T.C.
BATMAN ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
SİYASET BİLİMİ VE ULUSLARARASI İLİŞKİLER ANABİLİM DALI

SİBER GÜVENLİK BAĞLAMINDA YENİ TEHDİT ALGILAMALARININ TÜRKİYE'NİN GÜVENLİK POLİTİKALARINA ETKİLERİ

YÜKSEK LİSANS TEZİ

Hazırlayan
Ozan Zeki KİRAZ

Danışman
Dr. Öğr. Üyesi Murat CİHANGİR

NİSAN-2021
BATMAN

SİBER GÜVENLİK BAĞLAMINDA YENİ TEHDİT ALGILAMALARININ TÜRKİYE'NİN GÜVENLİK POLİTİKALARINA ETKİLERİ

ORİJİNALLİK RAPORU

%11	%10	%4	%
BENZERLİK ENDEKSİ	İNTERNET KAYNAKLARI	YAYINLAR	ÖĞRENCİ ÖDEVLERİ

BİRİNCİL KAYNAKLAR

1	adlisicil.adalet.gov.tr İnternet Kaynağı	%1
2	dergipark.org.tr İnternet Kaynağı	%1
3	www.researchgate.net İnternet Kaynağı	%1
4	afyonluoglu.org İnternet Kaynağı	<%1
5	www.batman.edu.tr İnternet Kaynağı	<%1
6	docplayer.biz.tr İnternet Kaynağı	<%1
7	cyberpolitikjournal.org İnternet Kaynağı	<%1
8	www.erkamtemir.com İnternet Kaynağı	<%1

TEZ BİLDİRİMİ

Bu tezdeki bütün bilgilerin etik davranış/akademik kurallar çerçevesinde elde edildiğini ve Sosyal Bilimler Enstitüsü Tez ve Seminer Yazım Kılavuzu kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

DECLARATION PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules/ethical conduct and Batman University Instute of Social Sciences' Thesis and Seminar Writing Guide. I also declare that, as required by these rules and conduct, I have fully cited and referenced all materials and results that are not original to this work.

İmza

Ozan Zeki KİRAZ

ÖNSÖZ

Bu çalışma, Siber Güvenlik Bağlamında yeni tehdit algılarının Türkiye'nin güvenlik politikalarına etkilerini incelemektedir. Bu sebeple siber güvenlik politikalarının güvenlik anlamında risk olarak algılanıp algılanmadığı sorgulanmış, siber güvenliğin uluslararası güvenlik içindeki yeri ve önemi araştırılmıştır.

Bilişim, internet veya siber suçlar olarak adlandırılan suçların işlenme oranlarının çok olması nedeniyle bu suçlardan mağdur olanların sayısı azımsanmayacak derecede çoktur. Ayrıca mağdurlar arasında özel şahıslarla birlikte özel ve kamu tüzel kişileri de bulunabilmektedir. Bu suçların önemli bir özelliği de kitle mağduriyeti yaratmalarıdır. Yani bu suçlardan bir tek hareketi ile binlerce veya milyonlarca kişiyi mağdur olarak etkileyebilmektedir. Doğal olarak bu sebeple kanun uygulayıcılarının işini zorlaştırmaktadır. Özellikle bu tür suçlarda sınır aşma olgusu çok sık karşılaşılan bir durumdur. Bu nedenle mücadelesi zor ve devletlerarası işbirliğini gerekli kılmaktadır. Devletlerarası işbirliğini gerekli kıldığı noktada uluslararası ilişkiler literatüründe incelenmesi ve öneminin araştırılması gerekmektedir. Teknoloji insan ve toplum yaşamının merkezine yerleşmiş durumdadır. Bu yeni ilişki biçimlerine ilişkin bilimsel incelemeler istenilen seviyede bulunmamaktadır. Bu çalışmanın bu anlamda literatüre katkı potansiyeli bakımından önem arz etmektedir.

Bu tezi hazırlarken çalışmalarımda yardım ve sabırları için anneme, babama, eşime ve oğluma teşekkürü borç bilirim. Tez danışmanlığımı üstlenerek çalışmalarımda ilgi ve alakasını esirgemeyen Dr. Öğr. Üyesi Murat CİHANGİR hocama yol göstericiliği ve desteklerinden ötürü minnettarım.

