette, 2015: 255).

4) Performans suçunun failleri olay öncesinde ve esnasında oluşturdukları elektronik arşivden kaçınılmaz olarak ortaya çıkacak ilgiden eğlence duymaktadır. Bu sahnenin Televizyon kanallarında, Facebook ya da Youtube gibi internet sitelerinde yayılması sonucu, suçun failleri yıldızlara dönüştürmektedir. Bu da suçlular için bir nevi ödül sayılmaktadır (O'Dea, 2015: 256).

3.3. Sosyal Medya Araçlarını Koruma Stratejileri:

Sosyal medya sitelerinin ilk ortaya çıkışından bu yana, belirli hedeflere ulaşmak isteyen bir takım topluluk ve gruplara çok sayıda kişisel ve halka açık ağlar ortaya çıkmış ve başlangıçtan günümüze internet siteleri hızla gelişerek hayatımıza girmiştir. Sosyal paylaşım ağlarının gelişmesiyle birlikte aralarındaki üstünlük yarışı, halk nezdinde en çok takip edilme sayısına göre gerçekleşir hale gelmiştir. Farklı toplumlardaki kullanıcı sayısındaki artış nedeniyle popüler olan ağlar listede baş sıraya oturmuştur. Örneğin, bir sitenin ortalama ziyaretçi sayısı asgari 100 milyonlara ulaşmış durumdadır. (De Kare-Silver, 2011: 368).

Sosyal paylaşım araçlarının toplumlara kazandırdığı büyük faydalara rağmen kötü yanları da bulunmaktadır. Yalan haberlerin yayılması, gerçekleri saptırarak verme ve teknolojiyi kötüye kullanma gibi nedenlerle sosyal paylaşım ağlarına dayalı büyük toplumsal zararlar meydana gelmektedir. Kimi zaman kullanıcı bireyleri çev-

relerinden soyutlamakta, zihinsel ve bedensel tembellik doğurarak hareketsizliğe yol açmaktadır. Sosyal ağlar, bazı ahlaksız materyaller içerdiğinden dolayı gençler ve çocuklar için tehlike oluşturmaktadır. Yine bu ağlar, kullanıcılarının derin tutkularından dolayı, sorulan bir soruya düşünmeden cevap vermeleri, hayal âleminde yaşamaları, düşünce eksikliğine yol açmakta ve sorumsuz sonuçlar doğurmaktadır. Bu nedenle, çoğunlukla akıl yürütme ve sağduyulu olma özelliklerini kaybettiren siteler olarak kabul edilmektedir. Caddelerde yürürken veya yollarda motorlu araçlar kullanırken pervasızca kullanılması nedeniyle kazaların artmasına neden olmaktadır. Sosyal medyada fazla vakit harcanması neticesinde temel ve gerçekçi becerilerin gelişiminde yetersizlik gözlemlenmektedir.

Sosyal medya bağımlılığı, bireylerinin birbirlerine yeterince zaman ayırmamasına ve dolayısıyla birbirlerini anlamamasına neden olabilmekte, hatta ailevi sorunları büyütebilmektedir. Dini bilgiler, gerçek din âlimlerinden alınması gerekirken, dini görünümlü yanlış fikirler ve radikal bilgiler daha etkin olmaktadır. Bireyler arasında sosyal ilişkilerin bozulmasının yanı sıra, aşırılık, terör, şiddet ve nefret yayılmaktadır. Sosyal medyanın diğer birçok zararı günümüz toplumunda hissedilmektedir. Bu nedenle bu sitelerin güvenli hale getirilmesi ve doğan zararın hükümetlerin uyguladığı programlar doğrultusunda azaltılması, hükümetlerin siber toplumu yönetecek birtakım standartları ortaya koyma rolünü üstlenmesi, ayrıca özellikle de farklı kıtalarda ulus ötesi küresel şirketlerin yayıldığı bir ortamda, sorumluların bazı tedbirleri ivedilikle uygulaması gerekmektedir.

3.3.1. Uluslararası Ülkeler ve Platformlarca Alınması Gereken Tedbirler:

1) Yeni Yasaların Oluşturulması:

Dünya devletleri birkaç yıldır elektronik suçlarla yasal olarak mücadele etmeye yönelmiştir. Gelişmiş ülkelerde modern suç olarak nitelendirilebilecek söz konusu fiillerle ilgili kanun ve yönetmelikler hazırlamanın önemine dikkat çekilmektedir. Her geçen gün bu gibi konularda yeni kanunlar duyulmaktadır. Ülkeler arasında özellikle de terör ve radikalizmle mücadele konusunda deneyim ve uzmanlık paylaşımı yaşanmaktadır.

Bu bağlamda, Avustralya hükümeti kısa bir süre önce terör saldırılarının internet ve sosyal ağlar üzerinden yayılmasını önlemek için yeni yasa tasarısı hazırlamıştır. Tasarı, muhtemel terör faaliyetlerinde, Yeni Zelanda'nın Christchurch kentindeki iki camiyi hedef alan terör saldırısında aşırı sağcı teröristin yaptığı katliamı 17 dakika boyunca Facebook platformu üzerinden canlı yayınla duyurmasına benzer şekilde sosyal ağların kötüye kullanılmasını önlemek amacıyla oluşturulmuştur.(Williams, 2011: 370).

Avustralya kanunları, sosyal paylaşım platformları bulunan ve bu kanalları yöneten şirketleri muhatap almakta, onlara terör vs. içeriklerinin derhal silinmesi ve hemen kaldırılmasına hazırlık bağlamında hızlıca tespit yapabilecek alternatif yollar bulma zorunluluğu getirmektedir. Avustralya hükümeti, sosyal medya araçlarını işleten internet devlerine milyarlarca dolarlık mali yaptırımlar uygulayabildiği gibi şiddet içeriklerini hızlı bir şekilde ortadan kaldırmayan hatalı şirket yetkililerine de hapis cezası verebilmektedir.

Bu kanun, yönetici şirketin şiddete, radikalliğe ve terörizme yönlendiren içeriklerden sorumlu tutulmamasını doğru bulmamaktadır. Kanun koyucu, kanun ve yönetmelikler aracılığıyla büyük teknoloji şirketleriyle ahlaki ve manevi sorumluluk temelinde bir ilişki kurmaktadır. Kimi ülkeler de uygulama engeli veya yasaklama gibi faaliyetleri önceleyen bir mantıkla hareket etmektedir. Birçok devletten fazla nüfuza sahip kıtalar ötesi teknoloji şirketlerine şimdiye dek sadece baskı yapmakla yetinilmişken, Avustralya'nın yaklaşımı konunun uzmanları tarafından takdire şayan bir gelişme olarak değerlendirilmektedir.(Zeng, 2014: 371).

2) Sosyal Medyaya Denetim Uygulanması:

Bütün dünya ülkelerinin farklı özelliklere sahip hükümet ve güvenlik güçlerinin, terör olayları neticesinde sosyal medya nedeniyle toplumun gördüğü zararların engellenmesi adına ivedilikle çalışması gerekmektedir. Zira terör olaylarının akabinde basın araçları ve sosyal medyanın önemli bir rolü bulunmaktadır. Basın ve yayın araçları, sosyal medya kaynaklı terör olaylarının kamuya verdiği zararları artırabildiği gibi, bazen de bu etkileri azaltabilmekte ve hatta durdurabilmektedir. Bu nedenle

yetkililer, terör olaylarını takip eden elektronik tedbirler almalı, karşı yansımaları yönetme stratejileri ortaya koymalı ve bunları uygulamalıdır (Combs, 2017: 372).

Cardiff Üniversitesi Araştırma ve Güvenlik Enstitüsü'nün, Michigan Eyalet Üniversitesi, Kanada Western Üniversitesi ve Sidney Yeni Güney Galler Üniversitesi iş birliğiyle hazırlanan raporda, Birleşik Krallık, Amerika Birleşik Devletleri, Kanada, Yeni Zelanda ve Avustralya'nın "Terör Saldırılarının Değerlendirilmesi" konusunda hazırladıkları raporlarda sürekli biçimde sosyal medyanın rolüne işaret edilmiştir. Terör olaylarının arka planında basın –yayın araçları ve sosyal medyanın rolü hakkında yayınlanan araştırmaların tamamına göre, detayların incelenmesi sonucu terör olaylarının ilk saldırının ardından şok dalgaları yaratıp vatandaşlarda korku ve paniğe neden olduğu gözlemlenmiştir.

Farklı gruplara ait iletişim kanallarının artması, aynı olayın değişik şekillerde yorumlanmasına neden olmaktadır. Bu durum ise olaya ilişkin farklı birtakım anlatı ve değerlendirmeleri doğurmaktadır, dolayısıyla bazı kesimlerde şiddetli tepkiler oluşabilmektedir. Teröristlerin çalıştığı hedef de çoğunlukla toplumda aşırı tepkilerin gözlemlenmesidir. Böylelikle sosyal medyanın rolü bazen kin ve nefret söylemlerinin yayılmasına aracılık yapmasından ötürü olumsuz olmakta, sosyal medya üzerinden bilerek ya da bilmeyerek terörün rol ve hedefleri gerçekleştirilmektedir. Hükümetler, devlet birimleri ve kamu güvenliğinden sorumlu yetkililerin olumsuz yansımaları azaltmak için, güvenilir bilgi sağlayan kanallar oluşturması zorunludur. (Sheppard, 2006: 373).

Hükümetler, internet trafiğini yönlendirmek ve disipline etmek için merkezler kurmak suretiyle, dünyanın her yerinde önemli internet ağlarının güvenlik ve istikrarını sağlamalıdır. Yine bir takım savunma mekanizmaları oluşturarak internet kullanıcılarını olumsuz etkileyen muhtelif tehditler karşısında, şirket sahiplerine caydırıcı ve disipline edici teknik prosedürler uygulamalı ve yasalara karşı yükümlü tutmalıdır.

3. Kullanıcıların Bilinçlendirilmesi:

Özellikle çocuk ve gençlerin sosyal medyayı sorumsuzca kullanmalarının önüne geçilmeli ve gerekli bilgilendirme yapılmalıdır. İnternette gizli risklerin kullanıcılara duyurulması ve gizliliğin korunmasının önemi ile ilgili kurs ve seminerler düzenlemek aracılığıyla halk bilinçlendirilmelidir. Modern teknolojinin olumlu yönlerinden faydalanabilmesi amacıyla akıllı telefonların ideal şekilde kullanılması ve uygun kullanım koşullarının belirlenmesi için, hükümet makamları ve özel şirketler iş birliği halinde olmalıdır (Zolait, 2014: 374).

4. İnternet Kullanımında Fayda Sağlayacak Yol ve Yöntemlerin Geliştirilmesi:

İnternet kullanımı esnasında karşılaşılabilecek tehditlere karşı ahlak ve davranış değerlerini destekleyecek olumlu tedbirler alınmalıdır. Örneğin, çocukların sanal dünyadaki davranışlarını yönlendirme konusunda bilinçli aile gözetimi ve koruması devreye sokulmalı, bu konuda ulusal kurumların ve hükümet birimlerinin çabaları desteklenmelidir (Dredge, 2014: 375).

5. Elektronik Koruma Sistemi, Anti-virüs Programlarının Sağlanması:

Farklı sektör ve katılımcı bireylerden oluşan toplumun her kesimini kapsayacak şekilde internet kullanıcılarına güvenli bir hizmet sunulabilmesi için filtreleme programları gibi bir takım koruma sistem ve araçları geliştirilebilir. Zira internette yapılan bilinçsizce gezintiler, farkına varmadan gençlerimizin milli ve manevi değerlerini ellerinden almaktadır. Bu nedenle onları yozlaşmış kültürlerin etkisinden kurtarmak için alınacak tedbirler kaçınılmaz hale gelmiştir (Hasebe, 1995: 376).

5. İnternet Kullanımında Etik Kurallarının Geliştirilmesi:

İnternet ve sosyal medya üzerinden hoşgörü değerlerinin ön planda tutulması, sorumluluk bilincinin aşılanması, olumsuz davranışlardan uzak durulması gibi olumlu davranışlar telkin edilmeli ve genel ahlak kuralları çerçevesinde hareket etme prensip haline getirilmelidir. (Westermeir, 2003: 377). Etik meseleler iki tür davada

ortaya çıkmaktadır: birincisi, bazı web siteleri, web sitesinin görüntüleneceği ülkelerin yasalarını aşmak için diğer ülkelerde bulunmaktadır. Bir süredir, ücretsiz indirilebilen müzik siteleri, etkinliklerinin yasak olduğu ülkelerde işlenmiştir Etik meseleler iki tür davada ortaya çıkmaktadır: birincisi, bazı web siteleri, web sitesinin görüntüleneceği ülkelerin yasalarını aşmak için diğer ülkelerde bulunmaktadır. Bir süredir, ücretsiz indirilebilen müzik siteleri, etkinliklerinin yasak olduğu ülkelerde işlenmiştir (DeLorme, 2001: 378).

3.3.2. İnternet Şirketleri ve Sosyal Medya Yöneticilerinin Üzerine Düşen Görevler:

Son zamanlarda, Facebook, Microsoft, Twitter ve Google programları Avrupa hükümetleri tarafından, sosyal paylaşım sitelerinde ve İnternet'te terörle mücadele konusunda yeterince çaba göstermemekle eleştirilmektedir. Birçok terör mağduru aile de aynı sebeple bu şirketlere dava açmıştır. Microsoft da dâhil büyük teknoloji şirketleri 2018 yılının sonunda Fransa ile ortaklaşa hazırladıkları bir bildiriye imza koydular. Bildiride, "internete köklü düzenleme", "elektronik saldırılar" gibi tehditlerle mücadele işbirliği amaçlanmıştır. "Paris elektronik dünya güvenlik ve emniyet çağrısı" adlı bildiri, internete denetim getirilmesi, kin ve nefret söylemlerinin internet ortamından çıkarılması ve engel olunmasını istemiştir (Shull, 2019: 379). Bildiriyi, birçok Avrupa ülkesi desteklerken, Çin ve Rusya ise, reddedilmiştir. Uluslararası ülkelerde gerçekleştirilen hükumet seçimlerine internet üzerinden yapılan müdahalelere karşı alınacak koruyucu tedbirlerin desteklenmesi, dolandırıcılık ve hırsızlıkların engellenmesi zihinleri tahrip eden diğer zararların önlenebilmesi için bir takım tedbirler tedarik edilmelidir. Bunları şu şekilde sıralamak mümkündür:

1. Terör gruplularının kin ve nefreti destekleyen yayınlarına ulaşarak her türlü hareketlerinin dikkatlice incelenmesi, takip edilmesi ve deşifre edilebilmesi için teknolojinin ulaştığı en son adım olan yapay zekâ kullanılmalıdır. Facebook'un yayın editörü Monika Bickert şöyle demektedir; "Terörle mücadele yöntemleri, teröre yönelik medya destek yöntemlerine göre değişmektedir. Terör ve şiddet içeren yayınları artık izlenmeden önce engelleme program ve teknik araçları kullanmaya odaklanıyoruz. Facebook'u bir terörle mücadele

ortamı olarak görmeliyiz. Bu bağlamda sosyal medyada teröre destek propagandalarını engellemek için elimizden gelen çabayı sarf ediyoruz. Facebook yönetimi, terörle mücadele uzmanından oluşan 150 kişilik bir hücre oluşturmuştur. Bu hücre, iletişim ve destek yöntemlerini sürekli değiştiren terör destekçilerini ortaya çıkarmak için şirketimizle sürekli ve doğrudan temas halindedir (Bickert, 2017: 380)."

2. Sosyal medyaya sahibi şirketlerin bir eğilimi bulunmalı, bu eğilim doğrultusunda medyada kitlesel şiddet söylemlerinin önüne geçilmelidir. Böylece internette dikkat çekme ve şöhret olma hedefleri yolunda suç işleyenlere prim verilmemelidir. Bu site ve platformlarda yayınlanan şiddet suçu ve nefret söylemleri içeren videoların kaldırılması ve yeniden yayınlanmasının engellenmesi noktasında daha bilinçli hale getirilmelidir (Chen, 2018: 381).

3. Toplumdan topluma farklılık gösteren ihtiyaç ve isteklerin doyurulması için davranış modellerine odaklanılmalıdır. Sosyal medyayı yöneten şirketlerin, internet kullanıcılarının ihtiyaçlarını belirli standartlarla ortaya koymaları gerekir. Dolaşım esnasında ortaya çıkan yeni ihtiyaçların ağ içerisinde belirli sitelere girmeye ve kullanmaya sebep olan nedenleri göz önünde bulundurmamız gerekir. Bunun için siteleri kullanım yoğunluğu, tüketicilere sunulan materyal kalitesi ve nesnelerin kötü kullanımından doğan zararları azaltma girişimleri izlenmelidir (Akay, 2013: 382).

Üçüncü Bölümün Sonu:

Çalışmamızın bu bölümünde, genel anlamda terörizm kavramına açıklık getirmenin yanı sıra, özelde ise elektronik terörizm kavramını netleştirmeye çalıştık. Terör örgütlerinin, elektronik araçlarla gerçekleştirdikleri terör eylemlerinin evrimini ve terörizmin belirli bir dine veya ırka isnat edilemeyeceğini, aksine farklı din ve etnik guruplar tarafından faaliyet sürdürdükleri konusunu ele aldık.

Çalışmamızda terörizmin, ideolojik radikal fikirlerden doğduğu ve bu tür yasa dışı odakların daha ziyade aşırılık yanlısı bireyler tarafından temsil edildiği vurgulanmıştır. Bu suç şebekelerinin belirli toplumlar, bireyler veya hükümetler arasına

korku ve panik ortamı oluşturmaya ya da düşüncelerini şiddet kullanarak eyleme dönüştürmeye ve belirli kurumlara zarar vermek amacıyla tahrip etmeye yeltenen yasadışı guruplar olduğu ortaya konmuştur.

Genelde, terör örgütlerinin amaçlarına ulaşmak için kullandıkları metotları ortaya koymanın yanı sıra, özel de ise elektronik araçların kullanımı, dijital ve siber saldırılarının gerçekleştirilmesinde bilgi teknolojisinden nasıl yararlandıkları analiz edilerek bu oluşumlara karşı internete sansür ve anti virüs uygulamaları gibi tedbir alan bir takım ülkelerin önlem ve çalışmalarına örnekler verilmiştir. Amerika Birleşik Devletleri, İngiltere ve Almanya'da elektronik kontrol araçlarıyla teröristleri hedef alan istihbarat faaliyetleri ve alınan önlemler arasında karşılaştırmalar yapılmıştır.

Bazı ülkelerin ulusal güvenliği koruma sloganıyla, internete sansür uygulamaya yasalarında izin verdiğinden ve bazı insan hakları savunucularının bu yasaların elektronik suçlara karşı caydırıcılık sağlayacağı nedeniyle desteklediğinden bahsederek, siber suçlarla mücadeleye dikkat çekilmiştir.

Terör örgütlerinin internet programları, iletişim ve şifreleme hizmetleri aracılığıyla yararlandıkları en önemli program ve uygulamalara değinilerek bu araçlar üzerinden farklı toplumlar arasında kin, nefret ve düşmanlığı körükleyici söylem ve faaliyetlerde bulundukları ortaya konmuş ve bu noktada sosyal medyayı güvence altına alacak stratejilerin geliştirilmesi gerektiğine vurgu yapılmıştır.

Öte yandan siber saldırıları azaltmaya katkıda bulunacak etkili yasalar hazırlanmasının önemine dikkat çekilerek caydırıcı tedbirler çerçevesinde modern teknolojik tekniklerden en iyi şekilde yararlanılması gerektiğine işaret edilmiştir. Bu nedenle hükümetlerin, uzmanlaşmış personel ihtiyacını karşılayabilmeleri için bu alanda eğitimin önemine vurgu yapılmıştır. vatandaşların huzur ve güven içerisinde teknolojiden yararlanmasını temin etmek, terör şebekeleri ve hacker saldırılarına karşı (özel bilgilerin, gizlilik ilkesi gereği) insan hak ve özgürlükleri çerçevesinde korunmasının, her devletin vatandaşlarına karşı yükümlülüğü olduğu belirtilmiştir.

DÖRDÜNCÜ BÖLÜM

4. ULUSAL GÜVENLİĞİN BİR BİLEŞENİ OLARAK IRAK'TA SİBER GÜVENLİK

4.1. Irak'ta Ulusal Güvenlik Kavramı ve Başlıca Kurumları:

Milletlerin ulaşmak istedikleri hedefler ve genel stratejileri farklılık göstermektedir. Çünkü genellikle, siyasi, ekonomik ve sosyal alanlarda, çeşitli çevre koşullarıyla birlikte, ulaşmak istedikleri hedefler orantılı olan belirli sütunlara dayandıkları için, halkın belirli bir zamanda ulusal güvenliğe ulaşma istekleri söz konusu olabiliyor. Bu yüzden alandaki kapsamlı güvenlik stratejisini inceleyerek "Irak'ta ulusal güvenlik" kavramını ekonomik, sosyal, politik, kültürel ve askeri boyutlarıyla tanımlayarak belirtmemiz gerekmektedir.

Irak'ın, özellikle 2003'te ABD tarafından işgal edilmesiyle başlayan altyapının çökmesive ve ardından çekilmesiyle baş gösteren süreçte ülkenin sosyal yapısı tahrip edilmiştir. Irak'ın işgaliyle ortaya çıkan durum, karmaşaya neden olmuş ve bir çeşit kültürel zenginlik faktörü olmaktan ziyade, bir dengesizlik göstergesi olarak etnik, dini ve ulusal unsurlar daha çaplı boyutlarda sorun almaya başlamıştır. Bu sosyal yapının öncelikli olarak dikkate alınması gerekmektedir. Çünkü dış sadakatlere bağlı ve dış çevresel desteklere dayalı etnik, ulusal ve dini ayrışmalar, giderek çeşitli sorunları beraberinde getirmiş ve kaçınılmaz olarak önemli bir güvenlik açığı yaratmıştır. Bu güvenlik açığı da kuşkusuz Irak gibi bir ülkede, ülke güvenliğini ve istikrarını olumsuz yönde etkilemiştir.

Sonuç olarak, "Irak'ın ulusal güvenliği" kavramı, Irak devletinin, başta iç ve dış güvenlik sıtratejisi olmak üzere, Irak halkının hayati değerlerini koruma hedefini kapsamaktadır. Askeri güçler, ekonomik kabiliyetler ve sosyal uyum gibi Irak'ın çeşitli mekanizmalarını içeren alanların tümü, öncelikli güvenlik ve koruma sağlayan genel bir çerçeveyi içermektedir. Irak, bu zeminde geniş çapta ulusal güvenliğin hedeflerini daha da büyüterek geliştirebilecektir. Irak'ın dış güvenliğinin savunulması, bütünüyle güçlü bir askeri sistemin kurulmasını gerektirmektedir. Ülkenin iç güvenliğinin sağlanması, vatandaşların eşitlik ilkesi doğrultusunda sosyal çevrede meşru

haklarının güvence altına alınması ve adaletin sağlanmasıyla kendilerini evlerinde güvenli hissetme ihtiyaçlarını karşılamayı amaçlamaktadır(al-Jubouri, 383, 2006).

2003'ten sonraki Irak'ın siyasi sistemi, ne politik ve ekonomik istikrara tanıklık edebilmiş, ne de net bir ulusal vizyonu benimseyen iç ve dış politikada sağlam bir stratejiye dayanma imkânı bulabilmiştir. Yeniden toparlanan Irak'ın, ulusal güvenliği için önemli bir strateji geliştirmesi, Irak halkının politik sisteminin ulusal çıkarlarının somutlaştırıldığı bir dizi verinin hayata geçirilmesinden ve bir takım somut adımların atılmasından geçmektedir. Bu veriler, alınacak tedbirler ve atılacak adımların en önemlileri şunlardır:

Birincisi: Irak ulusal güvenliğinin sağlanması için yeni bir Irak ulusal stratejisi belirlenmelidir. Irak halkının sosyal, dini, ulusal ve etnik yapısı dikkate alınarak atılcak adımlar ve önemli hedefler içermelidir. Irak siyasi arenasında yer alan siyasi partiler, doktrin ve dine dayanan dini partiler ya da siyasi kimliklerini belirlemede mezhep ve dini temel alan ulusal partilerdir. Ayrıca, Irak'taki laik siyasi akım safları birleştirmedeki zayıf siyasi rolüyle ve ülkenin liderliğinde etkili liderlik konumlarına ulaşma ile karakterize olunmalıdır(Atwan, 384, 2017).

İkincisi: Irak ulusal güvenliği için bir strateji geliştirirken Irak Anayasasına ve kanun maddelerine uyulmlu olmalıdır. Çünkü bu Irak'ın ulusal güvenliğine yansıyacak ve aynı zamanda Irak devletinin kurumları arasındaki işleyişini sağlayacaktır. Aksi takdirde Anayasa ile düzenlenmiş olan farklı kurumlar arasındaki yetki dağılımında düzensizlik ve dengesizlik oluşturacaktır(al-Ansari, 385, 2019).

Üçüncüsü: Irak ulusal güvenliği için uygulanacak bir strateji, uluslararası koşulları ve Irak'ı çevreleyen dış bölgesel ortamı dikkate almalıdır. Aynı zamanda Irak ile komşu ülkeler arasında bölgede güvenliğin temin edilmesi ve ortak istikrarın sağlanmasını garanti edecek şekilde ortak çıkarlara hizmet etmesine dikkat edilmelidir(Saleh, 386, 2019).

Dördüncüsü: Kapsayıcılık ilkesi çerçevesinde Irak ulusal güvenliği için ortaya konacak bir strateji, istikrarlı bir topluma ulaşabilmek için çeşitli siyasi, ekono-

mik ve sosyal alanlarda güvenliği tam olarak sağlama hedefini ortaya koyması gerekmektedir(Al-Ardawi, 387, 2015).

4.1.1. Irak Ulusal Güvenlik Bakanlığı (Ulusal Güvenlik Yüksek Kurulu):

2004 yılında kurulmuştur. "Irak Ulusal Güvenlik Konseyi" ya da "Irak Ulusal Güvenlik Danışmanlığı" adlarıyla da görevini icra eden kurum, bir nevi Bakanlar Kurulu görünümündedir. İstihbarat Daire Başkanlığı, İçişleri ve Dışişleri Bakanlığı, Adalet Bakanlığı, Maliye Bakanlığı gibi önemli kurumların güvenli bir şekilde işleyişlerini takip etmekte ve icraatlerinin işleyişini sağlamaktadır. Kurum, bir İstihbarat Direktörü, bir Ulusal Güvenlik Danışmanı ve iki Kıdemli Askeri Danışman tarafından temsil edilmektedir. Irak Ulusal Güvenlik Bakanlığı, Irak'ta toplumsal güvenliğin sağlanmasından ve bakanlıklar ile diğer kurumlar arasında ulusal güvenliği kapsayan çalışma ve politikaları koordine etmekten sorumludur. Irak'ın ulusal güvenliğini temin etmek ve güvenlik politikalarını geliştirmek amacıyla kurulmuştur. Irak Ulusal Güvenlik Danışmanlığı, ulusal güvenlik politikalarını geliştirmeyi amaçlayan bir kurum olarak, çeşitli güvenlik stratejilerini geliştirmek, bakanlıklar ile istihbarat teşkilatları arasındaki zorlukları gidermek, ortaya çıkan sorunları inceleyerek uygun politikalar geliştirmek ve koordine etmek, Irak halkının genel güvenliği, istikrar ve refahı için uygun kararları almaktan sorumludur. Ulusal güvenlik stratejisinin kapsamlı bir şekilde gerçekleştirilebilmesi, Irak'ın ve Irak halkının istikrar ve refahı odaklı bir güvenliğin sağlanması gerekmektedir. Bu ise, ancak uygun kararların alınması ve koordine edilmesiyle mümkündür. Kısaca, iç ve dış güvenliğin sağlanması şeklinde özetlenebilir. Buna, askeri, sağlık eğitim ve gıda gibi tüm sektörler dâhildir. (al- İraq, 388, 2004).

Konseyin Yetkileri:

- Ulusal güvenlikle ilgili stratejik planların gerçekleştirilmesini temin eden yasa taslakları dâhil, Irak'ın huzur ve güvenliği için özel politikaların araştırılması, Konseyin yetki alanı dâhilindedir.
- Çeşitli devlet kurumlarını, ulusal güvenlik çıkarına hizmet edecek stratejiler geliştirmeye yönlendirmek,

- Farklı kamu kurumları arasında ulusal güvenliği sağlayacak şekilde koordinasyon için gerekli mekanizmaların oluşturulması. Devlet kurumlarının meydana gelebilecek krizler ve afetlerle başa çıkma yeteneklerini geliştirmek ve bu tür kırizleri yönetebilme başarısı kazandırma çalışmalarını ortaya koymak,
- Ulusal güvenlik tehditlerine etkin şekilde yanıt verilmesini sağlamak adına Ulusal Güvenlik Stratejik Planının hazırlanmasını ve benimsenmesini denetlemek,
- Ülkenin karşılaşabileceği tehditler, riskler ve zorlukların kaynakları konusunda birleşik bir veri tabanının geliştirilmesini denetlemek,
- Ulusal güvenlikle ilgili, taslak safhasındaki sözleşmeler ve anlaşmalarla ilgili kararlar alınmadan önce, görüş bildirmek,
- Sıkıyönetim ve Genel Seferberlik ilan etme önerisinde bulunmak.(Bhar, 2013: 389).

Irak Ulusal Güvenlik (Bakanlığı) Konseyi, ABD'nin Irak'ı bilfiil işgal etmesinden sonra 11 Mayıs 2003- 28 Haziran 2004 tarihleri arasında Irak, Devlet Başkanlığı statüsünde olan Geçici Koalisyon Yönetimi tarafından kurulmuştur. Yönetimin başında bulunan Amerikalı sivil diplomat Lewis Paul Bremer'in emriyle, 2004 tarih ve 68 sayılı kararıyla onaylanmış ve kuruluş genelgesinin ön sözünde yer almıştır.

Ulusal Güvenlik Konseyi'nin misyonunda, Ulusal güvenlikten sorumlu Irak hükumeti ile kamu kurum ve kuruluşları arasında ulusal güvenlik politikasını kolaylaştırmak ve koordine etmekten sorumlu olduğuna dikkat çekilmiştir. Ayırca, Irak Ulusal Güvenlik Konseyi, bu konularda karar alma yetkisi bakımından Bakanlar Kurulu mesabesinde olup ana platformunu belirlemiştir. Kararın 1. Bölümünün ikinci paragrafına göre; yönetim otoritesinin, tümüyle geçici Irak hükümetine devredilene kadar, başkanlığını yaptığı Geçici Koalisyon İdaresinin idari direktörünün komutası, yönetimi ve kontrolü altında çalışacaktır. Bakanlar, Ulusal Güvenlik Komitesi'nin daimi üyeleri olarak, (İdare yetkisi Irak Geçiş Hükümeti'ne devredilene kadar) Geçici Koalisyon idaresinde var olacaktır. Yönetimin, geçiş hükümetine devri üzerine ise, Geçici Irak Hükümeti Başkanı, Ulusal Güvenlik Konseyine başkanlık edecektir. Bu daimi üyeler; İçişleri Bakanı, Dışişleri Bakanı, Adalet Bakanı ve Maliye Bakanından oluşmaktadır. Diğer bakanlar ise, başkanın isteği üzerine komitenin belirli toplantıla-

rına katılabileceklerdi. Bir bakanın seyahat veya fiziksel engellilik nedeniyle konseyin belirli bir toplantısına katılmasının mümkün olamaması halinde, milletvekillerinden biri veya bakanlığın belirlediği bir üst düzey bakanlık görevlisi tarafından temsil edilebilecektir. İlgili bakanlığın üst düzey delegeleri, tüm bakanların isimlendirilip ulusal güvenliğe katılmalarına kadar, Milli Güvenlik Konseyi'nin toplantılarına iştirak edebilirler şeklinde belirtilmiştir.

Irak Ulusal Güvenlik (Bakanlığı) Konseyi üyeliği; Irak Ulusal İstihbarat Teşkilatı Genel Müdürü ve Ulusal Güvenlik Danışmanı olmak üzere iki üst düzey askeri danışmandan oluşmaktadır. Ayrıca Irak'ta faaliyet gösteren çokuluslu kuvvetlerin komutanı, BM Güvenlik Konseyi'nin 1511 sayılı kararına istinaden ve müteakip diğer kararlar çerçevesinde Irak Ulusal Güvenlik Konseyi toplantılarına katılmaya davet edilebilir.(Law, 2004: 390).

4.1.2. Irak Ulusal İstihbarat Teşkilatı

2004 yılında Amerikan işgal güçleri tarafından Irak eski istihbarat servisinin kapatılmasından sonra, yeniden bir Irak Ulusal İstihbarat Teşkilatının inşa yetkisi, Geçici Koalisyon Otoritesinin 69 sayılı mevzuatı gereği CIA'ya verildi. Yeniden oluşturulan ve geliştirilen bu İstihbarat servisi CIA'nın gözetimi ve finansmanı altında şekillenmiştir. Anayasaya ve tanınmış insan hakları ilkelerine uygun olarak çalışacak olan Ulusal İstihbarat Servisinin görevleri; mevzuatta geçen düzenlemeleri hayata geçirmek, ulusal güvenliğe yönelik tehditleri değerlendirmeye alarak bu konuda bilgi toplamak, Irak hükümetine tavsiyelerde bulunmak, sivil kontrol altında ve yasama otoritesinin denetimine tabi olmak üzere şekillenmiştir. (Priest, 2003: 392).

Irak Ulusal İstihbarat Teşkilatı aşağıdaki konularda bilgi toplama ve ilgili istihbarat faaliyetlerini yönetme yetkisine sahiptir:

- Irak'ın Ulusal Güvenliğini tehdit eden unsurlar.
- Terörizm ve isyan hareketleri,
- Kimyasal, biyolojik veya nükleer silahlar gibi kitle imha silahlarının üretimi.
- Uyuşturucu üretimi ve ticareti,
- Tehlikeli organize suçlar. (Ajansı, 2019: 391).

İstihbarat Teşkilatının önemine binaen, 2013 yılında Nuri el Maliki başkanlığındaki Irak hükümeti, Temsilciler Meclisinde tartışmaya açılması üzere bir İstihbarat teşkilatı yasa taslağı önerisi hazırlamıştır. Teşkilatın başkanlık görevinin, Bakan düzeyinde ve Başbakana bağlı güvenlik danışmanı olarak sayılmasını da öngören 29 maddelik İstihbarat Teşkilatı Yasa taslağı önerisi Meclise sunulmuştur. Taslak görüşmeye alınmadan kısa bir süre önce Güvenlik, Savunma ve Hukuk Komitelerine de gönderilmiştir. Ancak bu yasa 2017 yılında değiştirilmiştir. Zira yasa, güvenlikten sorumlu makamların, Anayasa ile özgürlük hakları garanti altına alınan vatandaşların, başta cep telefonlarının dinlenmesi olmak üzere tüm iletişimlerin izlenmeye alınmasını, şahsi bilgilerine ulaşılmasını ve bireysel hak ve özgürlüklere müdahale edilmesini öngörüyordu. Bu da Irak Anayasasıyla çelişmekteydi. Çünkü Irak Anayasanın 40. Maddesi, "vatandaşların İletişim, posta, telgraf, telefon, elektronik ve diğer iletişim özgürlükleri garanti altındadır. Anayasal düzeni tehdit ve güvenlik gerekçesi dışında, yargı kararı bulunmaksızın izlenmesi, dinlenmesi veya açıklanmasına izin verilemez…" denilmektedir. (Al-Saeedi, 2016: 394).

Anayasa'nın 61. Maddesi 5. Bendinde; "Temsilciler Meclisi, Genelkurmay Başkanı ve yardımcılarını, Kuvvet Komutanları ile Birlik Komutanlarını ve üstlerini ve İstihbarat Teşkilatı Başkanını, atama yetkisine sahiptir."der.

61. Madde kapsamında yeni kurulan İstihbarat Organı ise, adeta Anti-Casusluk Birimi olarak faaliyet sürdürmektedir. Her türlü casuslukla mücadele eden bir organ olarak kabul edilmekte ve istihbarat çalışma sistemi içinde en önemli birim olarak karşımıza çıkmaktadır. Başta Irak'ta bulunan yabancı şahıs ve tesislerin, şirketler ve çalışanları dâhil olmak üzere faaliyetlerinin izlenmesi ve takibi, diplomatik misyonlar ve dış servis ajansları veya ülke dışına yapılan casusluk faaliyetleri, Siyasi, ekonomik, askeri ve diğer alanlarda gizli bilgi toplanması anayasanın izin verdiği salahiyyetle ilgili müdürlük tarafından ülke yararına takip edilir.

Bu İstihbarat Organı'nın, Milli Güvenlik Konseyi'nin hizmetinde olmasıyla, Devlet'in herhangi bir karar almadan önce uluslararası ikili ilişkiler ve anlaşmaların yapılmasından önce, ya da ülke güvenliğine karşı herhangi bir silahlı çatışmaya ha-

zırlıklı olunması için gerekli bilgi veritabanın oluşturulması hedeflenmiştir. (Staaf, 2014: 395).

4.2. Irak Ulusal Güvenliğinin Bir Bileşeni Olarak Siber Güvenlik

4.2.1. Irak'ın İnternet Güvenliği Sorunları

Irak genelinde internet güvenliği ile ilgili sorunları özetleyecek olursak:

1. Kamu ve özel sektörde henüz yeterince güvenlik önlemlerinin alınmaması ve güçlü bilgi güvenliği merkezlerinin kurulmamış olması.
2. Irak'ta kısa ve uzun vadede bir Hükümet Güvenlik Stratejisi geliştirecek mevzuat ve düzenlemelerinin eksikliği. Buna, ülkede siber güvenliği sağlama görevini üstlenen hükümetin, kamu ve özel kuruluşların çalışmalarını denetlemede zayıf kalması eşlik etmektedir.
3. Tüm devlet kurumlarının güvenliğini sağlama konusunda uluslararası standartların uygulanmasından faydalanılmaması. İnternet ve elektronik sistemler kullanılarak kısa adı HIPAA olan, Özel Sağlık Bilgi Standartları gibi, diğerler Uluslararası güvenlik standartları acil olarak hayata geçirilmelidir. Ayrıca kredi kartı ile yapılan işlemlerde güvenliğin sağlanmasını temin eden kısa adı PCI DSS olan Veri Güvenliği Standardı gibi kuruluşların çalışma ve işleyişlerine ayak uydurulmalıdır.
4. Irak'ta Siber Güvenlik alanında uzman kadrolarının eksikliği: Mevcut olan yerel yeteneklerin gerekli bilgilerle güçlendirilmesi ile siber güvenlik alanında ileri teknik bilgi ve güvenliği konusunda uzman profesyonellerin acil olarak yetiştirilip görev alanlarına yerleştirilmesi gerekmektedir.
5. Irak'ta siber güvenlik konusunda şimdilik yeterince uzmanlaşmış bir kurumun olmaması. Mevcut olan yapı ise aralarında koordinasyon bulunmayan, hatta profesyonel işbirliği olmayan, farklı bölümlerde çalışma alanı oluşturulmuş müstakil bölümlerden ibarettir.(staff, 2019: 399).
6. İnternet hizmetleri sunan şirketlerin dışarıya bağımlılığı veya siber güvenlik tedarikçilerinin çoğunun Irak pazarından uzak olması, güvenlik açısından istikrarsızlığın devam etmesine neden olmaktadır. Bu durum, Irak siber güvenlik

sistemi için büyük bir tehdit oluşturan önemli bir noktadır ki Irak devleti, kamu kurumlarının bilgi akışını Irak sınırları dışında bulunan hizmet tedarikçisi uydularla sağlamak üzere sözleşme yaptığı gerçeğine dayanmaktadır. Önemli bilgilerin yabancı ülkelerin sunucuları üzerinden Irak'a geri dönüşü, gizli kalması gereken bilgi güvenliği sisteminin, bu ülkeler tarafından ihlal edilmesine olanak sağlamakta ve Irak bilgi teknolojisinin temel altyapısının dış müdahalelere maruz kalmasına ve o ülkelerin iradelerine teslim olmasına yol açmaktadır. Aynı zamanda bu durum, Irak'ın dünyanın birçok ülkesinin siber stratejik saldırılarına maruz kalması olasılığını da ortaya koymaktadır. Nitekim Irak sahasında bulunan çeşitli etkili ülkeler, geçmişte Irak güvenlik kurumlarıyla ilgili bilgileri gözetleme, sızdırma ve nüfuz etme yöntemleriyle, Irak üzerinden bazı ülkelere siber saldırılar gerçekleştirmek suretiyle bu ülkelere sızmak ve siber altyapılarını vurmak için koridor olarak kullanmıştır. Bu nedenle yerel şirketleri güçlendirecek altıyapılar oluşturarak yüksek talepli sunucu şirketler pozisyonuna getirecek potansiyel güç sağlamak kaçınılmazdır. Arz ve talep pazarında layık olduğu sahada temsil edilme olanağı sağladıktan sonra bu yerli ve güvenilir şirketlerle ortak yatırımlar yapmak gerekmektedir.(AL-Awadi 2016).

7. Irak hükümeti, yerel Bilgi Teknolojisi şirketlerini ve İnternet tedarikçilerini küresel gelişime ayak uyduracak kendi güvenlik çözümlerini aramaya teşvik etmelidir. Çünkü bilgi teknolojisinin hızla gelişmesi, saldırganların ellerindeki modern teknolojiye karşın yerel tedarikçi işletme sahiplerinin sadece kopyalanan sahte programlara güvenerek kendilerini yeni sistemlere karşı geliştirememeleri ve eski bilgi teknolojisi sistemlerindeki boşluklar nedeniyle siber korsanlar için açık hale gelmiştir. Hükümet ayrıca Irak'ta bulunan diğer tüm Bilgi Teknolojisi şirketlerini de kapsayacak şekilde önemli bir entegrasyon süreci başlatmalıdır. (Crocker 2017).
8. Siyasi partilerin, yetkili bakanlıklara ait çalışmalara müdahale ederek sözleşme ve projelerin çoğunu farklı bakanlıklarla paylaşma yoluna gitmesi, devlet mekanizması içinde gizli yürütülmesi gereken siber güvenlik hizmetleriyle ilgili antlaşma ve sözleşmelerin bazı partilerin ve siyasi figürlerin kontrolüne geçmesi, zaten var olan mali yozlaşmanın daha da derinleşmesine sebep olmaktadır. Bu nedenle Irak hükümeti, bir taraftan devlet çıkarlarını gözeterek ilgili te-

darikçi şirketlerle sözleşme yaparken, diğer taraftan siyasi partilerin siyasi ve maddi hedeflere ulaşmak maksadıyla sisteme nüfuz ederek siber güvenlik sistemini zayıflatmasına ve olumsuz yönde etkilemesine dur diyecek önemli kararlar çıkartmalıdır.

Zira geçmişte Irak'taki seçim sistemini kontrol eden Bağımsız Seçim Komisyonu tarafından oluşturulan verilerin ve seçim sonuçlarının, internet üzerinden gönderildiği elektronik oylama sisteminin güvenliğine yönelik ciddi tehditlerin oluştuğu açıklanmıştır.

Irak'ın eski Cumhurbaşkanı Yardımcısı ve Ulusal Koalisyon Başkanı, (Iyad Allawi) 25.04.2018 tarihli bir televizyon kanalındaki röportajında, Irak'taki seçim sürecinin yönetilmesinde uydu sistemi ve bilgi teknolojisine virüslerle müdahale edilip edilmediği ile ilgili şüphellerini dile getirerek, uyarılarda bulunmuştur. Allawi konuşmasında, bu tür bir müdahalenin Irak kaynaklı olmasından ziyade, dış servislerin olasılığına dikkat çekmiştir. Dış aktörlerin seçim sonuçlarını etkileme konusundaki manipülasyon olasılığı ile ilgili şüphelerini ise; " Irak siyasetini olumsuz yönde etkileyecek bu çaptaki bir siber müdahalenin olmadığının bir güvencesi var mıdır? Ayrıca "ihlal olmadığından emin olmak için uygulanan mekanizma nedir?" diye sormuştur(Saad, 2018: 402). Nitekim seçimlerden hemen sonra, Cambridge Grubu ile dirsek temasında bulunup oylarını ve elde ettikleri pozisyonlarını siparişle satın aldıklarına dair bazı Irak'lı milletvekillerinin ses kayıtları ortaya çıkmıştır. Söz konusu grup, Irak dışından veya içinden veri aktarmak üzere kullanılan bilgisayar programlarına girme kabiliyetine sahip olduğundan, siyasi süreçte yaptığı müdahalelerle, korkunç şekilde nüfuz etmiştir. Sonuçta ise malesef halkın sesini temsil etmeyen insanların yükselişine ve başta yasama ve yürütme olmak üzere ülkenin önemli mekanizmalarında, haksız yere liyakatsiz kişilerin görev almasına neden olmuştur.

2003'ten sonra yayınlanan birçok raporda, Irak'ın siber güvenliğini hedef alan ve hükümete ait bazı web sitelerini deşifre eden ve bu konuda zirveye ulaşan boyutta ölümcül tehditlerin varlığı ortaya konulmuştur.

Bütün bunlar Siber casusluk faaliyetiyle, Irak'ın zenginliklerini yağmalamak, siyasi ve ekonomik olarak yönetimini kontrol etmek, ülkenin özel yeteneklerini ve

geleceğini karartarak idari ve mali yolsuzluğu da fırsat bilip farklı bağlılıklara sahip siyasi parti ve gruplar aracılığıyla devlet kurumları üzerinde ülke çıkarlarına kastetmekte olduğunu göstermektedir.

Irak henüz e-bilişim sistemini en geniş anlamıyla benimsememiş olsa da, bu konudaki çalışmalarla belli bir mesafenin alınmış olması dahi ülke güvenliği açısından önem arz etmektedir. Ayrıca bu tedbirlerin acilen alınması konusunda atılacak adımlar hayati önem taşımaktadır. Aksi takdirde, banka hesaplarımız ve tüm askeri sitelerimiz tehlikeli istatistiklere, devletin istihbarat teşkilatı ve askeri mekanizması başta olmak üzere önemli iletişim hatlarının ve hatta en basit ifadeyle trafik işaretlerimizin dahi siber saldırılarına maruz kalması kaçınılmaz olacaktır.

Hacker ve siber programları ile yapılması muhtemel saldırılarda, trafik ışıklarının bile Irak siber güvenlik sisteminin zayıflığı nedeniyle en kötü durumda olduğu aşikârdır (Al-Kubaisi, 2019: 403).

4.2.2. İlk Olarak, Irak Ulusal Güvenliğinin Siber Alan İçerisinde Karşılaştığı Zorluklar

Bilindiği gibi bir toplumun değer yargıları ve altyapısına doğrudan tehdit oluşturan bir takım faktörler vardır. Bu faktörler, genel anlamda o ülkenin ulusal güveliğine kastederk adeta meydan okur. Her ülkenin doğal olarak bunları bertaraf etme ve başaçıkma yötem ve çalışmaları vardır.

Irak'ın ulusal güvenlik bağlamında stratejik güvenlik sistemine doğrudan tehdit oluşturan bir dizi zorluklarla karşı karşıya kaldığı bir gerçektir. Bu zorlukları iki kısma ayırmak mümkündür. **Birincisi;** Etki ve tepkileri bakımından doğrudan basit bir araştrmayla tespit edilebilir ve gözle görülebilir nitelikteki zorluklardır. **İkincisi ise;** Etki ve tepkileri doğrudan tespit edilemeyen ve Ulusal Güvenlik Stratejik Sistemine daha büyük çapta tehdit oluşturan zorluklardır. Irak ulusal güvenliğine yönelik tespiti zor olan bu görünmez zorluklar, etki ve tepkileriyle başta vatandaşların yaşamlarını tehdit etmekte ve devletin altyapı stratejisi ile önemli kamu sektörlerini de ilgilendiren bir dizi faktörle kendini göstermektedir. Nüfus artışı ve zayıf stratejik planlama-

nın zorluklarına ek olarak Irak'ta Siber Tehditlerle temsil edilen Dijital Sistemin karşılaştığı zorluklar ise bu faktörlerin önemli ayağını oluşturmaktadır.(Al-Yasiri, 2019: 397).

Siber Güvenlik, ciddi bir ulusal güvenlik ve ekonomik anlamda ortaya çıkan zorluklardan biridir. Çünkü Irak halkı'da küreselleşen dünyada yerini alırken ister istemez kitle iletişim araçlarının gelişimi ile başta internetin yaygın olarak vatandaşlarca kullanılması ve hatta hayatın İnternet tabanlı araçlara ve hizmetlere bağımlı hale gelmesi bu konuda alınacak tedbirleri kaçınılmaz hale getirmiştir. Bu çerçevede, Irak'ta ulusal güvenliğin sağlıklı ilerleyebilmesi adına siber alan için sağlıklı bir altyapı oluşturma ve güvenli hale getirme ihtiyacı ortaya çıkmaktadır. Siber saldırıların engellenebilmesi; başta terör tehditlerinin gözetim altına alınması ve dijital saldırıların önlenmesi gerekmektedir. Bu da bireylere ve kamu kurum ve kuruluşarına ait dijital veri ve bilgi sistemlerinin korunmasıyla mümkündür (Manickam, 2018: 396).

Irak, siber saldırılara en hazırlıklı ülkeler içinde dünyada 159. Sırada yer almaktadır. Bunun nedeni ise, hiç şüphesiz zayıf elektronik altyapısıdır. Bu sıralama aynı zamanda Irak'ta siber güvenliğin karşı karşıya olduğu riskin hangi boyutta olduğunu göstermektedir. Bu durum, Irak hükümetinin siber güvenlik konusunda kapsamlı bir çalışma ile atacak adımları tekrar gözden geçirmesini ve siber güvenlik tedbirleri alanında küresel gelişmelere ayak uydurma strateji oluşturmak zorunda olduğunu ortaya koymaktadır. Özellikle Irak'ta dijital teknolojinin gelişimi sürecinde internetin altyapısının savaşlar nedeniyle ciddi şekilde hasar gördüğü bir gerçektir. Bu da internet kullanımının özgür ve sınırsız erişim hakkı ile karakterize edilmesine neden olmuştur. Irak hükümeti ve idari mekanizmadaki karar vericilerin, ülkenin siber güvenliğini ilerletmek için elektronik mevzuat yoluyla altyapıyı ve İnternet sektörünü güçlendirmesi ve desteklemesi gerekmektedir.

2005 Irak Anayasası'nda "kişisel mahremiyet hakkı" tanımına vurgu yapılmasına rağmen, Irak İçişleri Bakanlığı'na bağlı siber suçlar konusunda faaliyet gösteren basit bir bölüm dışında, Irak'ta siber güvenlik konularında uzmanlaşmış merkezlerin bulunmadığı oldukça dikkat çekicidir. Bununla birlikte, bu hakkı destekleyen

başka özel yasalar da bulunmamakta ve hala belirsizliğini sürdürmektedir. Oysa siber güvenliğin günümüzdeki önemine rağmen veri koruma mevzuatı bir türlü geliştirilememiştir. Irak'ta siber alan kullanıcılarının çoğu teknolojik olarak hala eski ürünleri benimsemekte ve kullanmaktadır. Yeni versiyonlu Anti-virüs programları veya Güvenlik Duvarları uygulamayan eski sürümlerin vazgeçilmezliği ise yeni güncellemeleri takip etmekte yetersiz kalmaya neden olmaktadır. Bu durum ise, ülkenin resmi ve gayrı resmi kuruluşları başta olmak üzere, bütün vatandaşlara ait bilgileri de her türlü tehdide açık tutmaktadır.(Union, 2017: 398).

4.2.3. Irak Siber Güvenliğinin Karşılaştığı Tehlikelerin Özellikleri:

Siber güvenliğin risk ve tehditleri açısından Irak'ın karşı karşıya kaldığı sorunları ele aldığımızda öncelikle; "yasama alanındaki açıklık ve nitelik eksikliği" ile "uygun bir yürütme ortamının bulunmaması" başlıkları altında incelememiz doğru olacaktır.

Yasama Alanındaki Açıklık ve Nitelik Eksikliği:

Irak yasama ortamı, maalesef çok zayıf bir siber güvenlik ve yetersiz bir bilgi iletişim teknolojisiyle karakterizedir. Bu iki konu, şimdiye kadar Irak kanun ve mevzuatlarının hiçbirinde yeterince değinilmemiştir. Ancak Irak parlamentosu koridorlarında hala incelenmekte olan Irak Bilgi Suçu Yasası mevcuttur. Bu nedenle ivedi olarak alınacak kararlar önem arzetmektedir. Ekonomik, ticari, politik, sosyal ve diğer faaliyetlerle ilgili, görev ve hakların açık bir tanımı yapılmalıdır. Bu karışık durumdan kaynaklanan tüm anlaşmazlıkların, bilgi ve iletişim teknolojisinin yeteneklerine olan güveni artırmaya katkıda bulunacak şekilde ele alınmasını sağlayacak değişimlere ve çalışmalara hayati ihtiyaç vardır.

Bu teknolojinin kullanıcıları ile siber alan aracılığıyla mevcut fırsatlara bağlı olanlar, başta kullanım haklarının korunmasına, para ve verilerinin aktarıldığı bu alanın güvenliğinin temin edilmesine ve bu çerçevede varlıklarının güvence altına alınmasına ihtiyaç duyarlar. Bu açıdan bakıldığında Irak'ta siber alanındaki saldırı ve risklerin varlığı ve buna karşın yasal güvenlik tedbirlerinin zayıflığı, var olan bir takım yasaların ise yoruma açık ve birbiriyle çelişkili olduğu göze çarpmaktadır. Bu

durumun tespiti ise, siber suçu faillerinin sayısı ile direkt endeksli olduğu açıktır. Öte yandan bu risklerin seviyesi, farklı ülkeler arasındaki işbirliği eksikliği ile de alakalıdır. Hatta sadece belli bir coğrafi düzlemde yapılacak sınır ötesi ticaretin güvenliği ve siber saldırıların bertaraf edilmesiyle ilgili atılacak adımlar da, dünyanın herhangi bir yerinde yaşayan bir vatandaşın haklarını güvence altına alınmadığı müddetçe, yeterli sayılamayacaktır (Jabour, 2012: 406).

Siber Altyapı:

Siber altyapı ve güvenliğinin artırılması konusunda Irak'ta henüz yeterli bir ulusal siber altyapı güvenlik mekanizmasının oluşturulmadığı ve bununla ilgili gerekli desteğin sağlanamadığı görülmektedir. Ayrıca daha önce de değindiğimiz gibi mevcut altyapıyı korumaya yönelik yasal bir mevzuatın da bulunmadığını vurgulayabiliriz. Bu nedenle Irak'ta, Irak ulusal siber altyapının geliştirilmesi, bakımı, destek sağlanması ve korunmasına yönelik merkezlerinin oluşturulması gerekmektedir (Al-Ali, 2018: 404).

Hak ve özgürlükler:

Irak vatandaşlarının gelişmiş dünya ülkelerindeki insan hak ve hürriyet standartlarına uygun bir şekilde bilgi teknolijisinden yararlanma güvencesi ile ilgili, 2001 yılında "ulusal güvenlik ve egemenlik" argümanıyla hazırlanan, üstelik ülkenin çeşitli bölgesel ve uluslararası müdahale ve ihlallere maruz kaldığı bir zamanda yasa tasarısı olarak sunulan Bilgi Suçu Yasa Önerisi, bugüne kadar Irak parlamentosunda bekletilmiş ve hala onaydan geçmemiştir. Bu mezkur önerinin özellikle, yürürlükte olan Irak Anayasasının 38. Maddesinin ikinci bölümünde yer alan; "vatandaşların her türlü ifade özgürlüğü, basın, yayın, reklam, medya, toplanma özgürlüğü ve barışçıl gösteri" hak ve özgürlüklerle ilgili açık anayasal ihlallerden muzdarip oluşunu, onayı önündeki engellerden saymak mümkündür.

Aynı zamanda söz konusu öneri, Irak anayasasının posta, telgraf, telefon ve elektronik iletişim ve yazışma özgürlüğünü güvence altına alan 40. Maddesine aykırılık teşkil ettiği gerekçesiyle de destek bulamamıştır. Çünkü ilgili madde bunların

izlenmesini, gizlice dinlenmesini veya ifşa edilmesini engellemeyi içermektedir(Konseyi, 2018: 407).

Fikri mülkiyet hakkı:

Telif hakkı ve fikri mülkiyet hakları, günümüzde İnternet ve bilişim teknolojisi alanında ortaya çıkan yeni teknolojilerle meydana gelen, bilimsel ve teknolojik ilerlemeden büyük ölçüde etkilenen en önemli konulardan biridir. Öte yandan telif hakkı ve fikri mülkiyet hakları teknik ve teknolojik altyapılarını geliştiren çoğu ülkenin karşılaştığı en önemli sorunlardan biri haline gelmiştir. Bu nedenle, dijital devrimin yarattığı yasal boşlukların ele alınması, bu alanda meydana gelen gelişmelere ayak uydurulması, dijital ortamda fikri mülkiyet ve temel özgürlüklerin belki de en başında sayılan, vatandaş ve yazar haklarını garanti altına alacak yeni ve modern yasal sistemler inşa edilmesi gerektirmektedir.

Şu da bir gerçektir ki Irak, bu alandaki teknolojik gelişmelere uygun yeni yasalar çıkaran ve vatandaşlarının haklarını garanti edecek tüm yasal boşlukları gidermeye çalışan ülkelerden biridir. Mevduat ve telif hakkı hukukunda temsil edilen fikri mülkiyet ile ilgili Irak Anayasası, Irak mahkemelerinin yargı kararları ve güvenilir temellere dayalı bir takım kanun ve yönetmelikler vardır. Özellikle, 1971 tarih ve 3. Sayılı Irak Telif Hakkı Koruma Yasası'nın 1/ 1. ve 1/ 3. Maddeleri ile 1993 tarihli Irak telif hakkı koruması yasası, Telif Hakkı Kanununun 3. Maddesi, ayrıca Kuzey Irak Bölgesel yönetimi, 2012 tarih ve 17. Sayılı kanun maddesi de buna örnek olarak gösterilebilir (Mustafa, 2009: 408).

Buna rağmen şimdiye kadar Irak'ta, Irak vatandaşının dijital ortamda gizliliğini garanti eden ve dijital entelektüel çalışmaları korumayı kapsayan hiçbir yasa kabul edilmemiştir. Bu nedenle, Irak'ta geleneksel fikri hakların yanı sıra dijital fikri hakların da korunmasını ve düzenlenmesini dikkate alan birleştirici bir fikri mülkiyet yasası çıkartılmalıdır. Ayrıca düşünce özgürlüğünü ve çeşitli düzeylerdeki kültür mozayiğini göz önünde bulundurarak, özgürlüklerin yeniden yapılandırılmasına ihtiyaç duyulmaktadır (Kazanchi, 2005: 405).

Tüketici koruma hakkı:

Toplumun mihenk taşı olan her birey, devlet nezdinde vatandaş olarak adlandırılır ve en yüksek sosyal değer olarak kabul edilir. Bu nedenle devlet, vatandaşlarını her türlü riskten korumayı garanti eder. Bunların başında ise, ifade özgürlüğü, seçme ve seçilme hakkı ve temel tüketici haklarının garanti altına alınması gelir. Bu meyanda Irak'ta 2010 yılında yürürlüğe giren Tüketici Koruma Yasasının 2. Maddesi, bu konuda amaçlanan en önemli kanun maddelerinden biridir. İlgili madde şunları içermektedir:

a) Temel tüketici haklarının sağlanması ve bu haklara zarar veren yasa dışı uygulamalardan korunması.

b) Tüketici bilinç düzeyinin yükseltilmesi.

c) Malların ithalat, üretim veya pazarlama kurallarını ihlal eden veya üretici ve tüketici menfaatlerinden uzaklaşan ve yanıltmaya yol açan hertürlü eylemin önlenmesi.

Söz konusu 3. Madde ise, hizmet üreten, tedarik eden, satan, satın alan, pazarlayan, ithal eden veya tanıtan tüm gerçek ve tüzel kişilerin hak ve hukukunu içermektedir.

Görüldüğü gibi bu kanun maddesi de, bir tüketici olarak kişisel verilerin hukuka aykırı olarak işlenmemesini, profesyonellik içeren bir ilişkinin risklerinden daha fazla etkiye sahip istenmeyen reklamların önüne geçilmesini, ne çevrimiçi satıcıyı veya hizmet sağlayıcıyı ne de tüketicinin bizzat Irak vatandaşını riske atacak siber saldırılara karşı güvenliğini ele almamıştır. Bilindiği gibi dijital ortamda ürünlerin reklamı ve pazarlanması ile ilgili birtakım zor ve riskli unsurlar vardır. Örneğin, uygulamanın detayları, hizmet veya ürünün güvenirliği ve kalitesi, teslim tarihi, iade şartları, çevirim içi yapılan satışın teahhüdü ve yasallığı gibi, dijital ortamda yapılan ticaretin sağlıklı bir şekilde yapılması garanti altına alınmalıdır. Bunun için de diğer ülkelerdeki alınan tedbirlerden de yararlanarak, dijital ortamda tüketici haklarını ko-

ruyacak bir takım kanun maddelerinin çıkartılmasına ihtiyaç duyulmaktadır. (Hussein, 2015: 409).