Tezimin faydalı olmasını umuyorum. Tezi ithaf etmek gerekirse bu vatan için şehadet şerbetini içen aziz şehitlerimize ve gazilerimize ithaf ediyorum.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR

AB :Avrupa Birliği

ABD :Amerika Birleşik Devletleri

AFAD :Afet ve Acil Durum Yönetimi Başkanlığı

AHİM : Avrupa İnsan Hakları Mahkemesi

ARPA :İleri Araştırma Projeleri Ajansı (Advanced Research Projects Agency)

ARPANET :İleri Araştırma Projeleri Ajansı Ağı (Advanced Research Projects Agency Network)

ASELSAN : Askeri Elektronik Sanayii

BM :Birleşmiş Milletler

BTK : Bilgi Teknolojileri ve İletişim Kurumu

CERT :Bilgisayar Acil Müdahale ekibi

CIA :Merkezi İstihbarat Teşkilatı (Central Intelligence Agency)

DDOS :Distributed Denial of Service(Dağıtılmış Hizmet Reddi-Dağıtılmış Ağ Saldırısı)

ENISA :Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (European Union Agency for Network and Information Security)

HAVELSAN : Hava Elektronik Sanayii

IMF :Uluslararası Para Fonu (International Monetary Fund)

IŞID :Irak Şam İslam Devleti örgütü

İHA : İnsansız Hava Aracı

MİT : Milli İstihbarat Teşkilatı

MOBESE :Mobil Elektronik Sistem Entegrasyonu

Mossad :Ha-Mossad leModi'in uleTafkidim Meyuhadim (İstihbarat ve Özel Harekatlar Enstitüsü)

NATO :Kuzey Atlantik Antlaşması Örgütü (Atlantic Treaty Organization)

SİHA : Silahlı İnsansız Hava Aracı

TİB : Telekomünikasyon İletişim Başkanlığı

TCK :Türk Ceza Kanunu

TSK : Türk Silahlı Kuvvetleri

TUBİTAK : Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

USOM :Ulusal Siber Olaylara Müdahale Merkezi

ÖZET

YÜKSEK LİSANS TEZİ

SİBER GÜVENLİK BAĞLAMINDA YENİ TEHDİT ALGILAMALARININ TÜRKİYE'NİN GÜVENLİK POLİTİKALARINA ETKİLERİ

Ozan Zeki KİRAZ

BATMAN ÜNİVERSİTESİ SOSYAL BİLİMLER ENSTİTÜSÜ
SİYASET BİLİMİ VE ULUSLARARASI İLİŞKİLER ANABİLİM DALI

DANIŞMAN: Dr. Öğr. Üyesi Murat CİHANGİR

2020, 118 Sayfa

Jüri
Dr. Öğr. Üyesi Murat CİHANGİR
Dr. Öğr. Üyesi Sadullah ÖZEL
Doç. Dr. Mehmet Halis ÖZER
Prof. Dr. Nihat AYDENİZ

Bu çalışmamın amacı, Türkiye'de siber güvenlik politikalarının güvenlikleştirme ve risk algısı üzerindeki etkisini araştırmaktır. Sosyal Medya ve İnternet, yeni arkadaşlarla tanışmak ve bilgiye ulaşmakta faydaları olmuştur. Ancak bilinçli kullanılırsa teknolojinin faydaları olabilir. Özellikle Çocuklarımızın ve gençlerin internet bağımlılığı konusunda bilinçlenmesi gerekmektedir. Hem devlet hem özel sektör, izleme ve gözetleme araçlarının kullanımını arttırmaktadır. Elektronik iletişimin izlenmesi, elektronik kimlik tespiti, e-imza, e-devlet, kamusal alanda olan kamera sistemleri gibi teknolojiler gündelik hayatımızda olağan karşılanmaktadır. İnternet yoluyla gerçekleşen insan hakları ihlalleri internetin gelişimi ile birlikte artmıştır. Bu ihlallerin toplum üzerindeki etkisi olmaktadır. Siber zorbalık, internette çocuk istismarı, yetkisiz erişim, özel hayatın gizliliğini ihlal, banka bilgilerinin ele geçirilmesi ve diğer siber suçlar internet yoluyla gerçekleşen insan hakları ihlalleridir. Siber zorbalık vakalarında öğretmenlere, okul yöneticilerine ve ailelere önemli görevler düşmektedir. Siber zorbalık ve siber suçların caydırıcı olabilmesi için ciddi hukuki düzenlemelere ihtiyaç duyulmaktadır. İnternet yoluyla işlenen İnsan hakları ihlallerinin olmaması için hem kamu sektörü hem özel sektöre önemli görevler düşmektedir. Çalışmamdan çıkan sonuç: Siber güvenliği sağlamada herkese görevler düşmektedir.

Anahtar Kelimeler: İnternet Bağımlılığı, Siber Güvenlik, Siber Hukuk, Siber Zorbalık.