Bilgi suçlarıyla mücadele:

Bugüne kadar birçok ülke bilgi ve siber suçlarla ilgili yasalar geliştirmekten kaçınmıştır. Siber alandaki zayıf altyapının güçlendirilip e-devlet sistemine geçilememesinin altında yatan sebeplere bakıldığında, "başta internet olmak üzere, bilgi teknolojisinin mevcut kanunların çıkartıldığı dönemlerde günümüzdeki gibi henüz etkin birşekilde hayatımıza girmemiş olması"nı iddia etmek, sadece bir bahaneden ibarettir. Bu nedenle "Iraklı yasa koyucunun, Anayasada öngörülen özgürlükleri göz önünde bulundurarak, bilgi akışındaki teknik gelişmelerle orantılı yeni yasaların düzenlenmesine büyük önem vermesi gerekmektedir."

Irak Yargı Kurumuna ait Medya Merkezi'nin bir raporunda şunlara yer verilmiştir: "İnternet gibi modern iletişim yöntemleri kullanılarak, elektronik suçun hâsıl olması; bireylere veya gruplara karşı doğrudan veya dolaylı olarak mağdurun itibarına, bedenine veya zihnine zarar verme kasdı ile işlenen her türlü hak ihlallerini kapsar." (admin, 2013: 411).

Irak'ta elektronik ve bilgi suçları iki surette ele alınmıştır: Birincisi, insanların sosyal medyada kasıtlı olarak gönderi ve paylaşımlarıyla ilgili suçlardır. Bunlar genelde ülkenin varlığına, birliğine halkın huzuruna kasteden ve ağır küfürlü hakaretler içeren paylaşımlardır. İkincisi ise, belirli bir yazılım aracılığıyla bilgisayarlar üzerinden şahıslara ait hesapların çalınması, önemli bilgi ve dökümanların başkaları tarafından izinsiz olarak gasp edilerek işlenen suçlardır.

Bu suçlar mahkemeye intikal ettiği takdirde, davacının iddasını ispat etmesi ve davalının iddialara cevap vermesi için savunma hakkı verilir. Söz konusu bilgi ve dökümanların kendisine ait olup olmadığını, suçu işleyip işlemediğini kanıtlayacak maddi materyaller istenir. Hâkimi ikna edecek, yeterli şahitlerin olmaması ve kanıt olarak bilgi ve materyallerin sunulma imkânının bulunamaması durumunda ise, tarafların yemin etmeleri istenir.

Bilgisayar ve elektronik bilgi korsanlığı suçları konusunda ise, "Irak yargısı henüz bu tür davalara, dijital suçlar ya da elektronik suçlar bağlamında bakmamaktadır. Ancak açılan davaya göre, saldırı veya güven ihlali gibi suç eylemlerini ele alırken, ceza kanununa atıfta bulunarak karara bağlama yoluna gitmektedir."

Irak'ta bilgi suçları, elektronik ve dijital araçların, özellikle internetin gelişmesi ve sosyal paylaşım sitelerinin (Facebook, Twitter, Instagram, WhatsApp gibi) yaygın olarak kullanılması sonucu, bir çok insanın, sanal âlemde dolaşırken bilerek ya da bilmeyerek bu alandaki özgürlüklerin sınırları ve yasaklarla ilgili bilgi yetersizliği nedeniyle çeşitli suçlara karışmışlardır. Gazete ve dergilerle ilgili yürürlükte olan Irak Anayasasının 1969 tarihli 111 sayılı Ceza Kanunu ile 1968 tarihli 206 sayılı Yayınlar Kanunu, günümüzde ortaya çıkan sosyal medya davaları için Irak mahkemeleri nezdinde yasal referans hükmündedir. Dijital suçlar ya beş yıldan az hapis cezası veya tazminat ile karara bağlanmaktadır.

"Ayrıca, Yayın ve Bilgi Mahkemesi dışındaki mahkemelerin, sınırlı yargı yetkisi nedeniyle siber suçlara bakması mümkün değildir."

Irak halkı, Irak Temsilciler Konseyi'nin bu konuda hazırladığı Irak Bilgi Suçu yasa taslağının onaydan geçirilip kanunlaşmasını beklmektedir. Ancak Irak'ta siyasi blokların derin görüş ayrılıkları içinde ve sürekli çekişmeli halde olmaları nedeniyle, henüz yakın gelecekte böyle önemli bir konuda bu yasaların çıkma ihtimali görülmemektedir.(Al-Zaidi, 2012: 410).

Medya Özgürlüğü ve Elektronik Denetleme:

Elektronik denetleme terimi, özellikle idari alan olmak üzere birçok alanda büyük etkisi olan teknolojik gelişmenin bir sonucu olarak ortaya çıkmış modern terimlerden biridir. Eskiden "elektronik kontrol" veya "bilgisayar kontrol sistemi" diye adlandırılan bu mekanizma, bilgisayarların kullanım güvencesinin temin edilmesi amacıyla belirli program ve uygulamalar sayesinde gerçekleştiriliyordu. Günümüzde bu denetimin gelişmiş elektronik cihazlar ve programlarla yapılması, mümkün olan en az riskle ve daha doğru bir şekilde gerekli sonuçlara ulaşmada çaba, zaman ve maliyet tasarrufu sağlayacaktır.

Hükümetler tarafından öngörülen siyasi nitelikteki web siteler ve bloglara dayatılan "elektronik sansür" kavramı ise, genellikle kurulduğu zamana, önceki ve sonraki kontrollere, adli ve yasal gözetimlere dayanarak, değişik formlarda, farklı takip, yöntem ve prosedürlerle biribirinden ayrılmaktadır. Irak'ta, bu kavramın 2003 Irak işgalinden sonra her ne kadar bir miktar gelişim süreci yaşamış olsa da, başta sistemin verimsizliği, tecrübe ve yetenek yoksunluğu, ayrıca düzenleyici sistemin tüm alanlarda zayıflamasına yol açan; mali ve idari yolsuzluğun yayılması ile siyasi sistemlerde meydana gelen gelişmeler, kontrol sistemindeki değişimi olumsuz yönde etkilemiştir. (Zidan, 2019: 412)."

2013 yılı sonlarında Irak nüfusunun ancak % 17,6'sı internete erişim imkânı bulabiliyordu. Bu gecikme, Ağustos 2009'da Irak, hükümetinin medya ve internet üzerinde ciddi bir baskı ve kontrolü sonucu baş göstermiştir ki, o dönemde terör faaliyetleri ve mezhepsel saldırıların önlenerek barış ve istikrarın sağlanması için alınan sıkı güvenlik tedbirleri ile muhalif rakipleri tasfiye etmek gibi tamamen politik hedefler arasında çakışan nedenlerden kaynaklanmıştır.

Irak anayasası, ifade hürriyeti ve basın özgürlüğü konusunda bir güvence sağlamaktadır. Hükümet uygulamada bu haklara elbette saygı göstermekle yükümlüdür. Ancak hükümetin interneti, sohbet odalarını, e-postaları ve diğer kişisel verileri gözetim ve denetimini engelleyen hiçbir kamu kısıtlaması bulunmamaktadır.

Bu özgürlüklerin şekli ve nevisi ne olursa olsun, hiçbir zaman kamu düzenini ihlal etmeye yeltenen terörist gruplarının ülke sınırlarını değiştirecek bölücü faaliyetlerine müsamahakâr olmamalıdır. Bu çeçevede Irak anayasasının (2005 yılı) bazı maddeleri bu konuya vurgu yapmaktadır (Wikipedia, 2019: 413).

Örneğin, Anayasanın 36. Maddesinin 2. Bölümü: Devlet, kamu düzeni ve kamu ahlakı ihlallerinin önlenmesini şu şekilde garanti eder:

1. Her türlü ifade özgürlüğünün sağlanması,

2. Basın, yayın ve dağıtım özgürlüğünün garanti altına alınması,

3. Yasalara uygun şekilde toplanma özgürlüğü ve barışçıl gösteri haklarının garanti altına alınması.

38. Maddenin 2. Bölümü ise; "telefon iletişimi, posta, telgraf, elektronik mail ve diğer yazışma özgürlükleri güvence altındadır. Bu haklar saklı olup güvenlik veya adli gerekçeler dışında izlenemez, gizlice dinlenemez veya ifşa edilemez." der. Ayrıca 40. Maddenin 2. Bölümünde ise, "herkesin düşünce, vicdan ve inanç özgürlüğü vardır."der. (Rashid, 2013: 414).

Elektronik işlemler:

Modern alışveriş yöntemlerinin vazgeçilmezi haline gelen Online alışverişin, küresel ticaret sektörü üzerindeki etkisi azımsanamaz seviyededir. Uluslararası anlaşmaların önemine rağmen, elektronik pazar ortamı veya sanal satış sitelerinin, ticari araçların gelişimine katkı sunduğu gerekçesiyle dünyadaki birçok kuruluştan sahte ürünler ithal edilerek dolandırıcılık ve sahtekârlık faaliyetlerinde bulunmaktadır. Bu dijital şebekelelere göz yumulması malesef Irak'ı büyük tehlikelerle karşı karşıya bırakmaktadır. Zira çoğu zaman teknolojik yöntemler kullanarak, özellikle hileli ve orijinal olmayan birçok ürün getiren bu sahte hesap sahipleri yasadışı girişimcilerin, pervasızca ülke ekonomisine kastetmelerinin altında, devlet sansürünün bulunmaması yatmaktadır. Bu sorumsuzluğun hala devam etmesini ise, sadece sahtekârların oyunun kurallarını iyi bildiklerine bağlamak yerine, yeterince bu konuda yeterli derecede önlem alınmadığına bağlamak doğru olacaktır.

Irak'ta yerel elektronik pazar ortamının, şimdilik normal pazarla rekabet edemediğine inanılmaktadır. Çünkü Irak halkı, genellikle bir ürünü satın almadan önce iyice inceledikten sonra fiyatı için pazarlık yapma eğilimi gösterip alışverişte titiz davranmayı ihmal etmemektedir. Irak'ta bu tür işlemlerin karşı karşıya kaldığı en büyük sıkıntı ve önemli zorlukların nedeni, yine yapım aşamasında olan ve bir türlü sonuç alınamayan Irak düzenleme ve yasama ortamındaki açıklıktan meydana gelmektedir. Bu nedenle elektronik Pazar ortamıyla ilgili yasa düzenlemeleri getirilirken, bu ortamın etkinliği, topluma olan uyumunun derecesi ve düzenlediği konu-

nun doğasını ne kadar içerdiğinin yanı sıra tepki verme kabiliyeti ve paydaşlar tarafından benimsenmesi ile ölçülmekte olduğu gözönünde bulundurulmalıdır.

Iraklı yasa koyucusunun içinde bulunduğu konum ise, elektronik işlemleri düzenleyen 2012 tarihli ve 78 sayılı yürürlükte olan elektronik imza ve elektronik işlemler yasası çerçevesinde kalmaktadır. Irak'ta özellikle elektronik ticaret alanında, yaygın olarak kullanılmaya başlayan medya ve elektronik işlemlerin gerçekleştirildiği elektronik imza sistemi gibi birtakım yeni programların uygulanmaya girmesi olumlu gelişmeler olarak değerlendirilebilir. Ancak küresel gelişime ayak uydurmada önemli ölçüde geç kalındığını vurgulamamız gerekmektedir. (Naglaa Abdel Hassan, 2013: 415).

4.2.4. Irak'ta Siber Güvenlik ve Üç Otorite Bünyesinde Bulunan Önemli Kurumları:

Yasama Otoritesi ve Siber Güvenlikle İlgili Önemli Kurumlar:

Irak'ta yasama yetkisi, Irak Parlamentosu ve görev tanımları çeşitli faaliyet alanlarına ve sektörlere dağılmış olan daimi komitelerden oluşmaktadır.

Bu parlamento komiteleri, kendilerine verilen görevleri yerine getirmekle mükelleftir. Bu görevler, genelde hükümet tarafından veya Irak parlamentosu tarafından önerilen yasa tasarılarını inceleyerek parlamentoya teklif ve tavsiyelerde bulunmayı kapsamaktadır. Dolayısıyla, bu komitelerin teklif ettiği veya tavsiyede bulunduğu yasa önerileri, kararların alınmasında önemli ve etkili bir rol oynamaktadır. Çünkü çoğunlukla bu komitelerde temsil edilen çeşitli siyasi blokların görüşleri de temsil edilerek halkın her kesiminin beklentilerini devlet otoritesine yansıtma imkânı sağlanmaktadır. (Harb, 2006, 421).

Parlamento komitelerinin kurulması fikri, temelde görev paylaşımı ve uzmanlık arayışı ilkesine dayanmaktadır. Her parlamenter bütün konularda ayrıntılı bir şekilde donanıma sahip olmayabilir. Bu nedenle hem görev yükünün paylaşımı hem de konunun uzmanları tarafından çok yönlü araştırma ve tecrübelere dayanan bilgilerden istifade edilmesi amaçlanmıştır. Zira bu konseyler, yasa önerilerini inceler, gö-

rüşlerini ifade eder ve gerekli tavsiyelerde bulunarak bir nevi parlamentonun doğru karar almada yardımcı olurlar. Parlamento ise bu öneri ve görüşlere güvenir ve çoğunlukla da aynı meyanda kararlar almaya çaba gösterir. Doğal olarak Meclisin, tüm üyeleriyle her konuda bir araya gelip işin içinden çıkılması zor ve karmaşık olan konular üzerinde inceleme yapması ve uzun uzadıya zaman harcaması da pek mantıklı görülmemektedir. İlgili konsey tarafından hazırlanan ve parlamentoya tavsiye niteliğinde sunulan öneriler, parlamento başkanı tarafından, sırayla tartışmaya ve daha sonra da oylamaya sunulur. Esasen dünya çağdaş siyasi sistemlerin de aynı şekilde hem parlamento çalışmalarını hızlandırmak, hem de görev paylaşımıyla konunun uzmanlarından öneriler almak maksadıyla bu tür komitelere başvurma gereği duyduklarını bilmekteyiz (Jassim, 2012: 416).

Siber güvenlikle ilgili sorunları izlemek ve güvenlik mevzuatları hazırlamakla Sorumlu önemli komiteler arasında şunları sayabiliriz:

1. Kültür, Sanat, Medya, Turizm ve Eski Eserler Komitesi:

Hükümetin telekomünikasyon sektöründeki çalışmaları ve bilgi teknolojisi üzerinde yasama ve gözetim rolü üstlenen önemli komitelerden biridir. Irak Temsilciler Konseyi iç sisteminin 100. Maddesinin 7. Fıkrasında; Kültür, Sanat, Enformasyon, Turizm ve Eski Eserler Komitesi, Medya ve İletişim Kurumunun çalışmalarını takip etmekle sorumlu olduğunu kapsamaktadır. Irakta faaliyet sürdüren söz konusu komisyon (komite), Ortadoğuda alanında bir ilktir. Medya ve iletişim sektörlerinin örgütler arası çalışmalarında refom ve standartlar oluşturulması ile ilgili olarak bu iki sektörün birbirinden ayrılması, bu kurumların gelişmesinin önünde bir engel oluşturmaktadır. Komite, Irak anayasası uyarınca herhangi bir devlet kurumuna bağlı olmayan bağımsız bir kurum olarak faaliyet sürdürmektedir. Medya ve İletişim Kurumu, yürürlükte olan 65 sayı ve 2004 tarihli yasa kapsamında Irak Cumhuriyeti'nde bilgi teknolojisi ve yazılım cihazlarının satışı, dolaşımı ve ithalatı ilgili konularda lisans vermekle münhasıran sorumludur (Al-Hiti, 2007: 418).

2. Ulusal Güvenlik ve Savunma Komitesi:

Irak Anayasasının 89. Maddesine göre kurulmuş olan Güvenlik ve Savunma Komitesi, şu alanları kapsam alanı içerisine alarak faaliyetlerini yürütmektedir:

- Devletin dış güvenlik işlerini takip etmek,
- Başta terör suçları olmak üzere iç güvenlik işlerini takip etmek,
- Silahlı Kuvvetleri ilgilendiren işlemlerin takibi,
- İstihbarat Teşkilatı kapsamına giren işlemlerin takibi,
- Silahlı Kuvvetler, Emniyet Teşkilatı ve İstihbarat Teşkilatına ait personel mevzuatı ile ilgili önerilerde bulunmak.

Komite, Irak Bilgi Suçu Kanunu taslağının hazırlanmasına da katılan önemli komiteler arasında yer aldığından, siber güvenlikle ilgili çalışmalarının merkezinde yer almaktadır. Halen Irak parlamentosunda bekletilen bu yasa tasarısının bir an evvel onaylanması için gerekli çalışmalar yürütmekte ve bu konuda, Yüksek Mahkeme Konseyi ile ortaklaşa birçok çalıştayda yer alarak bu yasanın uygulanmasındaki engellerin ve sorunların giderilmesine katkıda bulunmuştur (parliament 2019).

Yasama makamına sunulan "Irak Bilgi Suçu Yasası" teklifi, Güvenlik ve Savunma Komitesinin en önemli başarısı sayılmaktadır. Henüz Irak parlamentosunun koridorlarında görüşülmekte olan bu yasanın özeti aşağıdadır.

4.2.5. Irak Bilgi Suçu Yasa Önerisi:

İşbu 31 maddenin üzerinde olan yasa teklifi, elektronik bilgi teknolojisinin yaygın kullanımı konusunda güvenli bir zemine sahip olmayan Irak'ın, güvenlik standartları bakımından dünyanın gelişmekte olan ülkelerin seviyesine yükseltilmesi hedeflenmiştir. Irak'ta internetin hızlı bir şekilde yayılması, bu alanda çeşitli sorun ve çatışmaları beraberinde getirerek ülke güvenliğini sorgulanır hale gelmiştir. Bu nedenle Irak yasa koyucuları tarafından bu sorunların ele alınması ve suç unsurlarına karşı gerekli tedbirlerin alınması konusunda özel bir yasa düzenlemesini gerekli kılmıştır. Bu doğrultuda hem meydana gelen sorunların çözümü, hem de yasal sınırların

çerçevesini belirleyerek suça bulaşmayı önlemek amacıyla uygun yaptırımlar geliştirmek gerekmektedir. Bunları şu şekilde sıralayabiliriz:

1. Bilgi Suçu Yasasının Çıkarılmasına İlişkin Gerekçeler:

Bilgi teknolojisinin gelişmesiyle beraber siber alanda birçok suç faaliyetleri ortaya çıkmıştır. Bilgi teknolojisiyle ilk tanışmış olan ülkelerde olduğu gibi, kanun yapıcılarının caydırıcılık karinesiyle suçların önlenebilmesi amacıyla önce suçların cezayı müeyyidelerini ön plana çıkartarak ceza kanunları hükümlerinde değişiklik yapmış ve bir takım özel yasaları düzenleme yoluna gitmişlerdir.

Bu yasaları çıkartmanın gerekçelerini ortaya koyacak olursak; bilgi terörü ve casusluğu, resmi web sitelerinin hacklenmesi, özel bilgisayarların penetrasyonu ve bilgi iletişim sistemlerinin çökertilmesi başta olmak üzere daha birçok alanda devlete ve sisteme karşı potansiyel tehlike sayılacak suç unsurlarını saymamız mümkündür. Ayrıca hazır programların ve banka hesaplarının çalınması, kredi kartlarına ait kişisel bilgilerinin elde edilmesi, çocuklara yönelik cinsel suçlar, gizlilik haklarının ihlali gibi suçlar da bu kapsamda değerlendirilmektedir. Bunlara ek olarak, fikri mülkiyet haklarının kötüye kullanılması, fotoğraf ve mesajların izinsiz yayınlanması, telefon çağrılarının dinlenmesi, kamu kurum ve kuruluşlara ait gizli bilgilerin elde edilmesi, elektronik yollarla şantaj yapılması ve uyuşturucu maddelerinin reklamı ve pazalanması gibi suç alanlarını da sayabiliriz.

Bu suç faaliyetleri ön plana çıktığında, hâkimler bu tür davaları ele alırken ceza kanununa göre karara bağlamaktan başka çareleri kalmamaktaydı. Zira Bilgi Teknolojisinin gelişmesiyle ortaya çıkan bu yeni suçları özümsemek için, Anayasada bulunan ceza kanunu yeterli değildi. Dolayısıyla yargıçlar tamamen cezalandırıcı metne bağlı kalmak zorunda kalıyordu. Çünkü öngörülen kriminal çalışmalara göre ceza vermekten başka, özellikle de yazılı metin dışında herhangi bir suç çerçevesi ve ceza türü bulunmamaktaydı. Kamu ve özel kurumların çıkarlarıyla ilgili zararlı bir faaliyet suçu önlerine geldiğinde söz konusu eylemin hangi suçlara dâhil edileceği, hangi suçlarla kıyas edilebileceği karmaşası yaşanmıştır. Ayrıca bu suçların, özel suç kuralları gerektiren yeni suçlar olarak mı değerlendirilmesi gerektiği, yoksa önceden

sınırları belirlenen geleneksel suçlar dâhilinde kabul edilip, mevcut yasaların işletilmesini gerektiren suçlar olarak mı görmek gerektiği konusunda, üzerinde bir görüş-birliği sağlanamamıştır (Hâkim, 2019: 423).

Bilgi Teknolojisiyle günümüzde işlenen envai çeşit suçların nüksettiği ve geçtiğimiz bunca zaman diliminde meydana gelen karmaşa sonucunda, artık bu tür suçların, yeni bilgi teknolojisi suçları çerçevesinde değerlendirilmesi ve yeni yasal önlemlerle, niteliğinin hukuki seviyeye oturtulması zarureti ortaya çıkmıştır. Bilgi suçlarıyla mücadele için özel mevzuat çıkaran ilk ülkeler arasında İsveç, Kanada, ABD ve İngiltere'yi saymak mümkündür. Irak'ın bu ülkelere nazaran çok geç kaldığını söylememiz doğru olacaktır. Örneğin, İsveç Krallığı 1973 yılında Veri Yasasını yayınlamıştır. Amerika Birleşik Devletleri 1976 yılında bilgisayar sistemlerini korumak için özel bir yasa çıkarmıştır. Buna ek olarak, 1985- 1986 yıllarında ise bilgi suçu olarak addedilebilecek çeşitli fiil ve yelemlerin kapsamını belirlemiştir. Avrupa'da da, İngiltere 1981 yılında bilgisayar aracılığıyla gerçekleştirilen suçlara karşı, Korsan ve Sahtecilikle Mücadele Yasasını onaylamıştır. Kanada 1985 yılında Ceza Kanunu'nu bilgisayar ve internet suçlarına uyarlayarak değiştirmiş ve yeni yasalarla destekleyerek suç oluşumlarının önüne geçmeyi amaçlamıştır. Biz ise Irak'ta 2020 yılında, hala meclis envanterinde onay bekleyen Bilgi Suçlarıyla Mücadele Yasası gibi bir yasadan bahsedebiliyoruz. (Department, 2011: 424).

Geldiğimiz noktada, Irak hukuku hala bilgi teknolojisi ortamını düzenleyen mevzuattan yoksun durumdadır. Bilgi Suçu Yasası; Güvenlik ve Savunma Komitesi, Yükseköğretim Komisyonu, Hukuk Komitesi, Kültür Bilgi ve Turizm Komitesi, İnsan Hakları Komisyonu, Aile, Kadın ve Çocuk Hakları Komisyonu ve Hizmetler ve İmar Komitesi gibi, altı tane parlamento komitesinin ortak çabasının bir sonucu olarak Meclise sunulmuştur. Ancak, 2011 yılından bu yana ilk haliyle sunulan Bilgi Suçu Kanunu tasarısının Meclise sunulmasından sonra ilk olarak 2019 yılının başlarında dördüncü Meclis oturumunda iki defa ele alınabilmiş fakat mevzuatı, içeriği, paragrafları, sosyal yaşam, bireysel özgürlükler ve beklenen sonuçlar hakkında birçok karşıt görüşler nedeniyle ertelenmiş ve onaylanamamıştır. (Falahi, 2019: 425).

2. Önerilen Yasanın 2. Maddesi Şöyledir:

"Bu yasa, bilgisayar ve bilgi ağının yasal kullanımı için yasal koruma sağlamayı, kullanıcıların gerçek veya tüzel kişilerin haklarına saldırı teşkil eden eylemlerin faillerini cezalandırmayı ve bilgisayar suçlarının kötüye kullanılmasını önlemeyi amaçlamaktadır." Birçok kimse, dikkatli bir yasal mevzuat gerektiren basın, yayın, reklam, medya ve yayıncılık özgürlüğünü garanti altına alacak derin ulusal diyaloga tabi olması gerektiği düşüncesiyle bu yasanın, Irak anayasasının 38. maddesinin içeriğiyle çelişeceğinden endişe duymaktadır. Çünkü tüm Iraklıların hayatlarını etkileyecek olan bu yasanın uygulanması, bilgi teknolojilerini özümseme yetenekleri ve kamu yararı için nasıl kullanılacağı hususunda henüz fikirbirliğine ulaşılamamıştır.

Önerilen yaptırımların çoğunda açık bir zorlamaya mahal vereceği de bir gerçektir. Nitekim söz konusu yasa hükümlerini geniş elektronik bilgi ortamının kullanıcılarına uygularken, Irak halkının çoğunluğunu etkileyecek ve özellikle de iktidardaki siyasi sınıfların dâhil olacağı suç ithamlarıyla karşı karşıya kalınacaktır. Belki de hapishaneler, bu yasada ağır cezalara tabi olan herkesi ağırlamak için yeterli olamayacaktır (Article19, 2011: 426).

Yasa çerçevesinde cereyan eden dar bir görüş ise, elektronik bilgi ortamı suç kapsamının, internet ve dijital yollarla meydana gelmesinden dolayı çok geniş bir yer kaplayacağı düşüncesidir. Örnek olarak; 7. ve 8. Maddelerde; geçici hapis cezası süreleri belirtilmeden, mali para cezası ile geçici hapis cezası verilebileceği belirtilirken, 9. ila 23. Maddelerde ise, büyük mali para cezalarına ek olarak, bir yıldan on yıla kadar değişen hapis cezasına değinilmiştir. Bu cezaların işlendiği suçlara gelince, bunlar birden fazla ve çeşitlidir. Örneğin, 18. Maddenin ikinci fıkrası: "Bilgisayar ve internet bilgi ağını, ülkenin bağımsızlığı, birliği ve güvenliğini veya ekonomik, siyasi, askeri ya da üstün güvenlik çıkarlarını zedelemek amacıyla kullanan kişi; 3 yılı aşmayan bir hapis süresine ek olarak, asgari 2 milyon dinardan başlayıp 3 milyon dinarı aşmayacak bir para cezasıyla cezalandırılır." Şeklindedir. (Hamed, 2019: 427).

4.2.6. Bilgi Suçu Yasa Önerisi Etrafında Ortaya Çıkan Eleştiriler:

1. Bilgi Suçu Yasa Taslağı'nın, ugulamadaki Irak yasalarına birçok noktada aykırılık teşkil ettiği gerekçesiyle oylamaya sunulmaması gerektiği konusunda tereddütler oluşmuştur. Bunların başında, Uluslararası İnsan Hakları Örgütü tarafından hazırlanan ve 2012 yılında yayınlanan raporu gelmektedir. Raporda söz konusu yasa önerisinin ciddi cezalar verdiğine ve birçok yerde yoruma açık bırakılmış maddeler içerdiğine işaret edilmiş ve yeniden gözden geçirilmesi gerektiği konusunda tavsiyelerde bulunulmuştur.
2. Yasa önerisi, kaleme alındıktan sonraki dönemlerde gelişmiş olan bazı teknik ve teknolojik alanları kapsmaktan yoksun kalmıştır. Örneğin, İnternet ağları, mobil cihazlar, karasal ve uydu yayını yapan Radyo ve Tv kanallarını kapsamamaktadır. Zira metin, ses, resim veya video'lar aracılığıyla aktarılan bilgiler, akıllı cihazlar arasında kolayca bilgi paylaşımına imkan vermektedir.(Al-Musleh, 2019: 428).
3. Bu yasa önersi taslağının ikinci bölümünde diğer ülkelerin mevzuatlarıyla uyuşmayacak sert cezai hükümler içerdiği görülmektedir. 3, 4, 5 ve 6. maddelerde tekrarlanan ve çoğunlukla maksimum bir ceza gerektirmeyen türden çok sayıda suç içermekte, ancak bu suçlar için ömür boyu hapis cezası öngörülmektedir. Bunun bir örneği 6. Maddenin üçüncü paragrafında; "Elektronik finansal sisteme veya elektronik ticari ve finansal belgelere olan güveni zayıflatmak, ulusal ekonomiye ve devletin finansal güvenine zarar vermek amacıyla yanlış veya yanıltıcı bilgiler yayınlamak, ülke güvenliği, terörizm, insan ticareti, silahlı ayaklanma ve mezhepçilik çağrısı, ayaklanmaya kışkırtmak, vatandaşların mallarını manipüle etmek, sahtecilik, ticari manipülasyon, kara para aklama ve yanlış bilgi beyanıyla ulusal güvenliği tehtid etmek gibi konularda, tüm bu suçların dayandığı ortak kurala dikkat etmeksizin, mali yaptırımların yanı sıra geçici veya müebbet hapis cezasıyla tecziye edilir." denilmektedir. Ancak bu noktada eleştiride bulunanlara göre önerinin bu maddesi; bütün bu suçları da içine alan ve "Mali ve İdari yolsuzluk" adıyla geniş bir alanı kapsayan yürürlükteki Anayasa maddesiyle bütünleşmemiştir (Internatıonal, 2018: 430).

Ayrıca yasa, ülkenin güvenliğini tehdit eden veya terörle iltisaklı olan herkes için 25 ila 50 milyon Irak dinarı arasında para cezası ve hapis cezası öngörürken, web siteler ya da dijital suçlar kapsamında insan kaçakçılığı ve uyuşturucu madde kaçakçılığı amacıyla yayın yapan kişilere ömür boyu hapis cezası öngörmektedir. Ancak bu sefer de asgari cezayı 25 milyon Irak dinarından 30 milyon dinara yükseltmekte ve üst sınırını 50 milyondan 40 milyon Irak dinarına indirmektedir. Ayını şekilde sahtecilikle ilgili, hapis cezasına ek olarak mali cezayı 10 milyon dinardan daha az ve 15 milyondan daha fazla olmayacak şekilde bahsederken, failin devlet memur olması durumunda ise on yıl hapis cezasına ek olarak 20 ila 30 milyon Irak dinarı cezasını öngörülmiş ve mali cezası artırımını öngöermektedir. Öte yandan ticari manipülasyon, kara para aklama, yanlış bilgi beyanıyla sahtecilik, solandırıcılık, başkalarına ait bilimsel araştırmaları ele geçirme, şifre ve özel bilgilerin çalınması gibi suçlarda ise daha hafif cezaların öngörüldüğü tespit edilmiştir. (Stephen Rapp, 2012: 429).