ABSTRACT

MS THESIS

THE IMPACTS OF NEW THREAT PERCEPTİONS ON TURKEY'S SECURITY POLICIES IN THE CONTEXT OF CYBER SECURITY

Ozan Zeki KİRAZ

INSTITUTE OF SOCIAL SCIENCES OF BATMAN UNIVERSITY
DEPARTMENT OF POLİTİCAL SCİENCE AND İNTERNATİONAL RELATİONS

Advisor: Doc. Murat CİHANGİR

2020, 118 Pages

Jury
Dr. Murat CİHANGİR
Dr. Sadullah ÖZEL
Assoc. Dr. Mehmet Halis ÖZER
Prof. Dr. Nihat AYDENİZ

The aim of this study is to investigate the impact of securitization and risk perception of cyber security policy in Turkey. Social Media and internet have been helpful in meeting new friends and accessing information. Only if it is used consciously can be benefits of the technology. Especially children and young people need to be conscious about internet addiction. Both the government and the private sector increase the use of monitoring and surveillance tools. Technologies such as electronic communication monitoring, electronic identification, e-signature, e-government, and camera systems in public space are considered as normal in our daily lives. Human rights violations through the internet have increased with the development of the internet. These violations have a great impact on society. Cyberbullying, child abuse on the internet, unauthorized access, violation of privacy, seizure of bank information, and other cybercrime are human rights violations through the internet. In cases of cyber bullying, teachers, school administrators and families have important duties. Serious legal arrangements are needed to deter cyber bullying and cybercrime. In order to prevent human rights violations committed through the internet, both public and private sectors have important duties. The result of my work: In providing cyber security, everyone has a duty.

Keywords: İnternet Addiction, Cyber Bullying, Cyber Law, Cyber Security.

1.GİRİŞ

Teknoloji ve internetin gelişimi ile etkileşimlerin boyutu da değişmiştir. İletişim kanallarının tarihsel olarak gelişimi insanlığı geliştirmiş ve dönüştürmüştür. Siber Dünya da milyonlarca kullanıcının olması ve anlık etkileşim ulus devletlerde halklar üzerinde kontrolü kaybetme endişesine sevk etmiştir. Siber uzayda sadece disiplinler arası çalışma yapmakla kalmayıp küresel çapta bir bakış açısıyla çalışma yapmayı da gerekli kılmaktadır. Özellikle karar alıcılar, yöneticiler ve tüm bireyler bu küresel doğanın parçası olup birbirlerine network ağlarıyla bağlıdırlar.

Teknolojinin gelişimi ile insanlık hem olumlu hem olumsuz olarak bundan etkilenmiştir. Olumlu anlamda etkileşim hızlanmış ve yeni mecralarda yeni iletişim biçimleri türemiştir. Örneğin sosyal medyanın yeni arkadaşlarla tanışmak ve bilgiye ulaşmakta birçok faydası olmuştur. Özellikle kamuoyu oluşturma veya lobicilik yapma anlamında sosyal medyada algı oluşumu çok sık karşılaşılan durumdur. Bu olumlu anlamda etkiye örnek iken olumsuz etkiye örnek verilecekse; provokasyon ve tahrik yapılması yanında dezenformasyon yani yanlış bilgi yaymak veya gerçek bir bilgiyi çarpıtmak da teknolojinin gelişimi ile birlikte kolaylıkla uygulanabilen ve çok sık karşılaşılan bir durumdur.

Sosyal medyanın gücünün tartışılmaz olduğu günümüzde siber güvenliğe ve siber faaliyetlere yeterince önem verilmemektedir. Sosyal medyaya yansıyan olayların kitleleri harekete geçirme gücü hafife alınacak bir konu değildir. Sosyal medyada kamuoyu oluşturmak ve kamuoyu neticesinde olmayacak konuların hızlı bir şekilde yapıldığını görmek çok sık karşılaşılan bir durumdur. Bu sebeple sosyal medyada algı oluşturmak veya bir siber saldırı ile kişileri veya kurumları psikolojik olarak zedelemek mümkündür. Özellikle bunu bir siber saldırı yaparak birçok kişi ve durumu etkileyerek yapmak mümkündür. Bir kişi veya kurumu karalayıcı propaganda yapılarak takipçileri ve taraftarlarından olabileceği gibi gizli bilgi belgelere erişilerek ifşa veya şantaj yapılarak gündemde sansasyonel olay yapılabilmektedir. Bir siber saldırının ekonomik kazanç elde amacı olabileceği gibi siyasi bir amaç güderek saldırılar da yapılabilmektedir. Hangi amaç için yapılsın etkileri büyük olabilmektedir.

Günlük hayatta çok karşılaşılan kamuoyu kavramı çok sık kullanılmaktadır. "Kamu" (public) terimi ile grupları ve toplulukları ifade ederken, "oy" terimi ile anlaşılması gereken belirli bir eğilim ve kanaati ifade etmektedir. Genel olarak kamuoyu, belirli bir sorun

karşısında bu sorunla ilgili olan kişiler grubunun veya gruplarının kanaatleri veya görüşlerini ifade eder (Kapani, 2008: 160-161).