4. Bu yasa tüm Iraklıları bilgi kaynaklarını ortaya çıkarmaya zorlamaktadır. Öncelikle 18. Maddede; yanlış beyanda bulunan ya da adli ve idari makamlara bilgi vermekten kaçınanlar için 5 ila 10 milyon Irak dinarı arasında para cezası öngördüğü için halkın tümünü yargı ve idare yetkisinin boyunduruğuna tabi tutmaktadır. Bu durum ise açıkça resmi ve gayri resmi kurumlarının şeffaflık ve netlik eksikliğinden muzdarip bir toplumda gerçeği bulma ve ona ışık tutma girişimlerine engel teşkil etmektedir. Ayrıca bu madde, medya ve araştırma kurumları da dâhil olmak üzere, devlet dairelerinde çalışan milyonlarca vatandaşı zor durumda bırakacak ve zarara sokacak ipuçları taşımaktadır. Çünkü suç unsuruyla ilgili kesin materyal kanıtların bulunması, her zaman mevcut olmayan delillerin belki de sorumsuzca kullanılmasına, öte yandan kamuoyu görüşlerinin tarafsızca yayınlanması, yazılması ve ekranlara getirilmesi gibi önemli özgürlükleri halka sunan medya çalışmalarına engel olacaktır. (Iraq, 2012: 431).

5. Bu yasa önerisi, Anayasanın 73. Maddesinde işaret edilen Cumhurbaşkanının Anayasada temel değişiklikler yapmasına adeta davet etmektedir. Çünkü bu öneri her yönüyle yeni bir mevzuata ihtiyaç duymaktadır. Örneğin, 6. Maddede; bilgi teknolojisi ve bilgi ağını ulusal güvenliğe tehdit olarak kullananlar için, ömür boyu hapis veya geçici hapis cezası ile asgari 25 milyon dinar (20.000 dolar) ve azami 50 milyon dinar para cezası öngörülmektedir. Ancak "din ve demokrasi" çağrışımlarıyla etnik ve mezhepsel ayrışma ve çatışmalara çanak tutacak bilgi suçlarına ise 50 milyon dinar para cezası öngörülmektedir. Bu nedenle Anayasanın 2. Maddesinde de değinildiği gibi, bu öneri endişe verici önyargılar içermektedir.
6. Bu eleştirilere baktığımızda, söz konusu yasa taslağının Irak vatandaşının doğrudan ya da dolaylı bir şekilde düşman haline getirildiği, özellikle yurttaşların özgürlük alanlarının güvence altına alınması noktasında tutarlı gerekçelere dayanmadığı ortaya çıkmaktadır. Bu eleştiri sahiplerinin çoğu, tasarının diğer ülkelerdeki uluslararası ve bilimsel deneyimler üzerine hazırlandığından bihaberdir. Ayırca yasama organının bu taslakta ele alınmış olan önemli konuların farkında olmayışından kaynaklandığı da bir gerçektir. Örneğin komşumuz Türkiye'de 23 Mayıs 2007 tarihinde yürürlüğe girmiş olan "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Yayınlar Yoluyla İşlenen Suçlarla Mücadele" yasası, bu bakımdan örnek alınması gereken bir uyglma örneği olarak ele alınmalı ve incelenmelidir. Yasa, tüm internet sunucu işletmelere kayıt tutma zorunluluğu getirmiştir. Ayrıca tüm yayınların kontrol ve denetime açık tutularak sistematik bir şekilde bu yollarla işlenen suçlarla mücadele etmeyi kolaylaştırmıştır. Şüphesiz birçok alanda yasadışı odaklara müdahale etme imkânı veren bu yasa ile ülke güvenliğini tehtid eden unsurların etkisiz hale getirilmesi amaçlanmış ve vatandaşların daha güvenli bir ortamda işlem yapmaları sağlanmıştır(Durnagöl, 2011: 432).
7. Yasa, dini sembol ve terimlerin kullanılarak kamu ahlakını ihlal etme ve ülkenin birliği, bütünlüğü ve bağımsızlığını ihlal etmeye yeltenme girişimlerinin engellenmesi konusunda yargı makamlarının tespit edemeyeceği pek çok değişken terim içermekte olduğu gerekçesiyle eleştirilmiştir. Oysa Türkiye gibi diğer ülkelerle karşılaştırıldığında özellikle internet ve dijital ortamda ulusal

güvenlik konusunda ne kadar hassas davrandıkları açıkça görülecektir. İçerik sağlayıcı, web sitelerin yayınları, kablolu internet ve kablosuz erişim kullanıcı ve sağlayıcıların kontrolü önem arz etmektedir. Türkiye'de hükümet, ayrıca bu yasada öngörülen bilgi teknolojisiyle işlenen suçları internet üzerinden şikayat edilmesine olanak veren https://www.ihbarweb.org.tr/ adında bir ihbar hattı açmıştır. Böyece türlü suç şebekelerinin deşifre edilmesi ve ulusal güvenliğini tehtid eden unsurlardan anında haberdar olunması amaçlanmıştır. Bir örnek olması açısından, Türkiye Cumhuriyeti Anayasasına 2007 tarihinde yürürlüğe girmiş olan 5651 sayılı kanunun 8. Maddesinde, ilgili suçlar listelenirken şunlara değinilmiş:

1. 84. Maddede geçen "İntihar Suçu"
2. 103. Maddenin 1. Fıkrasında yer alan "Çocukların Cinsel İstismarı Suçu"
3. 190. Maddede geçen "Uyuşturucu veya Uyarıcı Madde Kullanılmasını Kolaylaştırma Suçu"
4. 194. Maddede yer alan "Sağlık için Tehlikeli Madde Temini"
5. 226. Maddede geçen "Müstehcenlik"
6. 228. Madde geçen "Kumar Oynanması için Yer ve İmkân Sağlama"
7. 5816 sayılı Kanunu ihlal eden suçlar. (Gedik, 2008: 433).

Ürdün'e baktığımızda, Ürdün'ün vatandaşlarının elektronik pazar ortamındaki ticari güvenini artırmak için siber saldırılarla mücadele konusunda uluslararası yasalara uygun bazı önemli tedbirler aldığını görmekteyiz. Ancak vatandaşların mülkiyet hakkına tecavüzlerin önlenmesi, kamu kurum ve kuruluşlarına ait işletmeleri tehlikeye atan ve ulusal ağlara karşı suç işleyen istismarcıların cezalarını hafifletme yoluna gidildiği göze çarpmaktadır. Örneğin, bir kamu ya da bireysel hesaba ait bilgilerin yasadışı yollarla elde edilme suçunda, en az bir haftalık süreyle hapis ve 140.000 ila 300.000 Irak dinarına eşdeğer, 100 ila 200 arası Ürdün dinarı para cezası uygulanmasıyla yetinilmiştir.

Ürdün Anayasası, herhangi bir ağa giren ve işlemleri iptal eden, silen veya kesintiye uğratan kişi için; bir yıldan fazla olmamak üzere en az üç aya kadar hapis cezası, mali yaptırım olarak da, 100.000 dinarı aşmamak kaydıyla en az 200 Ürdün di-

narı para cezasıyla tecziye edilmesini karara bağlamıştır. Ürdün İnternet yasası hapis cezasını artırma yoluna gitmiş ve buna göre verilecek ceza; bir yıldan az ve üç yıldan fazla olmamak kaydıyla, mali yaptırımda ise 500 dinardan az ve 2000 dinardan fazla olmayan bir para cezası getirmiştir. İnsanların parasını manipüle eden ve hesaplarına girerek suç işleyen devlet memurları için de Ürdün Anayasasının ceza miktarlarını artırmış olduğunu görmekteyiz.

Her ne kadar Irak Bilgi Suçu Yasası, vatandaşın modern teknolojilere olan güvenini artırmayı amaçladığını iddia etse de, gerçekte bilgi teknoloji devriminin hızla büyüme ve yayılma gösterdiği bir dönemde, maalesef bu gelişmelerden duyduğu bir takım yersiz endişe ve tereddütlerin etkisinde kalarak eski yapısını savunmak adına itici tavırlar aldığını görmekteyiz. Bu tür bir politika, dünya ile daha fazla etkileşime hazır olan ülkeler arasında bulunan Irak'a, her şeyden önce vatandaşlarının çıkarlarını ve güvenliğini sağlam ilkelerle güvence altına almak yerine, sadece daha fazla tecrit, geri kalmışlık ve kendi kabuğuna çekilmeyi getirecektir (Al-Sharaan, 2018: 434).

1. Yürütme Otoritesi ve Siber Güvenlikle ilgili Önemli Kurumlar:

Günümüzde hızla gelişen dijital teknolojik cihazlarıyla gerçekleştirilen tehditler, hayati altyapının kötü niyetli saldırılara karşı savunmasız olabileceğine dair artan korkuların ana nedeni haline gelmiştir. Özellikle yeni riskler oluşturan karmaşık elektronik virüsleri ve korsan saldırıları, Bilgi Teknolojisi ve fiziksel altyapıyı giderek daha fazla tehlikelere maruz bırakmaktadır. Yaşadığımız çağdaş dünyada milyonlarca kişinin yararlandığı özel ve kurumsal internet hesapların, bir anda tahrip edecek türdeki tehlikelerle karşı karşıya kalması, elektronik olayların riskleri ve potansiyel sonuçları ışığında ekonominin ve günlük yaşamın ne kadar etkilenebileceği ve ne tür riskler getirebileceğini kestirebilmek kolay değildir. Bu nedenle tehlikenin farkında olan uluslararsı ülkler, tayakuza geçmiş durumdalar. İçişleri, Adalet, Savunma ve Ulusal Güvenlik Bakanlıkları bünyesinde çeşitli ulusal güvenlik kurumları oluşturmuş ve siber alan güvenliğinin artırılması için önemli tedbirler almıştır. Bu tedbirler arasında; siber suçluları önlemek, caydırmak, teknik uzmanların istihdamını ve eğitimini öncellemek ve bu noktada standart yöntemler geliştirerek, elektronik müdahale ile ilgili uygulama araçlarını büyük ölçüde paylaşmak, cezai soruşturmalar

ve etkili önlemler gibi çalışma alanları yer almaktadır. Kötü aktörler tarafından kullanılan teknikleri derinlemesine bilen adli tıp araştırmacıları ve ağ güvenlik uzmanları da zayıf noktaları tespit ederek, siber olaylarını etkili bir şekilde yanıtlamayı ve araştırmayı hedeflemekte ve bu meyanda önemli rol üstlenmektedir (Creasey, 2013: 435).

Bununla birlikte, başta dünyanın herhangi bir yerinden faaliyet gösterme kabiliyeti olan kötü aktörlerin siber saldırılarına engel olabilmenin, pek de kolay olmadığı bir gerçektir. Özellikle siber alan ile fiziksel sistemler arasındaki bağlantıların varlığı ve bilgi ağlarındaki karmaşık güvenlik açıkları gibi bir dizi faktör nedeniyle siber ortamın kolayca korunabilmesi zordur. Yürütme otoritesi, siber güvenlik işlerinde yetkili otorite olması nedeniyle çeşitli alanlarda siber güvenliği sağlama görevine sahiptir (Maria, 2016: 436).

a) Irak Ulusal Güvenlik Konseyi (Ulusal Güvenlik Danışmanlığı):

Başbakan başkanlığındaki ve Savunma, İçişleri, Dışişleri, Adalet, Finans ve Ulusal Güvenlik Danışmanlarının üyeliği bünyesinde faaliyetine devam eden Ulusal Güvenlik Konseyi, tüm sektörleri kapsayacak şekilde ulusal güvenlik politikalarını sürdürme kararlılığı ve azmi içerisinde olan ve bu çerçevede teknik çalışmalar belirleyen sivil bir kurumdur. Ulusal Güvenlik Konseyi olarak bilinen ve 2004 tarihli Anayasanın 68. Maddesine istinaden Ulusal Güvenlik Danışmanlığına dönüştürülen kurum, iç ve dış güvenlik, askeri, gıda, sağlık ve eğitim alanlarında meydana gelen sorunları ele alarak bunlarla nasıl yüzleşilmesi gerektiği konusunda somut kararlar almaktadır.

Ulusal Güvenlik Konseyi çatısı altında görev alan başbakanlık danışmanları ile ulusal güvenlik merkezlerinde çalışan özel uzman ekipler arasında önemli istişareler gerçekleştirilmektedir. Konsey, aynı zamanda ulusal güvenlik politikalarını koordine etmeyi amaçlayan bir kurum olduğundan, yüksek nitelikteki bu deneyimli uzmanlar ve tecrübeli danışmanlar aracılığıyla çok yönlü fizibilite çalışmaları yapılmaktadır. Hazırlanan çalışmalar, Milli Güvenlik Konseyin incelemesine sunulmaktadır.

Irak Ulusal Güvenlik Danışmanlığı, siber saldırılara karşı mücadele verme noktasında uzmanlaşmış, internet ve bilgi teknolojisi alanında ileri düzeyde eğitim almış bir ekipten oluşmaktadır. Bu ekip aynı zamanda NATO uzmanları tarafından eğitilmiştir. Kuruluşundan bu yana özellikle internet üzerinden Irak'ın ulusal güvenliğini hedef alan saldırıları önlemede büyük rol üstlenmiştir. (EC-Council, 2019: 437). Ekip, siber alanında faaliyet gösteren ulusal ağları, veri merkezlerini ve resmi siteleri koruma ve kollama sorumluluğunu taşımakta ve ulusal çabaları koordine etmektedir. Ayrıca kamu ve özel sektördeki kurumların siber alandaki hizmetlerine destek vermektedir. Ekip, elektronik hizmetlerin geliştirilmesini teşvik etmekte, e-devlet projelerinin otomasyonunu desteklemekte, siber güvenlik alanında Irak'ı uluslararası düzeye yükseltmek için bir dizi hedefe ulaşmayı amaçlamaktadır. Bu hedeflerin en önemlileri arasında şunları sayabiliriz: Ulusal güvenliğe yapılan saldırılara müdahale etmek, etkilerini sınırlamak ve bu sakındırmak için proaktif önlemler sağlamaktır. Başlıklar halinde sıralayacak olursak;

- Kamu ve özel sektör arasında bilgi alışverişinde bulunarak işbirliği yapmaya teşvik etmek ve siber güvenliğin ulusal çerçevesini oluşturmak,
- e- Devlet hizmetleri kullanımı açısından vatandaşın güveninin artırılması.
- Bilgi teknolojisi sistemleri ve İnternet kullanıcılarına yönelik güvenlik bilincinin artırılması,
- Güvenlik sistemleriyle yapılan saldırılarla mücadele için Bilgi Teknoloji sistemleri yöneticilerinin güvenlik yeteneklerini geliştirmek,
- Güvenlik tehditlerini ve etkilerini analiz ederek, mücadele yolları hakkında bilgi sağlamak,
- Siber olaylarının doğru raporlanması için akredite bir merkez inşa etmek,
- Siber güvenlik konusunda araştırma ve geliştirmeyi teşvik etmek (Alshaab, 2019: 438).

b) Irak İstihbarat Servisi:

Eski Irak Genel İstihbarat Servisi'nin yerine 2004 yılında kurulmuştur. Irak Devletinin dış saldırılara karşı güvenliğini sağlamak için faaliyet sürdüren bir ana

kurum olarak tesis edilmiştir. Anayasa'nın 40. Maddesinde belirtilen; "iletişim, posta, telgraf, telefon, elektronik ve diğer yazışma özgürlüğünün garanti edildiği; yasal ve güvenlik gerekçeleri veya yargı kararları dışında bunların izlenmesine, dinlenmesine veya ifşa edilmesine izin verilemez" hükmüne rağmen, İstihbarat Servisine özel yetkiler verilmiştir. Bu yetki çerçevesine, İstihbarat Yasası'nın yüksek güvenlik gerekçesiyle telefonların dinlenmesi yetkisi veren paragraflarda şart koşulan siber etki alanı da dâhil edilmiştir. 2003'ten önce kurulan en önemli kurumlardan biri olan Irak istihbarat servisinin, dijital teknolojiyle ilgili konuları takip etmek için özel birimler oluşturak teknolojik gelişmelere ayak uyduralacağı kararlılığı göstermesi, dikkat çekicidir. Bu özel birimlerin önemli olanları şunlardır:

1. **Elektronik İstihbarat Müdürlüğü:**

Eski Irak istihbarat Servisinin 2003 yılından önce bünyesinde kurmuş olduğu dijital teknoloji alanında uzmanlaşmış en önemli kurumlarından biri olan "Elektronik İzleme Müdürlüğü"nün varlığı kimseye bir sır değildir. Elektronik İstihbarat Müdürlüğü, dijital veri akışlarını izleme, video analizi, ses dinleme cihazları ve kısmen de olsa sahtecilikle mücadeleden sorumludur.

2. **Planlama Ofisi:**

Radyo, gazete ve uydu kanalları dâhil olmak üzere dünyanın dört bir yanından bilgi toplamak ve analiz etmekle sorumludur.

3. **Propaganda Ofisi:**

Yanlış bilgilerin yayınlanması dâhil, düşman devletlere karşı psikolojik savaş operasyonlarından sorumludur.

4. **Teknik İşler Müdürlüğü:**

Bilgi teknolojisi de dâhil olmak üzere iletişim donanımları ve güvenlik kameralarının geliştirilmesinden sorumlu olan müdürlük, ileri düzey akademisyen, mühendis ve bilim insanını bünyesinde çalıştırmaktadır (Mohammed, 2012: 439).

c) Bakanlıklara Bağlı Bilgi Teknolojisi Özel Birimleri:

Bu birimlerin başında e-Devlet Komitesi; Bakanlar Kurulu Genel Sekreterliğine bağlı olarak faaliyet yürütmektedir. Ulusal İdari Geliştirme ve Bilgi Teknolojileri Merkezi; Planlama Bakanlığına bağlıdır. Federal İstihbarat ve Soruşturma İşleri Ajansı; İşleri İçişleri Bakanlığı'na bağlıdır. Siber Güvenlik Teknoloji ve Elektronik Suçları Takip Birimi; İçişleri Bakanlığına bağlıdır. Ayrıca İçişleri Bakanlığı, çeşitli alanlarda elektronik suçları takip etme görevi olan bilgisayar alanındaki uzmanlardan oluşan Emniyet Müdürlüğüne bağlı "Elektronik Polis" adlı özel bir bölüm de oluşturmuştur (Al-Azzawi, 2019: 440).

1. Yargı Otoritesi ve Siber Güvenlikle İlgili En Önemli Kurumları:

Yargı, ister fiziksel ister siber alanda olsun, bir güvenlik kuruluşunun başarısında etkin rol üstlenen en önemli makamlardan biri olarak kabul edilmiştir. Çünkü yürürlükteki mevzuatı uygulayarak insanların güvenliğini ve sosyal haklarını garanti altına alan hükümler yayınlamaktan sorumlu bir otoritedir.

12 Temmuz 2010'da yayıncılık ve medya konularında uzmanlaşmış bir mahkemenin kurulmasına karar veren Irak Yüksek Yargı Konseyi'nin, en önemli mahkemelerinden biridir. Irak'taki yargı sisteminin web sitesinde yayınlanan karar metninin ön sözünde "basın, yayın ve gazetecilerin takdiriyle, bunların yargısal işlemlerine bakacaktır" şeklinde bahsedilen, El-Rusâfa İsti'naf Mahkemesinin kurulması, Dördüncü Yargı Otoritesi tarafından karara bağlanmıştır. Mahkemenin kuruluş tüzüğünde; "Medya ve yayıncılıkla ilgili şikâyet ve davaları hukuki ve cezai yönleriyle ele alır." denilmektedir. Bu mahkeme deneyimli bir hâkimin atanmasıyla faaliyetini yürütmektedir. Basın- Yayın ve Medya mensuplarının mesleki çerçevede yasal sosyal statülerinin farkında olmalarını, bu bağlamda lehte ve aleyhte meydana gelen şikâyetleri, kanuni haklar dâhilinde orantılı bir şekilde davalarının görülmesini icra etmektedir.

Irak'ta dijital alan ve siber güvenlikle ilgili konularda uzmanlaşmış en önemli yargı makamları arasında şunları sayabiliriz:

1. Basın- Yayın Mahkemesi: Irak'ta bir bölgeden diğerine farklılık gösteren çeşitli mahkemelerce verilen muhtelif içtihatlar yerine, yayıncılık ve medya davalarında verilen kararları birleştirecek tek elden karara bağlanması hedeflenmiştir. Ayrıca, görsel ve işitsel dijital medyayının yargı yetkisi, bu mahkemenin yetki alanı dâhilindedir. Şikâyet edilen fiil ile ilgili olarak; suçun tanımı, öngörülen ceza, cezalandırılabilir bir suç olup olmadığı ya da tazminat miktarının belirlenmesi gibi diğer mahkemeler arasında ihtilaf konusu olan davaların, alanında uzman hâkimler tarafından ele alınmasını gerekli kılmıştır (Muhammad, 2018: 441).
2. El- Rusafa Kabahatler ve Cinayet Mahkemesi: Bu Mahkeme, Irak'ta bilgi suçları konusunda uzmanlaşmış en önemli mahkemelerden biridir. Irak'ta Bilgi Suçları Kanunu, bu mahkemenin, yayın tarihinden itibaren üç yıl boyunca Bilgi Suçu Kanunu ile ilgili davaları inceleme yetkisine sahip mahkeme olmasını şart koşmuştur.

4.3. Irak Siber Güvenlik Stratejisi ve Irak Hükümetinin Uygulanmasındaki Rolü

4.3.1. Irak Ulusal Güvenliğinin Seyri:

21. yüzyılda birçok ülke, devletin herhangi bir kurumuna yapılacak bir saldırıyı öngörerek, elde edilen bilgi ve bulguları değerlendirip olası krizleri iyi yönetebilmek için izleme ve analiz sistemlerini devreye koymuştur. Böylece devletin geleceği öngörmesine ve gelecekte ne tür tehlikeler doğurabileceğine yönelik tahminlere dayanan, önleyici bir güvenlik sistemini benimsemesiyle karakterize edilmiştir Bu yüzyılda ise alanlarını açıkça geliştiren ve çeşitlendiren yeni bir teknoloji gelişmiştir. Teknolojik anlamda gelinen noktada artık bilgi; iç ve dış tehditlere ve ulusal güvenliğe yönelik stratejik mücadelenin mekanizmasını yönetmeye ilişkin, karar vericiye sağladığı kazançla, ulusal güvenlik işlerinin yönetiminde önemli bir rol üstlenmiştir. Artık tüm dünya ülkelerinin bu gelişim süreciyle ulaşabildiği bilgi, kendileri için tanımlayabilen, sınırlayabilen, analiz etmeye müsait ve bağlantılı altyapı çerçevesinde olmaya çalıştıkları geniş bir alan haline gelmiştir. Gelişen stratejik gelişmelerin ardından, ulaşılan teknik bilgi sayesinde, ortaya çıkan durumlara göre senaryolar oluş-

turulmasına ve uygun analitik bilgi modellerine göre güvenlik stratejileri ortaya koyma yeteneği kazanılmıştır (Khalifa, 2011: 442).

Her ülkenin, devlet sisteminin işleyişi, huzur ve güveni için amaçladığı hedefleri, başarıya ulaşmak için gerekli araçları, içinde bulunacağı zaman dilimini, içerdiği coğrafi alanı ve bu stratejinin yerel veya bölgesel olarak etkileyeceği alan ve zamanı tanımlayan kapsamlı bir stratejisi vardır. Bu nedenle, Irak'ın, çevresindeki ciddi değişiklikler ışığında, Irak ulusal güvenliğini sağlayan, ciddi ve kapsamlı bir ulusal stratejinin genel hatlarını çizmeye, diğer ülkelerden daha fazla ihtiyacı vardır (Muhammad, 1975: 443).

4.3.2. Ulusal Güvenlik Stratejisi Bağlamında Siber Güvenlik Stratejisi:

Ulusal güvenlik stratejisine, herhangi bir insanın ulusal güvenliğini belirli bir zamanda gerçekleştirme isteklerini yansıttığı pençeresinden kapsamlı bir bakış açısıyla bakacak olursak, mevcut durumda hayati bilginin altyapısı ve bilgi sisteminin diğer kritik unsurlarıyla güvenliğin sağlanmasının büyük bir ulusal sorun olduğunu görürüz.

Ulusal güvenliğin sağlanabilmesi için, Siber güvenliğin mevcut altyapısının genişletilmesi ve gelecekte daha da geliştirilmiş durumuyla güvenlik ortamına kapsamlı bir yaklaşım sağlaması doğrultusunda tutarlı bir çerçevenin çizilmesine ihtiyaç duymaktadır. Çünkü bir devletin ulusal güvenliği, bilişim teknolojisi ve dijital mobil uygulaması ile altyapının gelişmesi ve ekonominin büyümesi, aynı paralelde hızla ilerlemektedir. Zira siber suçlara karışan hükümet ve hükümet dışı aktörler, eşi görülmemiş bir boyutta hasara neden olan karmaşık elektronik araçlarla yeterince donatılmıştır.

Siber güvenlik alanına siber güvenliğin dâhil edilmesi, ülkenin her türlü güvenlik tehditlerine karşı hazırlıklı olmasına, bunlara yanıt vermesine ve ülkenin dijital alandaki güvenlik açığının giderilmesine, meşru ve hükümet dışı aktörlerle ortak önlemler alma yeteneğini artırmaya yardımcı olacaktır. Bu faaliyetler, ulusal siber güvenlik politikasının ve Irak siber güvenlik stratejisinin ulusal güvenliğe hazırlan-

ması için tanımlandığı, konum belirlenmesinin bir stratejik mantığıdır (Ibtisam Hatem Alwan, 2013: 444).

Ulusal Siber Güvenlik Stratejisi, Irak'ın siber alandaki güvenliğini sağlamak, bilgi teknolojisi ve altyapısını korumak, güvenilir bir İnternet topluluğu oluşturmak, tutarlı ve stratejik önlemler almak için ulusal bir hazırlık stratejisi uygulanması gerekmektedir. Bir ulusal siber güvenlik stratejisi, çoğunlukla tüm ulusal öncelikleri kapsayan ve siber risklere karşı ulusal maruziyeti ele alan birkaç kısa, orta ve uzun vadeli stratejiden oluşmaktadır.

Bu tehditler, ülkenin güvenliğine zarar verme, önemli bilgi altyapı operasyonlarını bozma yeteneğine, devlet operasyonlarını ve ulusal güvenliği zayıflatma potansiyeline sahip olduğundan, hafife alınacak türden tehditler değildir. Bu nedenle, Ulusal Siber Güvenlik Stratejisi, ülkeyi ulusal siber güvenlik politikasıyla tanımlar, koordine eder, yönlendirir ve siber tehditlere karşı tutarlı önlemler alır. Ulusal siber alanın korunması ve savunulması bu şekilde garanti altına alınmış olur (Adviser, 2018: 445).

4.3.3. Irak Ulusal Siber Güvenlik Stratejisinin Amaçları:

Irak hükümeti, çeşitli girişimler ve mekanizmalar sağlayarak, bir dizi önemli hedefler içeren bu stratejiyi uygulamak ve başarmak için tutarlı bir yol haritası takip ederek, bu stratejiyi formüle edip, siber alandaki ulusal çıkarları doğrultusunda yeni Irak siber güvenlik vizyonunu gerçekleştirmeyi amaçlamaktadır. Bu hedefleri şöyle sıralayabiliriz:

1. **Savunma Mekanizmalarındaki Açıklıkların Giderilmesi:**

Bilgi sistemlerindeki açıklıkların giderilmesi, devlet mekanizmasına ait veriler, web siteleri, ağlar ve veri işleme uygulamaları üzerinde ülke düzeyinde kapsamlı bir değerlendirme yapma ve ülkenin hayati bilgilerinin altyapısında var olan zayıflıkları ortaya çıkarma süreci, bilgi sistemlerinin yapısındaki bu boşlukları ve zayıflıkları gidermeye yardımcı olan önemli bir konudur. İnsan ihmalinden kaynaklanan hayati bilgi altyapısının güçlendirilmesiyle teknik kusurların giderilmesi için alınacak ön-

lemler, hayati öeneme haizdir. Dolayısıyla koruma mekanizmalarıyla siber ulusal savunmadaki zayıflıkların giderilmesi, kamusal ve toplumsal alanda meydana gelen aksaklıkların onarılmasına ve bilgi altyapısı ile iletişim altyapısını koruma ihtiyacının değerlendirilmesine yardımcı olacaktır. Ülkenin sağlam bilgi sistemi, bilişim teknolojisinin altyapısı arasındaki güvenlik açıklarındaki büyük boşlukları ele alma yeteneğini kolaylaştıracak ve siber alanda gelecekteki varlığımızı koruyacak önlemli mekanizmalar oluşturacaktır (Team, 2016: 449).

2. Ulusal Hedeflere Ulaşma Stratejisi:

Bu Strateji, Irak hükümetinin hazırladığı ve ülkenin ulusal çıkarları ile orantılı belirli planlara göre faaliyet gösteren bir dizi farklı mekanizma ile ulusal hedeflere ulaşmayı amaçlamaktadır. Ayrıca teknik bilgilerin geliştirilme stratejisi, ulusal altyapıyı siber tehditlerden korumak için küresel düzeyde tutarlı ve koordineli bir ulusal çerçevenin temellerini tanımlamaktadır.

3. Bölgesel ve Küresel Önlemlerin Alınması:

Siber suçla mücadele için kapsamlı mevzuatların oluşturulması ve siber tehdide karşı ulusal düzeyde ve ülkenin siber alanının güvence altına alınması bağlamında bölgesel ve küresel düzeyde çeşitli önlemlerin alınması amaçlanmaktadır.

4. Acil Müdahale Mekanizmalarının Oluşturulması:

Irak Bilgisayar Acil Durum e- Müdahale Ekibi'nin (CERT) kapasitesini artırma ve gelişimini sağlama hedeflenmektedir. Irak e- Müdahale Ekibi (CERT) siber güvenlik açığını kapatmak ve altta yatan zayıflıklarını gidermek için önlem alma çalışmalarına başlamasıyla beraber, içerden ve dışardan bir takım saldırılara hedef olmuştur. Bu nedenle siber saldırılara hızlı ve etkili bir şekilde yanıt verme yeteneğini güçlendirmek için kapasite geliştirme, kamu bilinci, etkinleştirme becerileri ve ulusal mekanizmaların geliştirilmesi gerekmektedir. Irak e- Müdahale Ekibi (CERT) ayrıca, Irak siber güvenlik stratejisinin belirli bir zaman diliminde geliştirilmesini ve Telekomünikasyon Birliği'nin uluslararası standartlara uygun çalışmalar yürütebilmesi için birkaç koordinasyon ekibi oluşturmuştur (NATO, 2016: 450).

5. Siber Saldırılarını Caydırmak:

Devletin ve tüm vatandaşların çıkarlarını, her türlü siber saldırılarından korumak ve her düzeyde siber güvenlik girişimini koordine etmek için, tüm olasılıkları hesap ederek güvenilir bir mekanizma oluşturulması hedeflenmektedir. Siber tehditlere karşı ulusal kapasitelerin geliştirilmesi, kamu ve özel sektörlerinde birlikte koordineli bir şekilde işbirliği yapılması, bölgesel ve küresel paydaşlar arasında siber güvenlik konusunda koordinasyon ve işbirliğinin güçlendirilmesi için, birden fazla paydaşla bağlantı kurmak gerekmektedir.

6. Ulusal Güvenlikle Kamu Çıkarlarının Gözetilmesi:

Irak Siber Güvenlik Stratejisi, ulusal güvenliğe yönelik siber tehditlere yönelik bir hamledir. Ulusal güvenlik tehditlerinin varlığı, siber alanın yeterince güvence altına alınamamasının bir neticesi olarak karşımıza çıkmaktadır. Siber alandaki koordinasyonsuzluk her türlü tehlikeye maruz kalınmasına neden olmaktadır. Hazır bulunan ve gelecekte meydana gelebilecek güvenlik sorunlarının acil olarak çözüme kavuşturulması bağlamında, Irak Ulusal Siber Güvenlik Stratejisi, siber alandaki güvenlik tehditlerini, kamu ulusal güvenliği ve kamu yararı hedefleri doğrultusunda yönetmeyi amaçlamaktadır (States, 2004: 451).

7. Yeni Bir Vizyonla Daha Güvenlikli Bir Yapı Oluşturmak:

Siber güvenlik vizyonu, vatandaşlarına fırsatlar sağlayan, ulusal çıkarları koruyan, barışçıl etkileşimleri kollayan ve ulusal refah için siber alana proaktif katılım destekleyen; güvenli, aktif, esnek ve güvenilir bir topluma yöneliktir. Vizyon ayrıca, siber alandaki siber risklerle yüzleşmek ve ciddiyetini azaltmak için, Irak'ta siber güvenlik alanındaki ulusal kapasitelerin koordineli, sürdürülebilir ve entegre bir şekilde geliştirilmesini hedeflemektedir.

Irak Siber Güvenlik Stratejisi, çeşitli alanlardaki bilgi altyapısını korumayı amaçlamaktadır. Bunun için siber alandaki durumunu güvenli bir siber ortama yükselterek üzerinde çalışılması gereken koordineli bir uygulama çerçevesine kavuşturmayı amaçlamaktadır. Ayrıca, Irak'ta kritik bilgilerin altyapısına yönelik tehditlere

karşı koyma aşamasında, proaktif hazırlık sağlamak amacıyla erken uyarı sistemlerini çalıştırarak kriz yönetiminin nasıl değerlendirileceğini, geliştirileceğini ve uygulanacağını da belirleyecek prensipler ortaya koymayı hedeflemektedir. (Comunities, 2006: 452)

4.3.4. Irak Ulusal Siber Güvenlik Stratejisinin Kapsamı:

Bu strateji, siber alandaki en önemli tüm işçi haklarını kapsayan çeşitli alanları kapsamaktadır. Bu strateji, siber ortamda güvenli çalışma haklarını kapsayan çeşitli alanları içermektedir. Bunlar:

1. **E-Devlet uygulamasının etkinleştirilmesi:** Vatandaşa en iyi hizmetlerin sunulmasına ve zamandan ve emekten tasarruf edilmesine yardımcı olacaktır. Bu nedenle, kamu sektörü ile özel sektör arasında etkili işbirliğinin artırılması, resmi ve gayrı resmi bilgi paylaşımının güvence altına alınarak teşvik edilmesi, Kamu kurumları, özel sektör ve vatandaşlar arasında bilgi aktarımının hızlandırılmasını sağlayacaktır.
2. Mevzuat ve örgütsel çerçevenin oluşturulması: mevcut Irak siber güvenliğinin gözden geçirilmesi, iyileştirilmesi, iletişim ve bilgi alanındaki teknolojik gelişmenin tanık olduğu aşama ile orantılı olarak Irak siber güvenliğinin karşı karşıya olduğu tehlikelerin önlenmesi gerekmektedir. İletişim ve bilgi güvenliği konusunda, hukuk yasası olarak Irak siber yasal statüsünün güçlendirilmesi ve yeni mevzuat hazırlanması gerekir. Ulusal yürütme ve yasal organların, aşamalı kapasite geliştirme programları oluşturmasıyla gizlilik hakları gibi hak ve özgürlüklerin teminat altına alınması, kapsamı alanındadır. Geçerli yerel mevzuatın tümüyle eksiksiz olması, uluslararası yasalarla, antlaşma ve sözleşmelerle tutarlı olması teyit edilmelidir. (Authority, 2018: 453).
3. Siber Güvenlik Teknolojisinin çerçevesini oluşturmak: Siber güvenlik emniyetinin sağlanabilmesi için, Irak siber güvenliğinin kontrolüne ilişkin gerekliliklerı tanımlayan ulusal bir teknolojik çerçeve oluşturmak ve geliştirmek gerekmektedir. Ayrıca siber güvenlik sistemleri ürünlerine sertifikalar verilerek

ulusal bir değerlendirme programı oluşturmak için çalışmalar ortaya koymak gerekmektedir.

4. Siber Güvenlikle ilgili kapasite geliştirme kültürü oluşturmak: Ulusal siber güvenlik kültürünü oluşturmak, geliştirmek ve güçlendirmek için çalışmalar ortaya konulmalıdır. Siber güvenlik alanında farklı eğitim programları oluşturmak, birleştirmek ve koordine etmek gerekmektedir. Siber güvenlik hakkında ulusal düzeyde bilgi yaymak, toplumsal bilinç ve etkili bir mekanizma oluşturmaya çalışmak önem arz etmektedir. Bunun için de Bilgi güvenliği personeli için minimum gereksinimleri ve nitelikleri belirlemek ve geliştirmek gerekmektedir.(Gary Stoneburner (NIST), 2002: 455).
5. Araştırma ve geliştirmede özgüvenin kazandırılması: Siber güvenlik alanda araştırma ve geliştirmeyi koordine etmek için özgüvene sahip olmak gerekmektedir. Bunun için alanında uzmanlaşmış personelin geliştirilmesi ve güçlendirilmesi elzemdir. Ayrıca araştırmalar sonucu elde edilmiş kazanımlar ile fikri ve teknolojik mülkiyet ve yenilikleri teşvik etmek, geliştirmek ve pazarlamak da önemlidir. Siber güvenlik alanında yerel pazarlar oluşturmak ve endüstriyel ürünleri beslemek ve desteklemek gerekir. Uluslararası standartlara uygun Siber Güvenlik konusunda uzmanlaşmış bir üniversitenin açılması da hayati önem taşımaktadır (Othman, 2006: 456).
6. Fiili uygulama ve yürütme: Siber güvenlik risklerini değerlendirmek için standart bir çerçeveye ihtiyaç vardır. Irak devletinin tüm organlarında faaliyet sürdüren siber güvenlik sistemlerini birleştirerek, koordineli bir şekilde standartların izlenmesini, uygulama, güçlendirme ve geliştirme adımlarını başarıyla sürdürecek profesyonel bir ekibin oluşturulması hedeflenmelidir. Bilgi Suçu durumlarında ise Adli Tıp Uzmanlığı, araştırma yöntemleri ve kanıt ekleme metodları işletilmelidir. Hukuk Fakülteleri ve hâkimler, öğrencilerini bilgi suçlarıyla ilgili müfredat okutmalı ve uzmanlıklarını geliştirici bilgilerle donatmalıdır.
7. Siber Güvenlik saldırılarına hazırlıklı olmak: Irak Siber Olaylarla Müdahale Ekibi (CERT)'ni geliştirmek ve güçlendirmek gerekmektedir. Bunun için Siber güvenlik alanındaki tüm kurum ve kuruluşların çalışanlarını siber güven-

likle ilgili faaliyetleri takip etmeye ve izlemeye teşvik etmek gerekir. İş sürekliliği yönetimi için birleşik bir çerçeve standardı oluşturularak çalışılmalı ve siber güvenlikle ilgili güvenlik açıkları ve uyarıları hakkında zamanında önlemler alınmalıdır. Bunun için de tüm kuruluşların, siber saldırılara maruz kalma potansiyellerini incelemek ve değerlendirmek için periyodik programlar uygulanması teşvik edilmelidir.

8. Uluslararası işbirliği oluşturmak: İlgili tüm uluslararası ve küresel siber güvenlik kurumlarına aktif katılımın teşvik edilmesi, Irak Siber Güvenlik Stratejisinin Kapsamı içinde değerlendirilmelidir. Siber güvenlik ile ilgili tüm uluslararası etkinliklere, konferanslara ve forumlara aktif katılımın sağlanması teşvik edilmelidir. Siber güvenlik alanında uluslararası periyodik konferanslar düzenleyerek Irak'ın siber güvenlik stratejisinin konumu güçlendirilmelidir. Uluslararası Telekomünikasyon Örgütü (ITU) ile iletişim kurarak, Irak siber güvenlik bilinci ile ilgili dosyayı güncellemek ve bu konuda yararlı adımlar atmak gerekmektedir. Irak Elektronik Suçlarla Müdahale Ekibi (CERT) ile diğer uluslararası elektronik müdahale ekipleri arasında ortaklık antlaşmaları yapmak üzere etkin işbirliği için Irak ekibini geliştirerek çalışma ufkunu genişletmek gerekmektedir. (Staff, 2018: 457).

4.3.5. Irak'ın Siber Tehditlerle Mücadele Çabaları:

Irak, ulusal güvenlik sistemini etkileyen görünmez zorluklarla, başka bir ifadeyle elektronik (siber) tehditlerle mücadele etmiştir. Irak'ın 2013'ten sonra bilgi ve iletişim alanında tanık olduğu ve ulusal altyapının güvenlik, bankacılık gibi alanlarda zayıf elektronik güvenliğine sahip olduğu sıkıntılı bir dönem geçirmiştir. Teknolojik gelişmelerin yükselme dönemine denk gelen bu dönemde Irak, güvenlik kurumlarının bilgilerine nüfuz edilerek, dünyanın birçok ülkesinin stratejik casus saldırılarına maruz kalmıştır. Irak'ı zor durumda bırakmak için herhangi bir bilgiyi alıp pazarlık amacıyla kullanmanın yanı sıra, Irak o dönemde kendisisne siber saldırıları yönelten devletlerin sızma faaliyetleri için adeta deneme platformu haline gelmiştir.

Irak hükümeti, bütünleşmiş bir bilgi güvenliği sistemi kurarak önleme ve savunma faaliyeti sürdürmeye çalışmıştır. Özel ve kamu sektörleri ile siber alanda gü-

venliğin sağlanması, yerel ve uluslararası kuruluşlar arasında ortak bir işbirliğine gidilmesi ve bu alanda somut ilerleme sağlanmasındaki çabalar günümüze kadar önemli bir ivme kazanmıştır (Al-Ali, 2018: 404).

Irak hükümeti, Irak'ta resmi kurumları ve iş sektörlerini hedef alan siber saldırılarından ülkeyi korumak için, Irak Ulusal Güvenlik Konseyi tarafından onaylanan "Dijital Irak Güvenlik Duvarı" projesi olarak adlandırılan ve bir dizi teknik önlemlerin alınmasını kapsayan bir uygulamayı hayata geçirmeye çalışmıştır. Elektronik operasyonların çeşitli alanlarda kullanım alanları ve bunun gibi ileri teknolojilerin inşa edildiği niteliksel bir değişim olan elektronik anti-virüs kalkanları ve dijital Irak güvenlik duvarı, Irak'ta siber terörizmle mücadelede büyük bir güvenlik projesi olarak hayata geçmiştir.

Asıl hedefi, terörist ağları etkisiz hale getirmek olan Proje, çok modern sayısal ve teknik avantajlara sahip olmasıyla, Irak'a önemli ölçüde saygınlık kazandırmıştır. Örneğin, Birleşmiş Milletler Uluslararası Telekomünikasyon Birliği tarafından yayınlanan Küresel Siber Güvenlik Endeksi'nin (GCI) siber güvenlik alanındaki devletlerin durum listesinde Irak'ın bu alanda önemli ilerleme kaydetmiş olduğu göze çarpmaktadır. Siber saldırıları karşısında en güvenlikli ülkeler listesinde Irak, 2017 yılında 158. (Khalil, 2018: 458) Sırada yer alırken, 2018 yılında uluslararası arenada 107. Sıraya, Arap coğrafyasında ise Irak, 2017 yılında 19. Sırada yer alırken, 2018 yılında 13. Sırada yer almış ve konumunu açık farkla yükseltmiştir.

Dünya çapında 175 ülkeyi kapsayan değerlendirme raporu, ülkelerin sistemlerini, internet ağlarını, güvenlik programları ile dijital saldırılara karşı korumak için kullandıkları uygulama ve araçları izlemektedir. Ayrıca bu raporun beş ana eksene dayandığı belirtilmektedir. Bunlar; yasalarla temsil edilen yasama ekseni, yönetişim ile temsil edilen organizasyon ekseni, teknik eksen, kapasite oluşturma ekseni ve uluslararası işbirliği ekseni gibi önemli bir rapor olduğu göze çarpmaktadır.

4.4. Irak Ulusal Güvenliğinin Bir Bileşeni Olarak Siber Güvenliğin Boyutları

Askeri boyut:

Irak'ın ABD işgalinden önce tarihten gelen ve devleti himaye eden sağlam bir askeri gücü vardı. Şüphesiz bu askeri güç, bölgedeki en eski ordulardan biri olarak kabul edilmekteydi. Ancak bu önemli kurum, işgalinden sonra atanmış olan sivil idareci Paul Bremer'in kararıyla feshedilerek donanımlı Irak ordusuna ait tüm silah ve teçhizat işgal güçleri tarafından imha edilmiştir. Nitekim 2003'ten sonra iktidara gelen Irak hükümetleri, ülkeyi işgal eden güçlerin varlığından kaynaklanan bağımsızlık sorunu ve sınırların teröristlere açılması nedeniyle Irak topraklarının her türlü terör eylemlerine açık hale gelmesi nedeniyle uzun süre istikrarsızlık ve güvensizlik ortamından çıkartmak için bir dizi atılımlar yapma girişiminde bulunmuştur. Bu nedenle Irak ulusal güvenliğinin sağlanabilmesi için farklı askeri doktrin ve farklı altyapılara sahip yeni bir askeri kurumun inşa edilmesi gerektiği üzerinde durulmuştur.

Amerikan güçlerinin Irak'a karşı siber savaş teknikleriyle her türlü müdahale operasyonları gerçekleştirirken, başta Irak hükümetlerinin siber uzay konusunda bihaber olması ve askeri kurumun bünyesinde henüz bu alanda bir yapılaşmanın olmaması nedeniyle Siber Güvenlik günümüze kadar ihmal edilmiş olmanın bedelini ödemektedir.

Irak'ın işgali sırasında, ABD Savunma Bakanlığı'nın Irak üzerinden yeni bir strateji geliştirerek elde ettikleri bilgi ve bulguları askeri planda kendi ülke çıkarları doğrultusunda kullanmıştır. Bunlar ilk bakışta yüzeysel gibi görünse de hedeflenen kitlenin duygularını, motivasyonlarını, nesnel muhakemesini ve nihayetinde yabancı hükümetlerin, kuruluşların, grupların ve bireylerin davranışlarının aktarıldığı sistemli bir savaş tekniği olduğu tespit edilmiştir. Planlı bir şekilde gerçekleştirdikleri bu faaliyetleri, Psikolojik Operasyonlar (PSYOP) olarak adlandırmıştır(Lamb 2005).

Irak savaşı sırasında, ABD Hava Kuvvetlerine ait EC-130E uçaklarından ve Basra Körfezi'nde faaliyet gösteren donanma gemilerinden telsiz mesajları, e-posta, faks ve telefon görüşmeleri gerçekleştirilerek dönemin Irak Cumhurbaşkanı Saddam

Hüseyin'e karşı harekete geçirebilecekleri birçok Iraklı komutanla iletişime geçilmiştir(Joiner 2020). O dönemde Irak ordusunun psikolojik, maddi ve manevi yönden yeteneklerinin yetersiz olması, henüz o yılarda Bilgi Teknolojisinin zayıflığı ve siber saldırıları konusunda gelişmiş caydırıcı bir mekanizmanın bulunmaması nedeniyle ne dış müdahalelere ne de işgale engel olunabilmiştir. Bu nedenle artık Irak hükümetleri önceki zaafların getirdiği tehlikelerden ders çıkarmalıdır. Irak ordusunun siber alandaki yeteneklerini ivedilikle geliştirmeli ve Irak ulusal güvenliğinin korunmasının önemini anlamalıdır.

1- Irak ulusal güvenliği bağlamında siber güvenliğin siyasi boyutu:

Irak'ta siber güvenliğin siyasi boyutu, ülkenin iç ve dış politikaları, siyasi otorite ile Irak halkı arasındaki ilişkinin türü, yasama ve yürütme otoritelerinin oluşumuna ilişkin seçimlerin yapılma şekli, dış politika vb. birçok alanda etkili bir rol oynadığı bilinmektedir. Siber güvenlik, değerler ve kültürler üzerindeki etkisiyle devletin dış ve iç politikasını etkilemede ve dolayısıyla ulusun çıkarını temsil eden siyasi partilerin eğilimlerini etkilemede önemli bir role sahiptir. Aynı şekilde, siyasi sistemin kitleleri etkileme, siyasi örgütleri inceleme ve kitleleri hareket ettirme yeteneklerini belirlemektedir. Kamuoyunun harekete geçirilmesi, hükümetin hedeflerini açıklamada medyanın rolü ve politikacıların ardından kitleleri sürükleme yeteneği üzerindeki etkisi de unutulmamalıdır.

Siber güvenliğin, Irak'ta yasama ve yürütme organlarının işletilmesiyle gerçekleştirilen demokratik seçimlerinin korunması konusunda büyük etkisi vardır. 2018'de Irak'ta yapılan seçimlerde sayım için kullanılan elektronik cihazlarda dolandırıcılık yapıldığına dair şaibeler çıkmıştır. Siyasi partilere bağlı bir dizi komisyon ve çalışma guruplarının dolandırıcılığa maruz kalındığı ileri sürülmüş ve şikâyetlerde bulunulmuştur. Bazı siyasi bloklarca, seçim komisyonu tarafından benimsenen elektronik sistemi sorgulanmış ve bu seçimlerde hile yapıldığına dair bazı teknik boşlukların bulunduğu iddiaları doğru çıkmıştır(Mansour and van den Toorn 2018). Siyasi partiler ve blokların seçim dolandırıcılığı korkusu, Bağımsız Yüksek Seçim Komisyonu'ndaki elektronik sayma ve sıralama cihazlarının merkezi sunucularındaki bir kusurun ve seçim günü elektronik oylama sistemindeki bir açığın buna neden ol-

duğu da bu iddialara kanıt olarak kullanılmıştır. Yine bu iddialarla yetinilmeyip Seçim Komisyonu'ndan Irak'ın tüm seçim bölgelerindeki istasyonlar için elektronik sayma ve sıralama cihazlarına testler yapılmasını talep edilmiştir.

Öte yandan bu karmaşık durumunu fırsat bilip uluslararası gözlemcilerin denetiminde manuel sayım yapılması talebinde bulunulmuştur. Ancak bu durumdan memnun olmayan Siyasi partiler de itirazda bulunmuştur. Bu da siyasi otoritede bir güvensizliğe neden olmuştur. Çünkü ayrı siyasi bloklar elektronik ve manuel sayma ve sıralama sistemi üzerinden birbirleriyle mücadele ederken bu sefer de manuel sayımda hileye yol açılmış olmaktadır. Nitekim buna yeltenmeye yeteri kadar zamana sahip olunmaktadır. Manuel hesaplamada seçim sonuçlarının açıklanması bazen bir ayı geçebilmekte ve bu süre zarfında listelere, sandıklara müdahale etme fırsatı verilmektedir.

Gelinen aşamada Irak'ta birtakım tedbirlerin alınması sonucu siyasi arenada yer alan partiler, elektronik oylamadaki boşlukların epeyce giderildiğine ve elektronik sayma ve sıralama sistemiyle sonuçların seçimlerden 24 saat sonra açıklanması nedeniyle oluşabilecek birçok müdahaleyi kısmen de olsa azaltabileceğine inanmaktadır (Dodge 2018). Buna rağmen Siyasi partilerin ve seçmenlerin elektronik seçim sistemindeki korkuları varlığını sürdürmektedir. Bu tür endişeler Irak kamuoyu nezdinde birkaç soruda somutlaşmaktadır. Bunlar:

a) Uyduların yabancı ülkeler tarafından yönetildiği ve kesinlikle kontrol edilemediğine göre, seçimlerde elektronik sayım sisteminin kullanılması vatandaşların hür iradesinin doğru olarak seçimlere yansıması güvence altına alına bilir mi?

b) Irak'ta yapılan demokratik seçimlere dış mihraklarca nüfuz edilerek manipüle edilmesi gerçekten bir olasılık ise o halde seçimlerde kazanan parti ya da partilerin, ülke yönetimini devralacak organları bu dış mihrakların çıkarları doğrultusunda hareket etmeyeceğinin garantisi var mıdır?

3. Irak siber güvenliğinin sosyal boyutu:

2003 yılında Amerika'nın Irak'ı işgalinden bu yana, siber suç olgusu ülkede yaygınlaşmıştır. Bunun en önemli nedenlerinden biri, Irak toplumunda sosyal ve kültürel değer sisteminin etkisinin yanı sıra teknolojik gelişmeler ve modern iletişim araçlarıyla suçları teşvik eden programların Irak toplumu üzerinde menfi yöndeki etkisi olmuştur. Irak, uzun yıllardır bir arada yaşayan farklı etnik ve sosyal yapıya sahip bir ülkedir. Ancak dış müdahalelerin iç dengeleri sarsma faaliyetleri sonucu büyük bir kargaşa ve güvenlik kaybı yaşanmış ve sonucunda Irak toplumunu parçalayan bir iç savaşın yaşanmasına yol açmıştır. Bu durum iç dengelerde etnik unsurlar sorunu ve farklı din ve mezheplerin ayrışmalarına neden olmuştur.

Bu kutuplaşma fitilinin ateşlenmesinde sosyal medyanın büyük rolü olmuştur. Irak'ın ulusal güvenliğini tehdit eden yeni sorunlardan biri sayılan medya sorunu Irak'ın stratejik güvenlik sistemine yönelik en önemli görünmez tehditlerden biri olmuştur. Irak halkına yönelik algı faaliyetinde bulunan Arap ve bölgesel uydu kanalları ile Facebook ve Twitter gibi sosyal medyanın kötüye kullanımı bu sorunlara ivme kazandırmıştır(Aboud 2012). Bu nedenle, Irak toplumunun değer yargılarıyla çelişen elektronik medya ve dijital ortamın daha güvenilir bir ortama taşınması gerekmektedir. Bu nedenle Irak siber güvenlik sistemi gözden geçirilerek Irak toplumunun menfaati doğrultusunda uygun bir yasal mevzuatı yürürlüğe koymak gerekmektedir.

Irak Temsilciler Konseyi 2019'da PUBG ve Fortnite gibi popüler web oyunlarını yasaklayan ve özellikle gençler üzerindeki "olumsuz" etkilerini gündeme getiren bir yasayı onaylamıştır. Yasanın karar metninde yasağın "bazı elektronik oyunların toplum üzerindeki olumsuz etkileri" nedeniyle konulduğu belirtilmiştir. Irak toplumunun sağlığı, kültürü ve güvenliği açısından çocuklara ve genç nesillere yönelik sosyal ve ahlaki tehditlerin bu şekilde önlenmesi desteklenmelidir(staff 2019).

4. Ekonomik boyut:

Irak'ta siber güvenliğin ekonomik boyutunun açıklığa kavuşturulması, dijital ekonominin boyutunu ve uygulamalarını, ekonomik sektörün siber uzay kullanımının kapsamını ve bu uygulamaların korunmasındaki siber güvenliğin rolünü bilmemizi

gerektirmektedir. Dijital ekonomi alanında önemli bir takım teknik uygulama vardır. Bunlara kısaca değinecek olursak:

a) Elektronik Pazarlama: Bir araştırmada bilgi ve iletişim teknolojisi kullanılarak yapılır. Doğrudan iletişim ağları ve elektronik iletişim yoluyla pazarlama hedefleri buna örnektir.

b) Elektronik yatırım: Ağın yeteneklerinden ve sağladığı avantajlardan yararlanmaya çalışarak yatırım yapılır. Özellikle finansal piyasalar alanında yatırım kararları almaya yönelik bilgiler ve mekanizmalar buna örnektir.

c) Elektronik Ticaret: Mal değişimi yapmak için bilgi ve iletişim teknolojisinden yararlanılır. Bireyler arasındaki hizmetler ve bilgilerin akışı buna örnektir.

Bilişim teknolojisi gelirleri Irak ekonomisine gayri safi yurtiçi hasılanın % 1,8'i oranında katkı sağlamaktadır ki, bu da işgal altındaki Filistin'deki yüzdeye çok yakın bir oran olarak karşımıza çıkmaktadır. Irak ayrıca e-devlet hizmetlerinde 190'dan 172.inci sırada, iş amaçlı e-hizmetlerde ise 154. sırada yer almaktadır. Şu anda Irak, endüstri için gerekli eğitimsel ve dijital becerilerle ilgilenen Küresel Rekabet Forumunun öngördüğü 4.sıralamanın dışında yer almaktadır(Bahaa Abdul-Hadi 2020).

Irak devleti dijital ekonomi alanında gösterdiği çabalara rağmen, büyük gecikmeler yaşamakta ve küresel, bölgesel ve hatta Arap ülkelerine ayak uydurmada zorluk çekmektedir. Bunun nedenlerini şöyle açıklamak mümkündür:

1- Bilgi ve iletişim teknolojileri altyapısında var olan büyük eksiklikler.

2- Irak'ın bilişim kaynaklarını üretememesi.

3- Irak dijital ekonomisine yapılan yatırımın çok düşük seviyede olması.

4- Güvenlik ve hukuktaki istikrarsızlığın dijital ekonomiye yansımış durumda olması.

5- Dijital ekonomi için teknik ve bilgi sektörüne yönelik zayıf finansman ayrılması.

6- Irak ile gelişmiş ülkeler arasındaki teknik ve teknolojik gelişim farkı.

7- Irak'ın edindiği teknoloji, çoğunlukla gelişmiş ülkelerin stratejilerine tabi türden olduğu ve bu nedenle Irak devletinde gerçek kalkınmaya ve yerel uzmanlığın oluşturulmasına yardımcı olamayışı.

8- Irak'ta elektronik ödeme yöntemlerinin bulunmaması ve mevcut olanların da Irak vatandaşının güvenini kazanamayan özel bankalardan oluşması.

Yukarıda değindiğimiz hususlar ışığında Irak'ın dijital ekonomik sistemini korumada siber güvenliğin rolünün çok zayıf bir durumda olduğunu söyleyebiliriz. Bu zayıf rol elektronik ticaret konusunda da kendini belirgin bir şekilde ortaya koymaktadır. Irak hukukunda bu sektörde yer alan tüm alanları kapsamayan 2012 tarihli 78 sayılı Elektronik İşlemler ve Elektronik İmza Kanunu dışında bir elektronik ticaret düzenlemesi bulunmamaktadır. Ayrıca, ürünlerini internet üzerinden pazarlamaya çalışan Iraklı şirketler ile muhatap kitle olan toplumun kredi kartı kullanma oranının çok düşük seviyelerde olması da birçok zorluklarla karşı karşıya bırakmaktadır. Bankacılık sektörünün güvensizliği ya da ticaretin her alanında vatandaşların yararlanamaması nedeniyle kimi zaman vatandaşların "sahte şirketler" aracılığıyla dolandırıcıların tuzağına düştükleri görülmektedir.

Resmi daireler başta olmak üzere diğer kurum ve kuruluşların bilgi gizliliğinin korunması ve internet kullanıcılarının yasal güvenliğinin sağlanamaması gerekmektedir. Nitekim bilgisayarların korumasız olmasıyla virüs saldırılarına maruz kalınması ya da modern teknik araçları kullanımı konusunda deneyimsiz olunması birçok önemli tehditleri de beraberinde getirmektedir. Örneğin, donanım ve yazılımı çökerten teknik arızalar, bilgi hırsızlığı, veri hatlarının kesilmesi, elektronik imha, elektronik dolandırıcılık, elektronik ödeme araçlarının yasadışı kullanımı, tüketici kartı numaralarının çalınmasına maruz kalma gibi modern iletişim araçlarının gelişmesiyle doğru orantılı olarak ortaya çıkan teknik suç risklerini bu tehditlerden sadece bazı ana başlıklar olarak sayabiliriz(Hanan Muhammad Al-Qaisi 2017).

5. Kültürel boyut:

İnternet, farklı kültürler arasında bir rekabet alanı haline gelmiş ve sağladığı çok sayıdaki haber ve bilgi sayesinde, toplumdaki bireylerin ve grupların davranışlarını farklı şekillerde ve derecelerde etkileyen en önemli modern medya araçlarından biri olarak kabul edilmiştir. Bunun da ister istemez insanların gelenek, göreneklerine ve kültürlerine farklı yansımaları olmuştur. Bu durum ayrıca önemli bir yeni "kültürel karışım" sürecini beraberinde getirmiştir.

İnternetin ve sosyal medya sitelerinin bireyler ve gruplar tarafından yaygın olarak kullanılması sayesinde internetin yapısı, toplumsal düşünce üzerinde köklü değişiklikler yaratılabilmiştir. Bir topluluktan diğer bir topluma aktarılan gelenekler ve kültürel bağ, "küresel köy" teriminin somutlaşmış halini yansıtmaktadır. İnternet aracılığıyla yayılan kültürel semboller medya içerikleri, ulusal kültürleri ve kullanıcıların davranışlarını olumlu veya olumsuz etkileyeceğinde şüphe yoktur(Mackay 2004).

Irak da dâhil olmak üzere kimi ülkeler, internetin neden olduğu kültür yozlaşmasının önüne geçme çabaları ve buna yönelik çözüm arayışlarına girmeleri, bu meyanda siber uzayda özgürlükleri kısıtlayan yasalar koyarak kültürlerini korumaya çalışmaları çok işe yarayacak gibi görünmemektedir. Çünkü bu olgular statik bir varlık değil, sürekli etkileşim içinde olan bir canlı gibidir. Bu nedenle elbette ki hükümet internetin gücünü kullanmalı ancak kullanıcıların bilgi gizliliği ve güvenliğini de sağlamalıdır.

Irak'ta etnik farklılıkların aşılmasına katkıda bulunabilecek çeşitli etnik kültürler arasında hoşgörü ve kültür birliğini koruması için, elektronik kütüphaneler, arşivler ve kültür dünyasını desteklemesi de gerekmektedir. Bu noktadan hareketle hükümetinin sosyal medya sitelerini, kültürel ve akademik platformları dini ve siyasi hassasiyetlerden uzak tutacak bir politika izlemesi gerekmektedir. Ayrıca bu kültürel birikimi daha üst seviyelere taşımak için düşünce özgürlüğünü insan hak ve hürriyetlerine uygun olarak, elektronik fikri mülkiyeti koruma, siber alandaki bası ve yayın süreci ve telif hakkı konularında yeni yasal düzenlemeler çıkartılmalıdır.

Bölümün Özeti:

Bu bölümde Irak'ın hassas altyapısı, ekonomik durumu ve hatta vatandaşlarının çoğunun gelişmiş dijital teknolojiyi kullanma konusunda henüz yeni tanışmış olması ve Iraklı karar vericilerinin siber güvenliğe çok az ilgi duyması gibi nedenlerle siber uzaya girmekte yeni bir ülke olduğu sonucuna varıyoruz.

Irak hükümetinin eski kâğıt tabanlı sisteme bağlı kalmasında adeta ısrar etmesi, siber güvenlikten sorumlu özel organların henüz yeterince oluşturulamaması, Irak'ın dünya ile etkileşimi açısından, güvenlik sonuçlarını anlama ve potansiyel riskleri azaltma yeteneği bakımından önemli ölçüde zayıf kalmasına neden olmuştur.

Çalışma ayrıca Irak'ın maruz kaldığı güvensizlik ve istikrarsızlık nedeniyle, Irak yönetiminin, altyapıyı güçlendirme faaliyetlerini ivedilikle yapamamasına ve halka ait değerlerin korunmasını güvence altına alacak stratejik bir gösterim formüle edememesine neden olduğunu ortaya çıkarmıştır. Irak'ta güvenlik alanıyla ilgili, elektronik tehditler ve yeni ortaya çıkan siber suçlarla mücadele konusunda Irak mevzuatının zayıflığından da açıkça anlaşılmaktadır.

Ayrıca Irak'ın siber uzayda ülkenin güvenliğini koruma ve kollama konusunda yüksek tecrübe ve yetkinliğe sahip eğitimli ulusal kadrolarının bulunmaması ve soruşturma süreciyle ilgili siber saldırıları takip eden herhangi bir kurumun olmaması, siber uzayda suçlulara ve dolandırıcılara daha çok maruz kalmasına neden olmaktadır. Bu nedenle Irak'ın, başta siber güvenlik alanı olmak üzere, çeşitli alanlarda ulusal güvenliğini sağlayacak çalışmalar yapması gerekmektedir. Bu amaçla gelişmiş ülkelerin deneyimlerinden yararlanması ulusal yeterliliklere dayanan ve alanında daha tecrübeli personel barındıran kurumlar oluşturarak dijital altyapıyı yeniden inşa etmesi gerekmektedir.

Irak'ın ayrıca, siber saldırı ve suçlarla etkili bir mücadele mekanizması oluşturması gerekmektedir. Bunun için de öncelikle vatandaşların İnternet'e güvenli bir şekilde erişim özgürlüğünün sağlanması, düşünce ve ifade hürriyetinin güvence altına alınması ve bunlarla yüksek düzeyde ulusal güvenliğin sağlanması arasında denge sağlayan bir siber güvenlik mevzuatı hazırlanması gerekmektedir.

SONUÇ

Siber güvenlik, farklı sektörlerde kamusal yaşamın çeşitli alanlarını kapsayan siber alanın insan kullanımıyla süratle yaygınlaşan, gelişme ve genişleme yeteneğine sahip bir kavramdır. Kuşkusuz bilgi, gücü elinde bulundurma ve yükselme açısından, sahibinin en değerli metasıdır.

Bilgi güvenliği, yaşadığımız çağda özellikle elektronik suçların ulusal güvenliği tehdit etmesi, özel hayatın güvenliğinin ihlaline yol açması ve kişisel bilgilerin güvenliğini zedeleyerek çok tehlikeli hale getirmesi nedeniyle kamu kurum ve kuruluşları, özel şirketler ve vatandaşlar için büyük bir endişe haline gelmiştir.

Bu araştımamız, ulusal güvenliğin bir bileşeni olan siber güvenliğin önemini ortaya koymaya çalışmıştır. Siber alanda güvenliğin önemi, siyasi, ekonomik ve sosyal ilişkilerin güvence altına alınmasının zarureti ve siber alan üzerinden yapılan saldırıları bertaraf etmek üzere atılacak adımları ele almıştır. Ayrıca ulusal güvenlik için, kapsamlı bir güvenlik stratejisi geliştirilerek bilimsel ve teknolojik gelişmeleri takip etmenin gerekliliği üzerinde durmuştur.

Yaşadığımız çağda geleneksel savaş modelinden, dijital teknolojik savaş modeline geçiş yapıldığına şahit olmakatyız. Dijital iletişim sistemine bağlı elektronik orduların oluşturulması, uzaktan kumandalı elektronik aletler, yapay zeka yüklenerek üretimi yapılan robotlar, yakın zamanda savaş teknolojisi açısından önemli bir çığır açacaktır. Dünya ülkeleri, bu hızlı gelişen teknoloji yarışı karşısında ulusal güvenlikleri için gerekli çalışmalar yapmaktadır. Örneğin ABD gibi gelişmiş ülkeler, Siber Tehditleri İzleme Komiteleri kurarak, Erken Siber Uyarı Sistemi gibi programları devreye koymuştur.

Siber gücün, gelecekte neler getirebileceğine, günü geldiğinde akla durgunluk verecek teknolojik gelişmeler sayesinde ulaşılacaktır. Günümüz dünyasında ise uluslararası ilişkiler üzerindeki etkileri, siber alanda yaşamın çeşitli alanlarında dijital teknolojiye olan güvenin artmasıyla birlikte, yeni ve çok ileri bir aşama oluşturacağı anlaşılmaktadır.

Çıkarımlar:

1. Siber saldırıları engellemek için gerekli tedbirler alınarak sızmaya ve müdahaleye en açık noktalar tespit edilmelidir. Bunun için de öncelikle Siber koruma sistemleri modernize edilmeli ve geliştirilmelidir. Ayrıca vatandaşlar arasında farkındalık yaratmak ve teknik gelişmelere ayak uyduran bir altyapı geliştirmek için gerekli çalışmalar ivedilikle yapılmalıdır.

2. Ulusal Güvenlik kavramı, yaşamın çeşitli sektörlerini içeren geniş ve çok boyutlu bir kavramdır. Bir ülkenin belirli bir stratejiyle ulusal güvenliğini sağlaması, en doğal hedeflerinden biridir. Ulusal ekonominin etkilenerek yeni uluslararası çatışma ortamına sürüklenmesi, siber saldırıların sonuçlarından biri olarak karşımıza çıkmaktadır.

3. Ulusal ve uluslararası düzeyde siber uzayın koruma düzeyini yükselten, modern teknolojiler yerlileştirilmelidir.

4. Terörizm, belirli bir dine veya millete isnat edilemeyen ve uluslararası sınırları aşan yasadışı oluşumlardır. Yahudi, Hıristiyan, İslam ve diğer birçok din mensupları arasından çağlar boyunca ortaya çıkmıştır. Günümüzde ise siber uzay, bu olgunun sınırlar ötesine aktarılmasını kolaylaştırmıştır.

5. Güvenlik görecelidir, mutlak bir gerçeklik değildir. Göreceli olması, devletlerin güçlerini artırma konusundaki sürekli arayışlarından kaynaklanmaktadır. Bu da kimi zaman güvenliğe ulaşmak yerine güvensizlik hissini artırmaktadır. Bu yüzden sadece dengeyi sağlamakla yetinmeyen birçok devlet, üstünlük ve nüfuz elde etme yarışına girmiştir. Uluslararası ilişkilerde belirsizlik ve güvensizlik durumuyla karşılaşıldığında realistlerin de adlandırdığı "güvenlik ikilemi" ortaya çıkmaktadır.

6. Siber uzay, sürekli gelişmenin bir sonucu olarak giderek daha tehlikeli hale gelen tehditlerin belirsizliği, ciddiyeti ve çeşitliliği ile karakterize edilmektedir. Bu da ülkelerin askeri ve güvenlik stratejisi açısından öncelikli planları dâhilinde görülen Siber Güvenliği, Ulusal Güvenliğin önemli bir parçası haline getirmiştir.

7. Siber tehditler, devletlerin egemenliğini tehdit eden sınır ötesi tehditler olmanın yanı sıra kendine özgü teknik niteliklere sahiptir. Bundan dolay bu tehditlerle mücadele iki düzeyde gerçekleşir. Birincisi, güvenlik güçleri ve siber güvenlik kurumlarının teknik açıdan modernize edilmesi gerekmektedir. İkincisi ise barışçıl ve güvenli bir ortam için ulusal mevzuata önemli caydırıcı yasalar konulmalıdır. Bu yasal çerçeve bölgesel ve uluslararası işbirliği oluşturularak güçlendirilmelidir. (Bu anlamda küresel dünya, yeni bir siber sosyal sözleşmeye ihtiyaç duymaktadır).

8. Irak'ta siber güvenliğin durumunu incelediğimizde, Irak hükümetinin, ülkenin siber güvenliğini artırması ve bu alanda küresel gelişmelere ayak uydurma konusunda stratejiler geliştirmesinin kaçınılmaz olduğunu tespit ettik. Irak'ın ivedilikle elektronik ve siber uzay altyapısını modernize ederek bir gelecek planı geliştirmeyi amaçlayan kapsamlı bir çalışma yapması gerekmektedir.

9. Mevcut Irak mevzuatı, siber suçlardan kaynaklanan sorunları çözememektedir. Bu konu ile ilgili yasalar, önceki birikimlerden ve gelişmiş ülkelerin deneyimlerinden yararlanılarak yeniden formüle edilmesi gerekmektedir. Bu nedenle en azından siber suçların yayılmasından kaynaklanan zorluklara karşı koymak ve caydırıcılığın sağlanması için, Irak anayasasının güvence altına aldığı Irak insan hak ve özgürlüklerini gözetecek şekilde Irak Bilgi Suçları Yasası'nın yeniden düzenlenerek bir an önce onaylanması gerekmektedir.

10. Irak'ta siber güvenliğin önündeki en önemli engellerden biri, Irak'taki siber güvenlik sistemini koruyabilecek eğitimli ulusal kadroların eksikliği ve Irak'a internet hizmetleri sağlamaktan sorumlu ulusal kurumların güçsüzlüğü ve eksikliğidir.

11. Bilgi Suçları Kanunu, suç isnat hedefini sınırlı ölçüde tutmamaktadır. Aksine, bilgisayarların çeşitli faaliyetlerle bağlantılı olarak kullanılmasını dahi suç sayacak hükümler içermektedir. Bu nedenle kanunun hükümleri uluslararası hukuka ve Irak anayasasına aykırılık teşkil etmektedir. Bu haliyle uygulanması halinde Iraklıların ifade özgürlüğünün ciddi bir şekilde kısıtlanmasına neden olacaktır. Otoriteyi elinde bulunduranlar, dini veya sosyal çıkarlara tehdit oluşturduğu iddiasıyla sıradan

basit söylemleri, yasal çerçevedeki muhalif görüşleri cezalandırmaya, kendi politikalarına yönelik eleştirileri önlemek için kanunu kullanabilir. Dolayısıyla Irak hükümeti tarafından oluşturulacak mevzuat, uluslararası standartlara uygun ve Irak anayasasına aykırı olmayacak şekilde tasarlanmalıdır.

12. Siber Güvenlik, bir ülkenin ulusal güvenliğinin ayrılmaz bir parçasıdır. Bu, çeşitli alanlarda siber teknolojiye artan bağımlılıktan kaynaklanmaktadır. İnternet kullanımının hızla artmaya devam etmesi ve gelişen teknolojik gelişmeler, sosyal, siyasal ve ekonomik hayatın tüm alanlarını etkisi altına almayı sürdürdürmesi, bu teknolojik altyapının ve siber alanda sağladığı hizmetlerin güvence altına alınmasını zorunlu hale getirmektedir. Bundan dolayı ulusal ve uluslararası güvenliğin kapsamlı bir unsuru olan Siber Güvenliğin önemi ortaya çıkmaktadır.

13. Her ülke tarafından ön planlama yapılması ve siber alanda karşılaştığı tehditlerle orantılı olarak belirli bir strateji geliştirmenin gerekliliği önem arz etmektedir. Bu stratejinin en önemli fonksiyonu, ulusal güvenliği tehdit eden siber saldırıları ve tahrip potansiyelini önceden tahmin ederek bertaraf etmektir.

14. "Ulusal Güvenlik" kavramı, ortaya çıkışı itibariyle, güvenlik ve savunma konusunda devletin iç güvenliğini ilgilendiren tüm alanların emniyetine işaret etmiştir. Siber güvenlik kavramı ise ülkenin siber alan ve teknolojisinin altyapısını, verilerini ve bilgilerini koruma ihtiyacını ifade etmiştir. Siber güvenlik, dünyanın bu alanda tanık olduğu teknolojik ve bilimsel ilerlemelerle orantılı olarak genişleyebilen ve gelişebilen bir kavram olarak karşımıza çıkmaktadır. Ayrıca siber güvenliğin ulusal güvenlik kadar üzerinde durulması gereken bir konu olduğu gözardı edilmemelidir. Çünkü bu hassasiyet, her gün bir yenisinin ortaya çıktığı, bilimsel ve teknolojik gelişmelere eşlik eden modern ve gelişmiş koruma programları ile yeni yasal mevzuat gerektiren yeni tehdit ve tehlikelerin büyüklüğü ile orantılıdır.

15. Siber alan, özellikle diktatörlük veya yozlaşmış rejimler tarafından yönetilen ülkelerde, devlet ve toplum arasındaki ilişki üzerinde büyük bir etkiye sahiptir. Sosyal medyanın birçok ülkede büyük siyasi değişikliklere neden olan bir platform haline geldiği bir gerçektir. Twitter ve Facebook gibi sosyal medya prgramları, gele-

cekte toplumun sosyal altyapısını derinden etkileyecek büyük değişikliklere neden olacaktır. Çünkü toplumsal ve kültürel değerlerin açıkça teşhir edildiği, yoksul bireyler de dâhil her tabakadaki insanlar tarafından neredeyse serbestçe kullanılabilir hale gelen internet kullanımının, siber ortama entegre edilmesiyle; sağladıkları veri, haber ve bilgilerle, kapalı toplumları infiale dönüştürme ya da tersine ita altına alma yeteneği sağlayacaktır.

16. Siber güvenlik ve ulusal güvenlik alanında yeni algıların geliştirilmesi ve bu iki güvenlikle ilgili modern kavramların, yasaların ve mevzuatın ortaya çıkması, küresel kalkınmanın yaşadığı atılımlar ile orantılı bir şekilde meydana gelmiştir. Çağımızda bu gelişmelerin zirve yaptığı bir dönemde elbette ki yeni zorlukların, tehlikelerin ve tehditlerin ortaya çıkmasını beraberinde getirmiştir. Bu yeni gelişmeler, uluslararası yasalarda ve genel olarak uluslararası ortamda büyük değişikliklere yol açacak ve yenidünya düzeninde güç dengelerini kesinlikle etkileyecektir. Çünkü Siber güç, yakın gelecekte geleneksel askeri gücü destekleyen en önemli ve en etkili faktörü olacaktır.

17. Hukuk ve teknoloji arasındaki ilişki, karşılıklı bir ilişkidir. Farklı teknolojik gelişmeler, bu teknolojilerin kullanımından doğan hukuki sorunlara uygun olarak yasal mevzuatları takip etmeyi gerektirir. Siber alan, internet ve bilişim teknolojileri sınır ötesi teknolojiler olduğundan, siber suçları azaltmak için yasal çerçevelerin ve mevzuatın geliştirilmesi kaçınılmazdır. Siber alan kullanımından kaynaklanan hukuki anlaşmazlıkların zaman, yer ve çözümüne uymamak şu anda neredeyse imkânsızdır. Bu da, siber güvenlik ile ilgili konularda uluslararası mahkemelerin oluşmasına ve bu konuda destekleyici kurum ve kuruluşların önemli roller üstlenerek, uluslararası düzeyde işbirliği yapmalarını zorunlu hale getirmektedir.

18. Bilişim teknolojisi ve İnternet kullanım hakkının güvence altına alınması, zaman ve mekân bakımından siber ihlallerin ve bilgi suçlarının üstesinden gelinmesini zorunlu hale getirmektedir. Bu, ulusal ve uluslararası eksende siber alandaki güvenlik seviyesi ve yapısı ile ayırt edilebilir. Bu nedenle, siber güvenliğe ulaşmak için, uluslararası kural ve standartları düzenlemeyi gerektirmektedir. Uluslararası anlaşmalar ve sözleşmeler oratak suç ve suçlularla birlikte mücadele etme imkanı sağlaya-

caktır. Zira hiçbir ülkenin diğer ülkelerle koordinasyonu ve işbirliği olmadan, ortaya çıkan bu suç organlarıyla baş edebileceğini beklememeliyiz.

19. Irak hükümetinin bu alanda ilerleme sağlama çabalarına rağmen, Irak'ta siber güvenlik, küresel çevrenin çok gerisinde kalmıştır. Özellikle bankacılık, ekonomik, finansal ve ticari alanlarda internet kullanımı ve elektronik yönetime geçiş, günümüz dünyasının vazgeçilmez stratejisi olmasına rağmen, Irak'ın ancak yakın zamanlarda siber dünya ile tanışması ve bugüne kadar henüz e-devlet sistemine gerektiği kadar itimat etmemesinin bu gecikmeye neden olduğunu söyleyebiliriz. Irak için artık geciktirilmeden sağlam bir elektronik veri ve bilgi sistemi altyapısının oluşturulması gerekmektedir. Altyapı tasarımındaki modernite, performans, hız ve hizmet sunumunda uluslararası standartlar baz alınmalıdır. Aynı zamanda Irak kadrolarına uzman kadrolar da ilave edilerek, hizmetin sağlanmasından güvenliğin sağlanmasına kadar yeni bir düzenleme getirilmelidir. Böylece siber tehditler ve ihlallerden korunma da bu strateji kapsamında güvence altına alınmalıdır.

20. Modern çağımız, yeni küreselleşme sistemi altında ülkelere giren bilgi teknolojisindeki büyük gelişmelerle dikkat çekmektedir. İnternet çağı, birçok toplumun binlerce yıldır süregelen değer yargılarını, inançlarını, kültür ve sistemlerini etkilemiştir. Bu gelişmeler doğal olarak devletlerin egemenliğini tehdit edecek büyüklükte sorunları da beraberinde getirmiştir. Bu birçok ülke ve toplum için, ülkelerin siber alan kullanımı ışığında ulaştığı yeni gelişme ve ilerleme koşulları ile orantılı olarak, büyük yapısal ve sosyal değişikliklerin merkezinde kalındığı anlamına gelmektdir. Bundan dolayı yeni küreselleşme sistemi ve entegrasyonu bağlamında Ulusal Güvenlik Örgütü'nde büyük değişiklikler yapılmasını gerekli kılmaktadır.

21. Siber alan, insanlık için tehlikeli ve zararlı niyetler taşıyan herhangi bir kuruluşun, kişinin veya ülkenin, kötü emellerine ulaşmak için kullanabileceği geniş bir alandır. Bu durum, bazı terör örgütlerinin hedeflerine ulaşmak için, internet üzerinden siber saldırılarını nasıl gerçekleştirdiklerine dair istihbarat bilgileriyle tespit edilmiştir. Öncelikle şiddet ve terörizmin hedefleri için maşa olarak kullanılan bilgisayar korsanları başta olmak üzere tüm terör faaliyeti içerisindeki unsurların etkisiz hale getirilmesi, sahip oldukları bilgi, döküman ve web sitelerinin engellenmesi için

gerekli önlemlerin alınması gerekmektedir. Bu konuda, siber güvenliği sağlamada uluslararası işbirliğin rolü, bilgi suçuyla mücadelede özel mevzuatın geliştirilmesi ve terörizmle mücadele için, kapsamlı ve entegre stratejilerin geliştirilmesi kaçınılmaz olarak karşımıza çıkmaktadır.

22. Uluslararası siber güvenliğin sağlanabilmesi için herkesin sorumluluk taşımasını öngören ve özellikle de ülkelerin yerel oluşumları dışındaki yeni uluslararası aktörlerin ortaya çıkmasıyla "Kolektif Güvenlik Sistemi" diye adlandırılan bir çalışma platformu ile bu alanda fevkalade bir işbirliği oluşturulabilir. Bu organizasyon, çalışmalarında başarı sağlamak için, her ülkeye eşit mesafede durmayı temel alacak ve siber güvenlikle ilgili uluslararası sistemdeki tüm devletleri, örgüt ve aktörleri kendi bünyesine dâhil ederek, aralarında ortaya çıkacak anlaşmazlıkların giderilmesinde önemli rol oynayacak etkili bir rol üstlenebilecektir.

23. Irak'ta ulusal güvenlik ve siber güvenliğin sağlanabilmesi için, siber saldırılara karşı, erken uyarı sistemleriyle müdahale ederek bu tehditler bertaraf edilmelidir. Elektronik ve dijital suçlarla mücadelede etkin istihbarat birimleri kurulmalıdır. Üniversitelerde Siber güvenlik ve siber uzay derslerinin müfredata dâhil edilerek öğretim sistemlerinin geliştirilmesi ve yükseköğretim öğrencilerinin bu bağlamda araştırma yapmaya yönlendirilmesi önemli bir husustur. Ayrıca özel sektörde siber alanda uzmanlaşmış kobilere destek verilerek yazılım ve güvenlik sistemlerine yatırım yapmaya teşvik edilmesi de Irak ulusal ve siber güvenliği açısından önemlidir.

24. Siber faaliyetleri, çoğunlukla dikta rejimlerin değişmesine yol açtığı, halkların, sosyal medyanın, karar vericilerin ve hatta orduların politik algıları üzerindeki etkisiyle özellikle sosyal ve siyasal sistemler üzerinde büyük etkiler yaratmıştır. Aynı şekilde demokratik sistemler üzerindeki etkisi de küçümsenemeyecek derecededir. Siber saldırıların, birçok ülkede demokratik sürecin bütünlüğüne doğrudan veya dolaylı bir tehdit oluşturduğu da kanıtlanmıştır. Çoğunlukla meşruiyeti baltalamak için demokrasilere olan popüler desteği engelleyerek siber saldırı faaliyetleriyle çeşitli yönlendirmeler yapılabilmektedir. En son yapılan ABD seçimlerindeki şaibeler bunu kanıtlanmıştır. Bu nedenle demokratik sistemler, başta internet, bilişim teknolojisi ve

siber alanı kontrol altına almak için küresel bir yasama mekanizması oluşturmak zorundadır.

25. Siber güvenliğe ulaşmanın en önemli yollarından biri, hükümetlerin ve karar vericilerin, aşırılık yanlısı ideolojilere teşvik eden sosyal ağların tehlikelerine dikkat çekmeleri olacaktır. Bu programların ve sitelerin kötüye kullanılması sonucu özellikle insan hakları, uyuşturucu kaçakçılığı, insan kaçakçılığı, suç ihlalleri gasp ve terör faaliyetlerine teşvik ettikleri derhal tespit edilerek deşifre edilmesi gerekmektedir. Ayrıca bu sitelerin ve programların bu tür kötü hedeflerini önlemek için özel yasalar, mevzuatlar ve çeşitli cezai yaptırımlar çıkartılıp uygulanmalıdır.

KAYNAKLAR

19 Aralık 2006 tarihli Genel Kurul, International Security p Bağlamında Bilgi ve Telekomünikasyon Alanında Gelişmeler.

Abbott, Jason (2012). Democracy@ Internet. Org Revisited: Analysing the Socio-Political Impact of the Internet and New Social Media in East Asia. In Third World Quarterly, 33, 333-57.

Abdul Sadiq, Adel (2017). Siber Savaşın Paternleri ve Küresel Güvenlik İçin Etkileri. Uluslararası Politika Dergisi, (17.05.2017).

Abdul Sadiq, Adel (2009). Strength in International Relations: A New Style and Different Challenges Cairo. Center for Political and Strategic Studies.

Adams, J. (2001). Sanal Savunma. Dışişleri, 98-112

AKYEŞILMEN, Nezir. Cybersecurity and Human Rights: Need for a Paradigm Shift?,". Cyberpolitik Journal, 2016, 1.1.

Akyeşilmen, N. (2016). Siber Güvenlik ve Özgürlük. İlkses Gazetesi, Erişim Adresi: http://ilksesgazetesi. com/yazilar/siber-guvenlik-veozgurluk-3816.

Akdenizli, Banu (2011). İnternet, Egemenlik ve Devlet: İnternetin Ulusal ve Uluslararası Yönetime Etkileri Üzerine Bır Değerlendirme. Yeditepe University Global Media Journal Turkish Edition, 34-35.

Aleksovski, Stefan, Bakreski, Oliver and Avramovska, Biljana (2014). Collective Security–the Role of International Organizations–Implications in International Security Order. Mediterranean Journal of Social Sciences, 5, 274.

Aljazeera.net (2010). Virüs "nükleer" bilgisayarlara saldırıyor İran.

Aljibouri, Farook (2016). Iraq Cyber Security Overview, and Announcing Our Al-Cyber.

Allam, Rachid. Obstacles to the Development of Electronic Commerce in the Arab World.

Al-zubaidi, Fawzi Hussein (2015). National Security Risk Assessment Methodology an Analytical Study of National Security Risk Assessment Methodology. Strategic Perspectives, (July 2015), 10-11.

Arquilla, John and Ronfeldt, David (1993). Cyberwar Is Coming!. Comparative Strategy, 12, 141-65.

Awadi, Aws Al. (2016). Siber Bilgi Güvenliği. http://www.bayancenter.org/2016.08.2386/.

Baggott, Erin (2014). Diversionary Cheap Talk: Domestic Discontent and Us Foreign Policy, 1945-2006. Unpublished manuscript, Harvard University: 1.

Bahi, Raghda (2017). Siber Caydırma: Kavram, İkilemler ve Gereksinimler. Siyaset Bilimi ve Hukuk Dergisi, (21 Şubat 2017).

Bailes, Alyson JK and Cottey, Andrew (1992). 4. Regional Security Cooperation in the Early 21st Century. Paper presented at the Conference on Interaction and.

Baran, Taha and Macar, Elçin (2017). Değişen Güvenlik Yaklaşımları Örneğinde Kopenhag Okulunun Toplumsal Güvenlik Yaklaşımı, Journal of International Social Research, 10 (54), 255-256.

Bba. Llb, Hons. (September 2017). Role of Ipr in Cyber Space. International Journal of Advanced Educational Research, 2: 136-37.

Beasley, Matthew (2009). Regime Security Theory: Why Do States with No Clear Strategic Security Concerns Obtain Nuclear Weapons? University of Oregon.

Birdişli, Fikret (2011). Ulusal Güvenlik Kavramının Tarihsel ve Düşünsel Temelleri.

Booth, Ken (1999). Three Tyrannies. Human Rights in Global Politics, 41.

Brangetto, Pascal and Aubyn, MKS (2015). Economic Aspects of National Cyber Security Strategies: project report. Annex 1, 9-16.

Buckland, B.S., Schreier, F., Winkler, T. H. ve Armées, C. s. l. c. d. d. f. (2010). Siber Güvenliğin Demokratik Yönetişim Zorlukları. DCAF, s.

Burchill, Scott, Linklater, Andrew, Devetak, Richard, Donnelly, Jack, Nardin, Terry, Paterson, Matthew, Reus-Smit, Christian, and True, Jacqui (2013). Theories of International Relations. New York: Palgrave Macmillan.

Burns, John F and Somaiya, Ravi (2010). Wikileaks Founder on the Run, Trailed by Notoriety. New York Times, 23.

Busannad, H. M. (2016). Birleşmiş Milletlerin Liberalizm Teorisini Kullanması. Zayed Üniversitesi.

Busannad, H. M. (2016). Liberalizm Teorisi. Zayed Üniversitesi kullanarak Birleşmiş Milletler Oluşturma.

Buzan, Barry and Waever, Ole (2003). Regions and Powers: The Structure of International Security. Cambridge University Press, 91.

Büyükbaş, H. Atici, N. (2012). Liberal Democratic Bariş Kuramı ettik.

Canan-Sokullu, E. (2012). Hindi Içinde Münazara Güvenliği: Yirmi Birinci Yüzyılın. Lexington Books, s Zorluklar ve değişimler, 46-50.

Case Study of Algeria (2010). Arab British Academy Higher education.

Castells, Manuel (1996). The Rise of the Network Society. The Information Age: Economy, Society, and Culture Volume I (Information Age Series), London: Blackwell.

Chesterman, S. (2004). Sen, İnsanlar: Birleşmiş Milletler, Geçiş Yönetiminin ve Devlet Kurma. On Demand Oxford University Press, s.

Cilluffo, Frank J, Cardash, Sharon L. and Salmoiraghi, George C. (2012). A Blueprint for Cyber Deterrence: Building Stability through Strength. Military and Strategic Affairs, 4, 3-23.

Clark, Wesley K. and Levin, Peter L. (2009). Securing the Information Highway. Foreign Aff., 88, 2-6 8-10.

Clarke, Richard Alan and Knake, Robert K. (2014). Cyber War. Tantor Media, Incorporated.

Colarik, Andrew M. and Janczewski, Lech J. (2008). Introduction to Cyber Warfare and Cyber Terrorism. Cyber Warfare and Cyber Terrorism. Hershey: Information Science Reference, 13-30.

Cole, Kristina, Chetty, Marshini, LaRosa, Christopher, Rietta, Frank, Schmitt, Danika K., Goodman, Seymour E. and Atlanta, G.A. (2008). Cybersecurity in Africa: An Assessment. Atlanta, Georgia: Sam Nunn School of International Affairs, Georgia Institute of Technology.

Conferences, Academic and Publishing Limited (2017). 12th International Conference on Cyber Warfare and Security 2017 Proceedings. Academic Conferences and Publishing Limited.

Cornish, Paul, Livingstone, David, Clemente, Dave and Yorke, Claire (2010). On Cyber Warfare: Chatham House London.

Craig, Anthony, and Brandon Valeriano (2016). Reacting to Cyber Threats: Protection and Security in the Digital Age. Global Security and Intelligence Studies, 1, 4.

Çalış, Ş. İdealizm-Realizm Tartışması. Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, (18), 225-243

Deibert, R. J. Girit-Nishihata, M. (2012). Siber Controls. Küresel Yönetişim Yayılması, 18, 339-361 ettik.

Deibert, Ronalo J and Crete-Nishihata, Masashi (2012). The Spread of Cyberspace Controls. Global Governance, 18, 339-61.

Dixon W. J. (1993). Demokrasi ve Uluslararası Çatışma Yönetimi. Çatışma Çözümleri Dergisi, 37 (1), 42-68.

Drent, Margriet, Dinnissen, Rosa, Ginkel, Bibi van, Hogeboom, Hans, Homan, Kees, Zandee, Dick, Rood, Jan and Meijnders, Minke (2014a). The Relationship between External and Internal Security. Netherlands Institute of International Relations: 7.

Drent, Margriet, Dinnissen, Rosa, Ginkel, Bibi van, Hogeboom, Hans, Homan, Kees, Zandee, Dick, Rood, Jan and Meijnders, Minke (2014b). The Relationship between External and Internal Security. Netherlands Institute of International Relations.

Dutta, Soumitra and Bilbao-Osorio, Beñat (2012). The Global Information Technology Report 2012: Living in a Hyperconnected World.

Fikileri, A. (2018). Uluslararası Kolektif Güvenlik, Albilad, 22432 Kavramının Geliştirilmesi.

Fischer, Eric A. (2005). Creating a National Framework for Cybersecurity: An Analysis of Issues and Options.

Fjäder, Christian (2014). The Nation-State, National Security and Resilience in the Age of Globalisation. Resilience, 2, 114-29.

Friedberg, A. L. (1987). Askeri Gücünün Değerlendirilmesi: Bir Gözden Deneme. Uluslararası Güvenlik, 12 (3), 190-202.

Gandhi, Robin, Sharma, Anup, Mahoney, William, Sousan, William, Zhu, Qiuming and Laplante, Phillip (2011). Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. IEEE Technology and Society Magazine, 30, 28-38.

General Assembly (19 December 2006). General Assembly, Developments in the Field of Information and Telecommunications in the Context of International-security.

Gibson, William. Neuromancer. 31.

Guzzini, S. (2015), "seküritizasyon" bir çift tarih, 2015: 02, DIIS Çalışma Raporu, s.

Habermas, J. (2006). Medya Toplumda Siyasal İletişim Demokrasi Hala Epistemik Bir Boyut Keyfini mu? Deneysel Araştırmalar, İletişim Teorisi Normatif Teorinin Etkisi, 16 (4), 411-42

Hacker, K. L. ve van Dijk, J. (2000). Dijital demokrasi: Teori ve Pratik Meseleleri. Sage, s.

Hammes, T. (2016). Teknolojiler Yakınsama ve Güç Dağılımları: Küçük, Akıllı ve Ucuz Silahların Evrimi. Cato Enstitüsü, s.

Hansen, L. ve Nissenbaum, H. (2009). Dijital Felaket, Siber Güvenlik ve Kopenhag Okulu. Uluslararası Çalışmalar Üç Aylık, 53 (4), 1155-1175.

Helfstein, Scott (2012). Edges of Radicalization: Individuals, Networks and Ideas in Violent Extremism: Combating Terrorism Center at West Point.

Henderson, E. A. ve Tucker, R. (2001). Açık ve Mevcut Krizler: Medeniyetler Çatışması ve Uluslararası Çatışma. Uluslararası Çalışmalar Üç Aylık, 45 (2), 317-338.

Heurlin, Bertel, Kristensen, Kristian and Søby, Bertel (2006). International Security. International Relations, 2, 172-216.

Hobbes, Thomas (2010). Leviathan, or, the Matter, Forme, & Power of a Common-Wealth Ecclesiasticall and Civill. 90.

Husted, Bryan W. (2000). The Impact of National Culture on Software Piracy. Journal of Business Ethics, 26, 197-211.

Hüseyin, A. S. (2016). Siasat Arabistan, Uluslararası Ilişkiler Teorileri: Disiplin ve Çeşitlilik.

Iglesias, Mario A Laborie (2011). Framework Document 05/2011: The Evolution of the Concept of Security. Institute for Strategic Studies of Spain 1.

Intriligator, Michael D and Coulomb, Fanny (2008). Global Security and Human Security. In War, Peace and Security. Emerald Group Publishing Limited, 53-66.

Isin, Engin F and Turner, Bryan S. (2002). Handbook of Citizenship Studies. Sage.

Ivanova, Petja (2006). Cybercrime and Cybersecurity. ProCon Limited.

Jabbour, M. A. (2015). Siber Güvenlik Üzerine Arap Sözleşmesi'nin Önemi. Siber Uzayın Güvenliği ve Güvenliği Konusunda Uzmanların Dördüncü Yıllık Toplantısı, Beyrut Arap Hukuki ve Adli Araştırma Merkezi - Arap Devletleri Birliği.

Jackson-Preece, Jennifer (2011). Security in International Relations. Undergraduate study in Economics, Management, Finance and the Social Sciences, University of London, 90p.

Jameson, Fredric and Miyoshi, Masao (1998). The Cultures of Globalization. Duke University Press.

Jarupunphol, Pita and Mitchell, Chris J. (2002). E-Commerce and the Media—Influences on Security Risk Perceptions. In Internet Technologies, Applications and Societal Impact: Springer. 163-73.

Jerotijević, Z. ve Palević, M. (2016). Güç-Uluslararası Toplumun Güvenlik Kavramı Dengesi. učasopis, Ekonomika, br, 1.

Jones, Steve (1995). Cybersociety. Sage.

Kalashnikov, Anthony (2012). Differing Interpretations: Causes of the Collapse of the Soviet Union. Constellations, 3, 76.

Kaljurand, M. (2016). Birleşmiş Milletler Hükümet Uzmanları Grubu: Estonya Perspektifi, Uluslararası Siber Normlar: Hukuk, Politika ve Sanayi Perspektifleri. (ed. Anna-Maria Osula ve Henry Rigigas). Tallinn: NATO CCD COE, 111-127.

Kant, Immanuel (1984). Sürekli Barış Üstüne Felsefi Bir Deneme, Seçilmiş Yazılar, (Çev. Nejat Bozkurt). İstanbul: Remzi Kitabevi.

Katzenstein, Peter J. (1996). Introduction: Alternative Perspectives on National Security. The culture of national security: Norms and identity in world politics 1.

Kaufman, S. J., Little, R. ve Wohlforth, W. C. (2007). Dünya Tarihinde Güç Dengesi. Springer, s. 14.

Kemp, Richard (2017). Legal Aspects of the Internet of Things. http://www.kempitlaw.com/wp-content/uploads/2017/06/Legal-Aspects-of-the-Internet-of-Things-KITL-20170610.pdf.

Kenaroğlu, Bahar and Turkish Aerospace Industry TAI (2003). Implications of Information Technology in Developing Countries and Its Impact in Organizational Change. 10.

Kesler, B. (2011). Nükleer Tesislerin Siber Saldırıya Karşı Savunmasızlığı; Stratejik Anlayışlar. Bahar 2010, Stratejik Analizler.

Keyser, Mike (2017). The Council of Europe Convention on Cybercrime. In Computer Crime: Routledge, 131-70.

Kissinger, H. A. (1992). Güç Dengesi Sürdürüldü. G. Allison y G. Treverton (eds.).

Kissinger, Henry A. (1969). Nuclear Weapons and Foreign Policy London. W. W. Norton & Company: Abridged edition.

Kuehl, D. T. (2009). Siber Uzaydan Sibergüç'e: Sorunun Tanımlanması. Siber Güç ve Ulusal Güvenlik, 30.

Kurt, Selim (2015). Toplumsal Güvenliğin Yükselişi. International Journal of Social Science Studies, 469-70.

Kymlicka, W. (1989). Liberal Bireycilik ve Liberal Tarafsızlık. Etik, 99 (4), 883-905.

Labban, Sherif Darwish Al (2016). Unbridled Freedoms and Dangers: Social Networking Sites and Their Impact on Egyptian National Security. http://www.acrseg.org/40123.

Lamus, F. (2017). Makyavelli'nin Ahlaki Teorisi: Ahlaki Hristiyanlık Karşısında Civic Fazilet.

Lasswell, H. D. (1927). Siyasal Propaganda Teorisi. Amerikan Siyasal Bilimler Dergisi, 21 (3), 627-631.

Lee, Jyh-An (2018). Hacking into China's Cybersecurity Law.

Lewis, James Andrew (2002). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic & International Studies Washington, DC.

Libicki, Martin C. (2009). Cyberdeterrence and Cyberwar. Rand Corporation.

Lindsay, Jon R, Cheung, Tai Ming and Reveron, Derek S. (2015). China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain. USA: Oxford University Press.

Lippmann, Walter (1987). Us Foreign Policy: Shield of the Republic. (Boston: Little, Brown, 1943). See also Samuel P. Huntington. Coping with the Lippmann Gap. Foreign Affairs: America and the World, 88: 7-8.

Liu, Fang, Burton-Jones, Andrew and Xu, Dongming (2014). Rumors on Social Media in Disasters: Extending Transmission to Retransmission. Paper presented at the PACIS.

Lombaerde, Philippe de and Söderbaum, Fredrik (2013). Regionalism. Los Angeles: SAGE. SAGE library of international relations.

Luard, E. (2016). Güç Dengesi: Uluslararası İlişkiler Sistemi, 1648-1815. Springer, s. 26.

Luiijf, Ham, Besseling, Kim, Spoelstra, Maartje and Graaf, Patrick De (2011). Ten National Cyber Security Strategies: A Comparison. Paper presented at the International Workshop on Critical Information Infrastructures Security.

Lupovici, Amir (2011). Cyber Warfare and Deterrence: Trends and Challenges in Research. Military and Strategic Affairs, 3, 49-62.

Lynn, William J. (2010). Defending a New Domain: The Pentagon's Cyberstrategy. Foreign Affairs, 89, 97-108.

Mahiroğulları, Adnan (2010). Küreselleşmenin Kültürel Değerler Uzerine Etkisi. 1277-80.

Maier, Charles S. (1990). Peace and Security for the 1990s. Unpublished paper for the MacArthur Fellowship Program, Social Science Research Council, 12, 5.

Malec, Mieczyslaw (2003). Security Perception: Within and Beyond the Traditional Approach. Master of Arts in National Securty Affairs, Naval Postgraduate School Monterey Ca.

Masahiro, M. (2012). Egemenlik ve Uluslararası Hukuk. Aichi Üniversitesi, Japonya, 4-5

McDonald, M. (2008). Menkul Kıymetleştirme ve Güvenlik İnşaatı. Avrupa Uluslararası İlişkiler Dergisi, 14 (4), 563-587.

McKenzie, COL Timothy M. (2017). Is Cyber Deterrence Possible? Vol. 4, Perspectives on Cyber Power (Book 4), CreateSpace Independent Publishing Platform

McNamara, Robert S. (1968). The Essence of Security.

Melissen, J. (2005). Yeni Kamu Diplomasisi: Uluslararası İlişkilerde Yumuşak Güç. Springer, s. 12.

Melissen, Jan (2005). The New Public Diplomacy: Soft Power in International Relations. Springer.

Mesjasz, Czeslaw (2008). Ekonomik Güvenlik. Uluslararası İlişkiler/International Relations, 125-50.

Mirasola, Chris (2016). Understanding China's Cybersecurity Law. Lawfare, November 8.

Mohammed, Alaa Abdul Hafeez (2017). Ulusal Güvenlik Kavramı ve Boyutlarını Belirle.https://www.europarabct.com/%D9%85%D9%81%D9%87%D9%88%D9%85-%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D9%82%D9%88%D9%85%D9%8A-%D9%88%D8%AA%D8%AD%D8%AF%D9%8A%D8%AF-%D8%A3%D8%A8%D8%B9%D8%A7%D8%AF%D9%87. (17.07.2018).

Molla, A. ve Licker, P. S. (2001). E-ticaret Sistemleri Başarısı: IS Başarısının Delone ve MacLean Modelini Genişletme ve Saygı Gösterme Girişimi, J. Electron. Ticaret Res., 2 (4), 131-141.

Nasruddin, O. (2013). Liberal Teori. Arabi Ben Mehdi Cezayir Üniversitesi, 18.

Naughton, John (2016). The Evolution of the Internet: From Military Experiment to General Purpose Technology. Journal of Cyber Policy, 1, 5-28.

Nekola, Martin (2006). Political Participation and Governance Effectiveness–Does Participation Matter. Centre for Social and Economic Strategies (CESES), Faculty of Social Sciences, Charles University, Prague, Czech Republic.

Neu, Carl Richard and Charles Wolf Jr. (1994). The Economic Dimensions of National Security. In Secondary The Economic Dimensions of National Security, ed Secondary, 11. Reprint, Reprint.

Neyse, N. (2017). 2016 ABD Seçimi: Demokrasi Internetten Kurtulabilir mi? Demokrasi Dergisi, 28 (2), 63-76

Norris, P. ve Grömping, M. (2017). Populist Seçim Bütünlüğüne Yönelik Tehditler: Seçimlerde Yıl, 2016-2017.

Nye Jr, J. S. (2008). Kamu Diplomasisi ve Yumuşak Iktidar. Amerikan Siyasal ve Sosyal Bilimler Akademisinin Yıllıkları, 616 (1), 94-109.

Nye, J. S. (2004). Yumuşak Güç: Dünya Siyasetinde Başarı Aracı. Kamu İşleri, s.

Obama (2009). Obama Announces Strategy against Cyber Attacks. The New York Times.

OECD, O. (2004). OECD Kurumsal Yönetim İlkeleri. Contaduría y Administración (216).

Ohlin, Jens David (2016). Did Russian Cyber Interference in the 2016 Election Violate International Law. Tex. L. Rev., 95, 1579.

Oladiran, Olusegun and Adadevoh, Irene Omolola (2008). Cultural Dimensions of the National Security Problem. Rethinking Security in Nigeria: Conceptual Issues in the Quest for Social Order and National Integration, 95.

Owen IV, J. M. (2005). Irak ve Demokratik Barış - Demokrasilerin Mücadele Etmediğini Söyledi. Dış İlişkiler, 84, 122.

Özlük, E. (2007). uluslararasa ılışkıler tarihinin yapısökümü ettik.

Paret, Peter (1989). Military Power. The Journal of Military History, 53, 240.

Paulo, Sebastian (2014). International Cooperation and Development. Retrieved, March 20, 2016.

Persily, Nathaniel (2017). The 2016 Us Election: Can Democracy Survive the Internet? Journal of Democracy, 28, 63-76.

Piccone, T. (2017). Demokrasi, Cinsiyet Eşitliği ve Cinsiyet Güvenliği.

Reardon, Robert and Choucri, Nazli (2012). The Role of Cyberspace in International Relations: A View of the Literature. Paper presented at the ISA ANNUAL CONVENTION.

Risse-Kappen, Thomas (1991). "Did" Peace through Strength" End the Cold War? Lessons from Inf. International Security, 16, 162-88.

Rosenzweig, Paul (2015). The Cybersecurity Act of 2015. Lawfare: The Lawfare Institute, 16.

Rosso, Stephen J Del (1995). The Insecure State: Reflections on" the State" and" Security" in a Changing World. Daedalus, 175-207.

Russett, B.M. Oneal, J.R. ve Cox, M. (2000). Medeniyetler Çatışması ya da Realizm ve Liberalizm Dejavu? Bazı Kanıtlar. Barış Araştırmaları Dergisi, 37(5), 583-608.

Sadek, A. A. (2012). Elektronik İktidar: Siber Uzayda Kitle Yayılımı Silahları. Mısır, Siber Uzay Araştırmaları Merkezi.

Sadek, A. A. (2014a). Mısırlı Yorumlar, Mısır'da İnternet ve Siyasal Reform Için.

Sadek, A. A. (2014b). Arap Dünyasındaki Değişim Dalgalarında Elektronik Alan: Yerel ve Dünya Bağlamında Bir Çalışma.

Samaan, Jean-Loup (2011). Beyond the Rift in Cyber Strategy. Strategic Insights, 10, 4-14.

Sancak, Kadir (2003). Güvenlİk Kavrami Etrafindakİ Tartişmalar ve Uluslararasi Güvenliğin Dönüşümü. Sosyal Bilimler Dergisi, 126.

Sanger, David E and Markoff, John (2009). Obama Outlines Coordinated Cyber-Security Plan.

Sarkesian, Sam Charles, Williams, John Allen and Cimbala, Stephen J. (2012). Us National Security: Policymakers, Processes, and Politics. Lynne Rienner Publishers.

Schouten, P. (2009). Theory Konuşması: 37: Dünya Emirleri Üzerine Robert Cox, Tarihsel Değişim ve Uluslararası Ilişkilerde Teorinin Amacı. Teori Konuşmaları, 1-8.

Semenova, E. (2011). Yönetici-Egemen Bir Sistemde Bakanlık ve Parlamento Seçkinleri: Sovyet Sonrası Rusya 1991-2009. Karşılaştırmalı Sosyoloji, 10 (6), 908-927.

Sempa, F. P. (2015). Hans Morgenthau ve Asya'da Güç Dengesi. Erişim Adresi, https://thediplomat.com/2015/05/hans-morghenthau-and-the-balance-of-power-in-asia.

Shinder, Deb (2011). What Makes Cybercrime Laws So Difficult to Enforce. IT Security.

Snyder, Jack L. (1977). The Soviet Strategic Culture. Implications for Limited Nuclear Operations. In Secondary The Soviet Strategic Culture. Implications for Limited Nuclear Operations, ed Secondary ———, 8. Reprint, Reprint.

Stats, IW. (2018). Internet Usage Statistics, the Internet Big Picture. World Internet Users and Population Stats. Miniwatts Marketing Group.

Stigall, Dan E, Miller, Chris and Donnatucci, Lauren (2018). The 2018 Us National Strategy for Counterterrorism: A Synoptic Overview. Dan Stigall et al., The.

Sulmeyer, Michael (2018). Military Set for Cyber Attacks on Foreign Infrastructure. April 11. Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School.

Sur, M. (2013). Birleşmiş Milletler Örgütünün Gelişimi ve Geleceği. Yaşar Üniversitesi Dergisi, 8 (Özel), 2535-2550.

Şener, Bülent (2014). Küreselleşme Sürecında Ulus-Devlet ve Egemenlik Olguları.

Tajine, F. (2017). Malezya'nın Dijital Ortamın Güvenlik Tehditleri Altındaki Savunma Politikaları: Gerçeklik ve Zorluklar. Üniversite Kasdi Merbah Ouargla UKMO Cezayir.

Tarboshi, Jabbar Abdul (2010). Irak Ulusal Güvenlik Kavramı.

Teivāns-Treinovskis, Jānis and Jefimovs, Nikolajs (2012). State National Security: Aspect of Recorded Crime. Journal of Security & Sustainability, 2, 42.

Telgraf, t. (2011). Pentagon, sosyal medyaya yeni savaş alanı olarak bakıyor. Erişim Adresi, https://www.telegraph.co.uk/technology/social-media/8651284/Pentagon-looks-to-social-media-as-new-battlefield.htm

Timonen, Heidi and Nikander, Maarit (2017). Interdependence of Internal and External Security.

Timothy, M Mckenzie (2017). Is Cyber Deterrence Possible? (Pdf Only). AIR University Press.

Tshtoush, Hail Abdul Mawla (2012). Ulusal Güvenlik ve Yeni Dünya Düzeni Altında Devlet Gücü Unsurları. Ürdün: Dar Al Hamed Yayıncılık ve Dağıtım.

Ve İdari Bilimler Fakültesi Dergisi (40), 1-19 ettik Eleştirel Bir Değerlendirme, Erciyes Üniversitesi İktisadi:

Von Solms, Rossouw and Niekerk, Johan Van (2013). From Information Security to Cyber Security. Computers & Security, 38, 97-102.

Waever, Ole (2008). Toplumsal Güvenliğin Değişen Gündemi. Uluslararası İlişkiler/International Relations, 151-78.

Watson, Cynthia Ann (2002). Us National Security. A Reference Handbook: Abc-clio.

Wee, By Sui-Lee (2017). China's New Cybersecurity Law Leaves Foreign Firms Guessing. The New York Times: B3.

Wiener, Norbert (1961). Cybernetics or Control and Communication in the Animal and the Machine. Vol. 25, MIT press.

Wolfers, Arnold (1952). "National Security" as an Ambiguous Symbol. Political Science Quarterly, 67, 481-502.

Work, Robert O. (2017). "An Interview with Robert O. Work." In Joint Force Quarterly 84. (ed. William T. Eliason). Washington: National Defense University Press, NDU Press. 6 - 11.

Yalçın, Hasan Basri (2017). Ulusal Güvenlik Stratejisi: Abd-İngiltere-Fransa-Rusya-Çin. SET Vakfı İktisadi İşletmesi.

Yeşil, Salih (2009). Kültürel Farklılıkların Yönetimi ve Alternatif Bir Strateji: Kültürel Zeka. 104.

Zeadally, Sherali and Flowers, Angelyn (2014). Cyberwar: The What, When, Why, and How [Commentary]. IEEE Technology and Society Magazine, 33, 14-21.

Zukrowska, Katarzyna (1999). The Link between Economics, Stability and Security in a Transforming Economy. Economic Developments and Reforms in Cooperation Partner Countries: The Link Between Economics, Security and Stability, 269-83.

(Lene Hansen, Görüntüler ve Uluslararası Güvenlik Proje Direktörü ve Kopenhag Üniversitesi Siyaset Bilimi Bölümü'nde Uluslararası İlişkiler Profesörüdür)

Abbott, Jason. 2012. "Democracy@ Internet. Org Revisited: Analysing the Socio-Political Impact of the Internet and New Social Media in East Asia." In Third World Quarterly. Vol. 33. 333-57.

Abdul Sadiq, Adel. 2009. Strength in International Relations: A New Style and Different Challenges

Cairo: Center for Political and Strategic Studies, .

Adams, James. 2001. "Virtual Defense." Foreign Affairs: 98-112.

Adel Abdul - Sadiq. 2017. " Siber Savaşın Paternleri Ve Küresel Güvenlik İçin Etkileri,." Uluslararası Politika Dergisi, (17.05.2017).

Adel Abdul. Sadek. 2014a. "The Electronic Space in the Waves of Change in the Arab World: A Study in the Local and World Context." 29,12,2014 ed: Arab Center for Cyberspace Research.

———. 2014b. ""For Internet and Political Reform in Egypt." Egyptian Comments." http://accronline.com/article_detail.aspx?id=18456.

akdenizli, Banu. 2011. "ınternnet ,Egemenlik Ve Devlet :Internetin Ulusal Veuluslararası Yönetime Etkileri Uzerine Bır Değerlendirme ". Yeditepe University Global Media Journal Turkish Edition: 34-35.

Akyeşilmen, Nezir. 2016a. "Cybersecurity and Human Rights: Need for a Paradigm Shift?,"." Cyberpolitik Journal 1: 44-46.

———. 2016b. "Siber Güvenlik Ve Özgürlük." İlkses Gazetesi, Erişim Adresi: http://ilksesgazetesi. com/yazilar/siber-guvenlik-veozgurluk-3816.

AL-Awadi, Aws . . 2016. "Siber Bilgi Güvenliği.". http://www.bayancenter.org/2016/08/2386/.

Al-Jibouri, Farook. 2016. "Iraq Cyber Security Overview, and Announcing Our Cyber ..".

Al-Rodhan, Nayef RF, and Gérard Stoudmann. 2006. "Definitions of Globalization: A Comprehensive Overview and a Proposed Definition." Program on the Geopolitical Implications of Globalization and Transnational Security 6.

Al-Zubaidi, Fawzi Hussein. 2015. "National Security Risk Assessment Methodology an Analytical Study of National Security Risk Assessment Methodology ". Strategic Perspectives (July 2015.). 10-11.

Aleksovski, Stefan, Oliver Bakreski, and Biljana Avramovska. 2014. "Collective Security–the Role of International Organizations–Implications in International Security Order." Mediterranean Journal of Social Sciences 5: 274.

aljazeera. 2020. Amerika, İran ve Rusya'yı seçimlere müdahale etmekle suçluyor ve iki ülke inkar ediyor. https://www.aljazeera.net/news/2020/10/22/%D8%A7%D9%84%D8%A7%D8%B3%D8%AA%D8%AE%D8%A8%D8%A7%D8%B1%D8%A7%D8%AA-%D8%A7%D9%84%D8%A3%D9%85%D9%8A%D8%B1%D9%83%D9%8A%D8%A9-%D8%AA%D8%AA%D9%87%D9%85-%D8%A5%D9%8A%D8%B1%D8%A7%D9%86-2.

aljazeera.net. 2010. . ""Virus Attacks "Nuclear" Computers Iran."." https://www.aljazeera.net/news/international/2010/9/28/%D9%81%D9%8A%D8%B1%D9%88%D8%B3-%D9%8A%D8%B6%D8%B1%D8%A8-%D8%A2%D9%84%D8%A7%D9%81-%D8%A7%D9%84%D8%AD%D9%88%D8%A7%D8%B3%D9%8A%D8%A8-%D8%A8%D8%A5%D9%8A%D8%B1%D8%A7%D9%86.

Allam, Rachid. "Obstacles to the Development of Electronic Commerce in the Arab World

Case Study of Algeria." Arab British Academy Higher education, 2010.

Amador, FV Garcia, Louis Bruno Sohn, and Richard R Baxter. 1974. Recent Codification of the Law of State Responsibility for Injuries to Aliens: Martinus Nijhoff Publishers.

Arquilla, John, and David Ronfeldt. 1993. "Cyberwar Is Coming!". Comparative Strategy 12: 141-65.

Awadi, Aws Al. 2016. "Siber Bilgi Güvenliği.". http://www.bayancenter.org/2016/08/2386/.

Bagdasaryan, Eugene, Andreas Veit, Yiqing Hua, Deborah Estrin, and Vitaly Shmatikov. 2020. "How to Backdoor Federated Learning." Paper presented at the International Conference on Artificial Intelligence and Statistics.

Baggott, Erin. 2014. "Diversionary Cheap Talk: Domestic Discontent and Us Foreign Policy, 1945-2006." Unpublished manuscript, Harvard University: 1.

Bahi, Raghda. 2017. "Siber Caydırma: Kavram, İkilemler Ve Gereksinimler." Siyaset Bilimi ve Hukuk Dergisi'nin (21. Şubat 2017).

Bailes, Alyson JK, and Andrew Cottey. 1992. "4. Regional Security Cooperation in the Early 21st Century." Paper presented at the Conference on Interaction and.

Barack., Obama. 2015. National Security Strategy: White House.

Baran, Taha, and Elçin macar. 2017. "Değişen Güvenlik Yaklaşımları Örneğinde Kopenhag Okulunun Toplumsal Güvenlik Yaklaşımı." Journal of International Social Research 10.

BBA. LLB, Hons. September 2017. "Role of Ipr in Cyber Space". International Journal of Advanced Educational Research 2: 136-37.

Beasley, Matthew. "Regime Security Theory: Why Do States with No Clear Strategic Security Concerns Obtain Nuclear Weapons?", University of Oregon, 2009.

Ben-Asher, Noam, and Cleotilde Gonzalez. 2015. "Effects of Cyber Security Knowledge on Attack Detection." Computers in Human Behavior 48: 51-61.

Bennetts, Simon. 2013. "Owasp Zed Attack Proxy." AppSec USA.

Betz, David J, and Tim Stevens. 2011. "Chapter Three: Cyberspace and War." Adelphi Series 51: 75-98.

BİRDİŞLİ, Fikret. 2011. "Ulusal Güvenlik Kavramının Tarihsel Ve Düşünsel Temelleri."

Booth, Ken. 1999. "Three Tyrannies." Human rights in global politics: 41.

Bos, Adriaan. 2005. "The Importance of the 1899, 1907 and 1999 Hague Conferences for the Legal Protection of Cultural Property in the Event of Armed Conflict." Museum international 57: 32-40.

Brangetto, Pascal, and MKS Aubyn. 2015. "Economic Aspects of National Cyber Security Strategies." Brangetto P., Aubyn MK-S. Economic Aspects of National Cyber Security Strategies: project report. Annex 1: 9-16.

Brophy, Peter, and Edward Halpin. 1999. "Through the Net to Freedom: Information, the Internet and Human Rights." Journal of information science 25: 351-64.

Buckland, Benjamin S, Fred Schreier, Theodor H Winkler, and Centre pour le contrôle démocratique des forces armées. 2010. Democratic Governance Challenges of Cyber Security: DCAF.

Burchill, Scott, Andrew Linklater, Richard Devetak, Jack Donnelly, Terry Nardin, Matthew Paterson, Christian Reus-Smit, and Jacqui True. 2013. Theories of International Relations. New York,: Palgrave Macmillan.

Burns, John F, and Ravi Somaiya. 2010. "Wikileaks Founder on the Run, Trailed by Notoriety." New York Times 23.

Busannad, Hamda Mohd. 2016. "Creation of the United Nations Using the Liberalism Theory." academia.

Büyükbaş, Hakkı, and Nilgün Atici. 2012. "Liberal Demokratik Barış Kuramı: Eleştirel Bir Değerlendirme." Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi: 1-19.

Buzan, Barry, Barry G Buzan, Ole Waever, Ole W'ver, Ole Waever Barry Buzan, and Ole Wver. 2003. Regions and Powers: The Structure of International Security. Vol. 91: Cambridge University Press.

ÇALIŞ, Şaban, and Erdem Özlük. 2007. "Uluslararasi İlİşkİler Tarİhİnİn YapisÖkÜmÜ: İdealİzm-RealİZm Tartişmasi." Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi: 225-43.

Canan-Sokullu, Ebru. 2012. Debating Security in Turkey: Challenges and Changes in the Twenty-First Century: Lexington Books.

Carnahan, Burrus M. 1998. "Lincoln, Lieber and the Laws of War: The Origins and Limits of the Principle of Military Necessity." Am. J. Int'l L. 92: 213.

Castells, Manuel. 1996. The Rise of the Network Society. The Information Age: Economy, Society, and Culture Volume I (Information Age Series): London: Blackwell.

Chang, Rocky KC. 2002. "Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial." IEEE communications magazine 40: 42-51.

Chauvin, Justine. 2016. "Book Review:" Cyber War Will Not Take Place"." Interstate-Journal of International Affairs 2015.

Chen, Kai. 2017. "No Place to Hide: Edward Snowden, the Nsa, and the Us Surveillance State." Taylor & Francis.

Chen, Ping, Lieven Desmet, and Christophe Huygens. 2014. "A Study on Advanced Persistent Threats." Paper presented at the IFIP International Conference on Communications and Multimedia Security.

Cilluffo, Frank J, Sharon L Cardash, and George C Salmoiraghi. 2012. "A Blueprint for Cyber Deterrence: Building Stability through Strength." Military and Strategic Affairs 4: 3-23.

Clapper, James R. . 2011. "Statement for the Record on the Worldwide Threat Assessment of the Us Intelligence Community for the House Permanent Select Committee on Intelligence." In Secondary Statement for the Record on the Worldwide Threat Assessment of the Us Intelligence Community for the House Permanent Select Committee on Intelligence., ed Secondary ———, 35. washington Reprint, Reprint.

Clark, Wesley K, and Peter L Levin. 2009. "Securing the Information Highway." Foreign Aff. 88: 2-6 8-10.

Clarke, Richard Alan, and Robert K Knake. 2014. Cyber War: Tantor Media, Incorporated.

Cohen, Eliot A. 1996. "A Revolution in Warfare." Foreign Affairs: 37-54.

Cohen, Fred. 1988. "On the Implications of Computer Viruses and Methods of Defense." Computers & Security 7: 167-84.

Colarik, Andrew M, and Lech J Janczewski. 2008. "Introduction to Cyber Warfare and Cyber Terrorism." Janczewski and Colarik. Cyber Warfare and Cyber Terrorism. Hershey: Information Science Reference, pp xiii-xxx.

Cole, Kristina, Marshini Chetty, Christopher LaRosa, Frank Rietta, Danika K Schmitt, Seymour E Goodman, and GA Atlanta. 2008. "Cybersecurity in Africa: An Assessment." Atlanta, Georgia, Sam Nunn School of International Affairs, Georgia Institute of Technology.

Conferences, Academic, and Publishing Limited. 2017. 12th International Conference on Cyber Warfare and Security 2017 Proceedings: Academic Conferences and Publishing Limited.

Cornish, Paul, David Livingstone, Dave Clemente, and Claire Yorke. 2010. On Cyber Warfare: Chatham House London.

Cory, Nigel. 2017. "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" In Secondary Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?, ed Secondary ———. Reprint, Reprint.

Craig, Anthony, and Brandon Valeriano. 2016. "Reacting to Cyber Threats: Protection and Security in the Digital Age." Global Security and Intelligence Studies 1: 4.

Crocker, Ryan. 2017. "Working Group Report

the Future of Iraq." In Secondary Working Group Report

the Future of Iraq, ed Secondary ———: Rafic Hariri Center for the Middle East. Reprint, Reprint.

Deibert, Ronalo J, and Masashi Crete-Nishihata. 2012. "The Spread of Cyberspace Controls." Global Governance 18: 339-61.

Dixon, William J. 1993. "Democracy and the Management of International Conflict." Journal of Conflict Resolution 37: 42-68.

Drent, Margriet, Rosa Dinnissen, Bibi van Ginkel, Hans Hogeboom, Kees Homan, Dick Zandee, Jan Rood, and Minke Meijnders. 2014a. "The Relationship between External and Internal Security." Netherlands Institute of International Relations.

———. 2014b. "The Relationship between External and Internal Security." Netherlands Institute of International Relations: 7.

Droege, Cordula. 2012. "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians." International Review of the Red Cross 94: 533-78.

Dutta, Soumitra, and Beñat Bilbao-Osorio. 2012. "The Global Information Technology Report 2012: Living in a Hyperconnected World."

Erendor, Mehmet Emin, and Gürkan Tamer. 2017. "The New Face of the War: Cyber Warfare." Cyberpolitik Journal 2: 53-70.

Fiki, Abeer. . 2018. " "Development of the Concept of International Collective Security.". albilad 22430.

Fischer, Eric A. 2005. "Creating a National Framework for Cybersecurity: An Analysis of Issues and Options."

Fjäder, Christian. 2014. "The Nation-State, National Security and Resilience in the Age of Globalisation." Resilience 2: 114-29.

Friedberg, Aaron L. 1987. "The Assessment of Military Power: A Review Essay." International Security 12: 190-202.

Gagandeep, Aashima, and Pawan Kumar. 2012. "Analysis of Different Security Attacks in Manets on Protocol Stack a-Review." International Journal of Engineering and Advanced Technology (IJEAT) 1: 269-75.

Gandhi, Robin, Anup Sharma, William Mahoney, William Sousan, Qiuming Zhu, and Phillip Laplante. 2011. "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political." IEEE Technology and Society Magazine 30: 28-38.

Garfinkel, Robert, Ram Gopal, and Paulo Goes. 2002. "Privacy Protection of Binary Confidential Data against Deterministic, Stochastic, and Insider Threat." Management Science 48: 749-64.

Giani, Annarita, Eilyan Bitar, Manuel Garcia, Miles McQueen, Pramod Khargonekar, and Kameshwar Poolla. 2013. "Smart Grid Data Integrity Attacks." IEEE Transactions on Smart Grid 4: 1244-53.

Gibson, William. "Neuromancer." 31.

Glass, Amy Jocelyn, Kamal Saggi, Amitava Dutt, and Jaime Ros. 2008. "The Role of Foreign Direct Investment in International Technology Transfer." International handbook of development economics 2: 137-49.

Gomez, Miguel Alberto N. . 2016. ""Arming Cyberspace: The Militarization of a Virtual Domain." ". Global Security and Intelligence Studies 1.

Guzzini, Stefano. 2015. A Dual History of" Securitisation": JSTOR.

Habermas, Jürgen. 2006. "Political Communication in Media Society: Does Democracy Still Enjoy an Epistemic Dimension? The Impact of Normative Theory on Empirical Research." Communication theory 16: 411-26.

Hacker, Kenneth L, and Jan van Dijk. 2000. Digital Democracy: Issues of Theory and Practice: Sage.

Hai, Quan Tran, and Seong Oun Hwang. . 2018. " "An Efficient Classification of Malware Behavior Using Deep Neural Network." .". Journal of Intelligent & 35: , 5801-14.

Hammes, Thomas X. 2016. "Technologies Converge and Power Diffuses." Cato Institute Policy Analysis.

Hansen, Lene, and Helen Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School." International Studies Quarterly 53: 1155-75.

Hathaway, Oona A, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel. 2012. "The Law of Cyber-Attack." California Law Review: 817-85.

Helfstein, Scott. 2012. Edges of Radicalization: Individuals, Networks and Ideas in Violent Extremism: Combating Terrorism Center at West Point.

Henderson, Errol A, and Richard Tucker. 2001. "Clear and Present Strangers: The Clash of Civilizations and International Conflict." International Studies Quarterly 45: 317-38.

Heurlin, Bertel, Kristian KRISTENSEN, and Bertel SØBY. 2006. "International Security." International Relations 2: 172-216.

Hirst, Paul, and Grahame Thompson. . 1995. . " "Globalization and the Future of the Nation State." Economy A." Economy and Society 24: 408-44.

Hobbes, Thomas. 2010. "Leviathan, or, the Matter, Forme, & Power of a Common-Wealth Ecclesiasticall and Civill." 90.

Hoffman, Frank G. 2007. . Conflict in the 21st Century: The Rise of Hybrid Wars:. (Quantico, Virginia),: Potomac Institute for Policy Studies Arlington.

Hong, Jason. 2012. "The State of Phishing Attacks." Communications of the ACM 55: 74-81.

Hughes, Christopher R. 2002. "China and the Globalization of Icts: Implications for International Relations." New Media & Society 4: 205-24.

Hussein, Ahmad Qassem. . 2016. " "International Relations Theories: Discipline and Diversity." ". siasat arabia: 123-24.

Iglesias, Mario A Laborie. 2011. "Framework Document 05/2011: The Evolution of the Concept of Security." Institute for Strategic Studies of Spain 1.

Ingols, Kyle, Matthew Chu, Richard Lippmann, Seth Webster, and Stephen Boyer. 2009. "Modeling Modern Network Attacks and Countermeasures Using Attack Graphs." Paper presented at the 2009 Annual Computer Security Applications Conference.

Intriligator, Michael D, and Fanny Coulomb. 2008. "Global Security and Human Security." In War, Peace and Security: Emerald Group Publishing Limited. 53-66.

Isin, Engin F, and Bryan S Turner. 2002. Handbook of Citizenship Studies: Sage.

Ivanova, Petja. 2006. Cybercrime and Cybersecurity: ProCon Limited.

Jabbour, Mona Ashkar. . 2015. ""The Importance of the Arab Convention on Cybersecurity."." Paper presented at the Paper presented at the The fourth annual meeting of the specialists in the security and safety of cyberspace,, Beirut.

Jablon, David P. 1997. "Extended Password Key Exchange Protocols Immune to Dictionary Attack." Paper presented at the Proceedings of IEEE 6th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises.

Jackson-Preece, Jennifer. 2011. "Security in International Relations." Undergraduate study in Economics, Management, Finance and the Social Sciences. Undergraduate study in Economics, Management, Finance and the Social Sciences University of London, 90p.

Jackson, Stephen. 2016. "Nato Article 5 and Cyber Warfare: Nato's Ambiguous and Outdated Procedure for Determining When Cyber Aggression Qualifies as an Armed Attack." The CIP Report.

Jameson, Fredric, and Masao Miyoshi. 1998. The Cultures of Globalization: Duke University Press.

Jarupunphol, Pita, and Chris J Mitchell. 2002. "E-Commerce and the Media—Influences on Security Risk Perceptions." In Internet Technologies, Applications and Societal Impact: Springer. 163-73.

Jensen, Eric Talbot. 2016. "The Tallinn Manual 2.0: Highlights and Insights." Geo. J. Int'l L. 48: 735.

Jerotijević, Z, and M Palević. 2016. "The Balance of Power–the Security Concept of the International Community, Učasopis." Ekonomika, br 1.

Jones, Steve. 1995. Cybersociety: Sage.

Joyce, Daniel. 2015. "Internet Freedom and Human Rights." European Journal of International Law 26.

Kahn, Paul W. 1987. "From Nuremberg to the Hague: The United States Position in Nicaragua V. United States and the Development of International Law." Yale J. Int'l l. 12: 1.

Kalashnikov, Anthony. 2012. "Differing Interpretations: Causes of the Collapse of the Soviet Union." Constellations 3: 76.

Kaljurand, Marina. 2016. "United Nations Group of Governmental Experts: The Estonian Perspective." International Cyber Norms: Legal, Policy & Industry Perspectives. Tallinn: NATO CCD COE Publications, Tallinn. Available at: https://ccdcoe. org/library/publications/international-cyber-normslegal-policy-industry-perspectives.

Kant, Immanuel. 1984. "Sürekli Barış Üstüne Felsefi Bir Deneme." Seçilmiş Yazılar, Çev: Nejat Bozkurt, Remzi Kitabeevi, İstanbul.

Katzenstein, Peter J. 1996. "Introduction: Alternative Perspectives on National Security." The culture of national security: Norms and identity in world politics 1.

Kaufman, Stuart J, Richard Little, and William Curti Wohlforth. 2007. The Balance of Power in World History: Springer.

Kellenberger, Jakob. 2011. "International Humanitarian Law and New Weapon Technologies." 34th Round Table on current issues of international humanitarian law, San Remo: 8-10.

Kemp, Richard. 2017. "Legal Aspects of the

Internet of Things." http://www.kempitlaw.com/wp-content/uploads/2017/06/Legal-Aspects-of-the-Internet-of-Things-KITL-20170610.pdf.

Kenaroğlu, Bahar, and Turkish Aerospace Industry TAI. 2003. "Implications of Information Technology in Developing Countries and Its Impact in Organizational Change." 10.

Keyser, Mike. 2017. "The Council of Europe Convention on Cybercrime." In Computer Crime: Routledge. 131-70.

Kissinger, Henry A. 1992. "Balance of Power Sustained." G. Allison y G. Treverton (eds.).

———. 1969. Nuclear Weapons and Foreign Policy London: W. W. Norton & Company; Abridged edition.

köse, Esra. 2017. "Dİjİtal Dİplomasİ Nİn Sosyo-Ekonomİk Ve Sosyo-Polİtİk Yapiya Etkİsİ .". Suleyman Demirel University

The Journal of Faculty of Economics

and Administrative Sciences

22: pp.2347-70.

Krombholz, Katharina, Heidelinde Hobel, Markus Huber, and Edgar Weippl. 2015. "Advanced Social Engineering Attacks." Journal of Information Security and applications 22: 113-22.

Kuehl, Daniel T. 2009. "From Cyberspace to Cyberpower: Defining the Problem." Cyberpower and national security 30.

Kundu, Shusmoy, et al. ". 2018. "Cyber Crime Trend in Bangladesh, an Analysis and Ways out to Combat the Threat."." Paper presented at the International Conference on Advanced Communication Technology (ICACT). IEEE,, Dhaka, Bangladesh.

KURT, Öğr Gör Selim. 2015. "Toplumsal Güvenliğin Yükselişi." International Journal of Social Science Studies: 469-70.

Kymlicka, Will. 1989. "Liberal Individualism and Liberal Neutrality." Ethics 99: 883-905.

Labban, Sherif Darwish Al -. 2016. "Unbridled Freedoms and Dangers: Social Networking Sites and Their Impact on Egyptian National Security." http://www.acrseg.org/40123.

Lamus, Felipe. "Machiavelli's Moral Theory: Moral Christianity Versus Civic Virtue." MA Thesis. Duke University, 2016.

Lasswell, Harold D. 1927. "The Theory of Political Propaganda." The American Political Science Review 21: 627-31.

Lee, Jyh-An. 2018. "Hacking into China's Cybersecurity Law."

Lewis, James Andrew. 2002. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats: Center for Strategic & International Studies Washington, DC.

Libicki, Martin C. 2009. Cyberdeterrence and Cyberwar: Rand Corporation.

Lieverman, Theodore M. 1986. "Law and Power: Some Reflections on Nicaragua, the United States, and the World Court." HeinOnline.

Limnéll, Jarno. 2016. "The Cyber Arms Race Is Accelerating–What Are the Consequences?". Journal of Cyber Policy 1: 50-60.

Lindsay, Jon R, Tai Ming Cheung, and Derek S Reveron. 2015. China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain: Oxford University Press, USA.

Lippmann, Walter. 1987. "Us Foreign Policy: Shield of the Republic (Boston: Little, Brown, 1943)." See also Samuel P. Huntington,“Coping with the Lippmann Gap,” Foreign Affairs: America and the World 88: 7-8.

Liu, Fang, Andrew Burton-Jones, and Dongming Xu. 2014. "Rumors on Social Media in Disasters: Extending Transmission to Retransmission." Paper presented at the PACIS.

LOMBAERDE, Philippe de, and Fredrik SÖDERBAUM. 2013. "Regionalism." Los Angeles: SAGE. SAGE library of international relations.

Luard, Evan. 2016. The Balance of Power: The System of International Relations, 1648–1815: Springer.

Luiijf, HAM, Kim Besseling, Maartje Spoelstra, and Patrick De Graaf. 2011. "Ten National Cyber Security Strategies: A Comparison." Paper presented at the International Workshop on Critical Information Infrastructures Security.

Lupovici, Amir. 2011. "Cyber Warfare and Deterrence: Trends and Challenges in Research." Military and Strategic Affairs 3: 49-62.

Lynn, William J. 2010. "Defending a New Domain: The Pentagon's Cyberstrategy." Foreign Affairs 89: 97-108.

mahiroğulları, Adnan. . 2005. "Küreselleşmenin Kültürel Değerler Uzerine Etkisi." Sosyal Siyaset Konferansları Dergisi: 1275-88.

Maier, Charles S. 1990. "Peace and Security for the 1990s." Unpublished paper for the MacArthur Fellowship Program, Social Science Research Council 12: 5.

Malec, Mieczyslaw. "Security Perception: Within and Beyond the Traditional Approach." MASTER OF ARTS IN NATIONAL SECURITY AFFAIRS, NAVAL POSTGRADUATE SCHOOL MONTEREY CA, 2003.

Mallik, Amitav. 2004. Technology and Security in the 21st Century: A Demand-Side Perpective: Oxford university press.

Maogoto, Jackson, and Steven Freeland. 2007. "The Final Frontier: The Laws of Armed Conflict and Space Warfare." Conn. J. Int'l L. 23: 165.

Masahiro, Miyoshi. 2012. "Sovereignty and International Law." Aichi University, Japan: 4-5.

Mastapeter, Craig W. 2008. "The Instruments of National Power: Achieving the Strategic Advantage in a Changing World." In Secondary The Instruments of National Power: Achieving the Strategic Advantage in a Changing World, ed Secondary ———. Reprint, Reprint.

McDonald, Matt. 2008. "Securitization and the Construction of Security." European journal of international relations 14: 563-87.

McGraw, Gary, and Greg Morrisett. 2000. "Attacking Malicious Code: A Report to the Infosec Research Council." IEEE software 17: 33-41.

McKenzie, COL Timothy M. 2017. Is Cyber Deterrence Possible? Vol. 4, Perspectives on Cyber Power (Book 4): CreateSpace Independent Publishing Platform

McNamara, Robert S. 1968. "The Essence of Security."

Melissen, Jan. 2005. The New Public Diplomacy: Soft Power in International Relations: Springer.

Meron, Theodor. 2006. The Humanization of International Law: Brill Nijhoff.

Meserve, Stephen A, and Daniel Pemstein. 2020. "Terrorism and Internet Censorship." Journal of Peace Research: 0022343320959369.

Mesjasz, Czeslaw. 2008. "Ekonomik Güvenlik." Uluslararası İlişkiler/International Relations: 125-50.

Michael, James Bret, Thomas C Wingfield, and Duminda Wijesekera. 2003. "Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System." Paper presented at the Proceedings 27th Annual International Computer Software and Applications Conference. COMPAC 2003.

Mills, John R. 2010. "Counterinsurgency in Cyberspace." Geo. J. Int'l Aff. 11: 157.

Mirasola, Chris. 2016. "Understanding China's Cybersecurity Law." Lawfare. November 8.

Mohammed, Alaa Abdul Hafeez. 2017. "Ulusal Güvenlik Kavramı

Ve Boyutlarını Belirle." https://www.europarabct.com/%D9%85%D9%81%D9%87%D9%88%D9%85-%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D9%82%D9%88%D9%85%D9%8A-%D9%88%D8%AA%D8%AD%D8%AF%D9%8A%D8%AF-%D8%A3%D8%A8%D8%B9%D8%A7%D8%AF%D9%87. (17.07.2018).

Molla, A., & Licker, P. S. . 2001. "E-Commerce Systems Success: An Attempt to Extend and Respecify the Delone and Maclean Model of Is Success. ." Journal of Electronic Commerce Research, 2.

Moravcsik, Andrew. 2010. "Liberal Theories of International Relations: A Primer." Princeton, NJ: Princeton University.

Najeeb bin Omar, Owainat. 2017. "Electronic Terrorism: The Concept and International and Regional Efforts to Combat It." The journal of Teacher Researcher of Legal and Political Studies 06: 18.

Nasruddin, Oshin. . " Liberal Theory in International Relations." University of Arabi Ben Mehdi, 2013.

Nations, Secretary-General of the United. 2019. "Countering the Use of Information and Communications Technologies

for Criminal Purposes." In Secondary Countering the Use of Information and Communications Technologies

for Criminal Purposes, ed Secondary ———, 82. New York: United Nations A/74/130 and General Assembly. Reprint, Reprint.

Naughton, John. 2016. "The Evolution of the Internet: From Military Experiment to General Purpose Technology." Journal of Cyber Policy 1: 5-28.

Nekola, Martin. 2006. "Political Participation and Governance Effectiveness–Does Participation Matter." Centre for Social and Economic Strategies (CESES), Faculty of Social Sciences, Charles University, Prague, Czech Republic.

Neu, Carl Richard, and Charles Wolf Jr. 1994. "The Economic Dimensions of National Security." In Secondary The Economic Dimensions of National Security, ed Secondary ———, 11. Reprint, Reprint.

Norris, Pippa, and Max Grömping. 2017. "Populist Threats to Electoral Integrity: The Year in Elections, 2016-2017." Electoral Integrity Project, PEI 5.

Nye, JR, and S Joseph. 2008. "Public Diplomacy and Soft Power, the Annals of the American Academy of Political and Social Science." New York: Routledge Handbook.

Nye Jr, Joseph S. 2004. Soft Power: The Means to Success in World Politics: Public affairs.

Nye Jr, Joseph S. . 2010. "Cyber Power." In Secondary Cyber Power., ed Secondary ———, 31. Cambridge: Belfer Center for Science and International Harvard Kennedy School and Affairs. Reprint, Reprint.

Obama. 2009. "Obama Announces Strategy against Cyber Attacks." The New York Times.

OECD, OCDE. 2004. "The Oecd Principles of Corporate Governance." Contaduría y Administración.

Oladiran, Olusegun, and Irene Omolola Adadevoh. 2008. "Cultural Dimensions of the National Security Problem." Rethinking Security in Nigeria: Conceptual Issues in the Quest for Social Order and National Integration: 95.

Owen IV, John M. 2005. "Iraq and the Democratic Peace-Who Says Democracies Don't Fight." Foreign Aff. 84: 122.

Paret, Peter. 1989. "Military Power." The Journal of Military History 53: 240.

parliament, Iraqi. 2019. "The Internal System of the Iraqi Parliament." http://en.parliament.iq/.

Paul, Christopher, Isaac Porche, and Elliot Axelband. . 2014. The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces. Santa Monica, California: . Rand Corporation,.

Paul Cornish, Rex Hughes and David Livingstone. 2009. "Cyberspace and the National Security of the United Kingdom Threats and Responses." In Secondary Cyberspace and the National Security of the United Kingdom

Threats and Responses, ed Secondary ———, 46. London,: Royal Institute of International Affairs Reprint, Reprint.

Paulo, Sebastian. 2014. "International Cooperation and Development." Retrieved March 20: 2016.

Pax, Thomas J. 1985. "Nicaragua V. United States in the International Court of Justice: Compulsory Jurisdiction or Just Compulsion." BC Int'l & Comp. L. Rev. 8: 471.

Persily, Nathaniel. 2017. "The 2016 Us Election: Can Democracy Survive the Internet?". Journal of democracy 28: 63-76.

Petreski, Milorad. . 2015. ""The International Public Law and the Use of Force by the States."." J. Liberty & Int'l Aff. 1 9.

phys.org. 2011. "Pentagon Looks to Social Media as New Battlefield." ". " https://phys.org/news/2011-07-pentagon-social-media-battlefield.html.

Piccone, ted. 2017. "Democracy, Gender Equality, and Gender Security."

Podhorec, Milan. 2012. "Cyber Security within the Globalization Process." Journal of Defense Resources Management (JoDRM) 3: 19-26.

Rabet, Delphine. 2009. "Human Rights and Globalization: The Myth of Corporate Social Responsibility?".

Radanliev, Petar, David Charles De Roure, Razvan Nicolescu, Michael Huth, Rafael Mantilla Montalvo, Stacy Cannady, and Peter Burnap. 2018. "Future Developments in Cyber Risk Assessment for the Internet of Things." elsevier 102: 14-22.

Reardon, Robert, and Nazli Choucri. 2012. "The Role of Cyberspace in International Relations: A View of the Literature." Paper presented at the ISA ANNUAL CONVENTION.

Risse-Kappen, Thomas. 1991. "Did" Peace through Strength" End the Cold War? Lessons from Inf." International Security 16: 162-88.

Rogan, Hanna. . 2006. " "Jihadism Online-a Study of How Al-Qaida and Radical Islamist Groups Use the Internet for Terrorist Purposes."." In Secondary "Jihadism Online-a Study of How Al-Qaida and Radical Islamist Groups Use the Internet for Terrorist Purposes.", ed Secondary ———. Kjeller, Norway Norwegian Defence Research Establishment (FFI). Reprint, Reprint.

Rosenzweig, Paul. 2015. "The Cybersecurity Act of 2015." Lawfare. The Lawfare Institute 16.

Rosso, Stephen J Del. 1995. "The Insecure State: Reflections on" the State" and" Security" in a Changing World." Daedalus: 175-207.

Russett, Bruce M, John R Oneal, and Michaelene Cox. 2000. "Clash of Civilizations, or Realism and Liberalism Déjà Vu? Some Evidence." Journal of Peace Research 37: 583-608.

Şafak, Erdi. 2020. "Uluslararası Hukukta Değişen Güvenlik Algısı Ve Saldırı Suçu Bağlamında Siber Saldırılar." Selçuk Üniversitesi Hukuk Fakültesi Dergisi 28: 127-60.

Sancak, Kadir. 2003. "GÜvenlİk Kavrami Etrafindakİ Tartişmalar Ve Uluslararasi GÜvenlİğİn DÖnÜşÜmÜ." Sosyal Bilimler Dergisi: 126.

Sanger, David E, David D Kirkpatrick, and Nicole Perlroth. 2017. "The World Once Laughed at North Korean Cyberpower. No More." The New York Times 15.

Sanger, David E, and John Markoff. 2009. "Obama Outlines Coordinated Cyber-Security Plan."

Sarkesian, Sam Charles, John Allen Williams, and Stephen J Cimbala. 2012. Us National Security: Policymakers, Processes, and Politics: Lynne Rienner Publishers.

Sassen, Saskia. 1999. "Digital Networks and Power." Spaces of culture: City, nation, world: 49-63.

Schmitt, Michael N. 1998. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." Colum. J. Transnat'l L. 37: 885.

Schmitt, Michael N, and Liis Vihul. 2014. "Proxy Wars in Cyberspace: The Evolving International Law of Attribution." Fletcher Sec. Rev. 1: 53.

Schouten, Peer. 2009. "Theory Talk# 37: Robert Cox on World Orders, Historical Change, and the Purpose of Theory in International Relations." Theory Talks: 2.

Semenova, Elena. 2011. "Ministerial and Parliamentary Elites in an Executive-Dominated System: Post-Soviet Russia 1991–2009." Comparative Sociology 10: 908-27.

Sempa, Francis P. 2015. "Hans Morgenthau and the Balance of Power in Asia." The Diplomat 25.

Şener, Bülent. 2014. " Küreselleşme Sürecında Ulus-Devlet Ve Egemenlik Olguları."

Shaalan, Sulafa Al. 2016. "Adapting the Use of Electronic Warfare in Armed Conflicts in Accordance with International Humanitarian Law." Kufa Journal of Legal and Political Sciences. 41.

Shackelford, Scott J. 2009. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law." Berkeley J. Int'l Law 27: 192.

Shackelford, Scott J, and Richard B Andres. 2010. "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem." Geo. J. Int'l L. 42: 971.

Shafqat, Narmeen, and Ashraf Masood. 2016. "Comparative Analysis of Various National Cyber Security Strategies." International Journal of Computer Science and Information Security 14: 129.

Shinder, Deb. 2011. "What Makes Cybercrime Laws So Difficult to Enforce." IT Security.

Snyder, Jack L. 1977. "The Soviet Strategic Culture. Implications for Limited Nuclear Operations." In Secondary The Soviet Strategic Culture. Implications for Limited Nuclear Operations, ed Secondary ———, 8. Reprint, Reprint.

Stigall, Dan E, Chris Miller, and Lauren Donnatucci. 2018. "The 2018 Us National Strategy for Counterterrorism: A Synoptic Overview." Dan Stigall et al., The.

Sulmeyer, Michael. , 2018. "“Military Set for Cyber Attacks on Foreign Infrastructure.” , April 11." Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School.

Tajine, Farida. . 2017. ""Malaysia's Defense Policies under the Security Threats of the Digital Environment: Reality and Challenges." Paper presented at the The second international forum on national defense policies, Algeria.

Tanizawa, Toshi, Gerald Paul, Reuven Cohen, Shlomo Havlin, and H Eugene Stanley. 2005. "Optimization of Network Robustness to Waves of Targeted and Random Attacks." Physical review E 71: 047101.

Tarboshi, Jabbar Abdul. 2010. "Irak Ulusal Güvenlik Kavramı."

Teivāns-Treinovskis, Jānis, and Nikolajs Jefimovs. 2012. "State National Security: Aspect of Recorded Crime." Journal of Security & Sustainability Issues 2: 42.

Ticehurst, Rupert. 1997. "The Martens Clause and the Laws of Armed Conflict." International Review of the Red Cross Archive 37: 125-34.

Tiirmaa-Klaar, Heli. 2011. "Cyber Security Threats and Responses at Global, Nation-State, Industry and Individual Levels." Ceri SciencesPo: 1-10.

Timonen, Heidi, and Maarit Nikander. 2017. "Interdependence of Internal and External Security."

Tshtoush, Hail Abdul Mawla. 2012. Ulusal Güvenlik Ve Yeni Dünya Düzeni Altında Devlet Gücü Unsurları. Ürdün: Dar Al Hamed Yayıncılık ve Dağıtım.

Von Solms, Rossouw, and Johan Van Niekerk. 2013. "From Information Security to Cyber Security." computers & security 38: 97-102.

Waever, Ole. 2008. "Toplumsal Güvenliğin Değişen Gündemi." Uluslararası İlişkiler/International Relations: 151-78.

Waltz, Kenneth N. 2008. Realism and International Politics: Routledge.

———. 2010. Theory of International Politics: Waveland Press.

Watson, Cynthia Ann. 2002. Us National Security: A Reference Handbook: Abc-clio.

Wee, By Sui-Lee. 2017. "China’s New Cybersecurity Law Leaves Foreign Firms Guessing." The New York Times: B3.

Wendt, Alexander. 1995a. "Anarchy Is What States Make of It: The Social Construction of Power Politics (1992)." In International Theory: Springer. 129-77.

———. 1995b. "Constructing International Politics." International Security 20: 71-81.

Wiener, Antje. 2006. "Constructivist Approaches in International Relations Theory: Puzzles and Promises." Constitutionalism Webpapers, ConWEB.

Wiener, Norbert. 1961. Cybernetics or Control and Communication in the Animal and the Machine. Vol. 25: MIT press.

Wigand, Rolf T. 1997. "Electronic Commerce: Definition, Theory, and Context." The information society 13: 1-16.

Williams, Meredydd, Louise Axon, Jason RC Nurse, and Sadie Creese. 2016. "Future Scenarios and Challenges for Security and Privacy." Paper presented at the 2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI).

Williams, Paul D. 2012. Security Studies: An Introduction: Routledge.

Wolfers, Arnold. 1952. "" National Security" as an Ambiguous Symbol." Political Science Quarterly 67: 481-502.

Work, Robert O. 2017. "An Interview with Robert O. Work." In Joint Force Quarterly 84, ed. William T. Eliason. Washington: National Defense University Press,NDU Press. 6 - 11.

Yalçın, Hasan Basri. 2017. Ulusal Güvenlik Stratejisi: Abd-İngiltere-Fransa-Rusya-Çin: SET Vakfı İktisadi İşletmesi.

Yardi, Sarita, Daniel Romero, and Grant Schoenebeck. 2010. "Detecting Spam in a Twitter Network." First Monday.

Yasar, Nurgul, Fatih Yasar, and Yucel Topcu. 2012. Operational Advantages of Using Cyber Electronic Warfare (Cew) in the Battlefield. Vol. 8408, Spie Defense, Security, and Sensing: SPIE.

Yen, Ting-Fang, and Michael K Reiter. 2008. "Traffic Aggregation for Malware Detection." Paper presented at the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment.

Yeşil, Salih. 2009. "Kültürel Farklılıkların Yönetimi Ve Alternatif Bir Strateji: Kültürel Zeka." 104.

Yılmaz, Sait. 2008. "Uluslararası İlişkilerde Güç Ve Güç Dengesinin Evrimi." Stratejik Araştırmalar Dergisi 1: 27-65.

Yusuf, Özer. 2018. "Savaşın Değişen Karakteri :Teori Ve Uygulamada Hibrit Savaşın ". Güvenlik Bilimleri Dergisi 7: 29-56.

Zeadally, Sherali, and Angelyn Flowers. 2014. "Cyberwar: The What, When, Why, and How [Commentary]." IEEE Technology and Society Magazine 33: 14-21.

Zinnes, Dina A. 1967. "An Analytical Study of the Balance of Power Theories." Journal of Peace Research 4: 270-87.

Zukrowska, Katarzyna. 1999. "The Link between Economics, Stability and Security in a Transforming Economy." Economic Developments and Reforms in Cooperation Partner Countries: The Link Between Economics, Security and Stability: 269-83.