Sosyal Medyada da belli bir düşünce ve tutumun kamuoyu oluşturularak yaygınlaşmakta olduğunu veya yaygınlaştırılmaya çalışıldığı görülebilmektedir. Özellikle tweeter kullanıcılarının konu başlığı olarak adlandırılan "hashtag" oluşturulması ve bu konu üzerinde belirli bir eğilim ve kanaat oluşturacak şekilde paylaşım yapması çok yoğun olarak kullanılmaktadır. Bu sosyal medyanın gücü kitleleri ve toplumu yönlendirmede anlık ve güçlü bir etkiye sahiptir. Bu lobicilik faaliyeti gibi bir baskı grubu olmuştur.

Özellikle siyasi liderler başta olmak üzere politik aktörler sosyal medya aracılığı ile dinleyici hedeflerine kolay şekilde ulaşması ve maksimum fayda ile yararlanmaya çalışmaktadırlar. Siyasi kurum ve liderleri; kampanyalarını, pazarlayacakları argümanlarını, kamu diplomasisi ve halkla ilişkilerini en hızlı ve ekonomik olarak sosyal medya araçları sayesinde sağlayabilmektedirler (Cihangir, 2020: 194).

Sosyal medyanın geniş kitleleri etkilediği bir gerçeklik olup bu etkilerin politik boyutlarının olduğu da kaçınılmazdır. Bu etkinin dönüştürücü ve değiştirici tarafları vardır. Sosyal medyanın değiştirici gücünü Murse 10 temel başlıkta açıklamıştır:

1. Seçmenler ile doğrudan iletişim
2. Reklam için para vermeden reklam yapmak
3. Kampanyaların viralleştirilmesi
4. Mesajların dinleyiciye uyumlaştırılması
5. Bağış katkısı
6. Tartışma
7. Geri Bildirim
8. Kamuoyu tartışması
9. Moda olması/ Modaya uygun olması
10. Çoğunluğun-herkesin gücü olması (Murse,2019).

Günümüzde baskı grupları da önem kazanmıştır. Genel olarak faaliyetleri doğrudan doğruya ve dolaylı olarak ayrılabilir. Doğrudan doğruya etkilemenin tezahürü "Lobicilik" (Lobbying) olarak görülmektedir. İngilizce "Lobbying" kelimesinden gelen ve hol, koridor anlamında olup dilimize "kulisçilik" olarak çevrilir. Siyasal karar organlarını etkilemekle

birlikte çıkması istenen kanunu çıkarmak veya çıkacak kanunu engellemek için faaliyeti ifade eder (Kapani, 2008: 224-225).

ABD yasama sistemi içinde çeşitli baskı gruplarınca bir kararın alınması veya alınmaması için yapılan faaliyetler için kullanılan lobicilik terimi, günümüzde başka ülkelerde kullanılan benzer faaliyetler için kullanılmaktadır (Arıboğan &Ayman& Dedeoğlu, 2005: 449).

Devletlerin dış politikalarında uluslararası propaganda çok önem kazanmıştır. Asıl olarak Birinci Dünya Savaşı sonrasında yoğun olarak kullanılsa da iletişim teknolojisindeki gelişmeler propaganda kullanımını kolaylaştırıp yaygınlaştırmıştır. Propaganda, belli bir grubun duygu, düşünce veya siyasetini etkilemeye yönelik tasarlanan ve üretilen faaliyetler bütünü olarak tanımlanır. Diplomatik faaliyetlerin uzantısı olarak kullanılmakla birlikte devletin dış politikasının etkinliğini arttırmaya çalışır (Arıboğan &Ayman& Dedeoğlu, 2005: 676-677).

Sosyal medyanın kitleler üzerinde etkisi günümüzde bilinen bir gerçektir. ABD'de Wall Street'i işgal et hareketi hızla yayılan halk hareketinin en bilinen örneğidir. Bu önemli halk hareketi Amerika da gerçekleşmiş olan 1968 hareketlerinden sonra en önemli ve dikkat çeken politik olay olmuştur. Amerika'nın zengin sınıfına karşı yapılan fakir ve çoğunluğu genç insandan oluşan eylemler yapılmıştı. Ayrıca Ortadoğu da diktatörlere karşı ayaklanma hareketi olan Arap Baharı süreci ve Türkiye'de ortaya çıkmış olan Gezi Parkı Eylemleri sosyal medyanın kitleler üzerindeki etkisini ve gücünü göstermiştir (Eren & Aydın, 2014: 199-200).

Türkiye'nin güvenlik politikaları ve aldığı kararlar incelenecek olursa siber güvenliğe ve önemine yer verilmekle birlikte bunun yeterli olup olmadığı tartışmalı bir konudur. Özellikle diğer ülkeler incelendiğinde ya adımların yetersiz olduğu ya da alınmış olan önlemlerin ilan edilmemesi ve haberleştirilmediği için bilinmiyor olması sebepleriyle siber güvenlik anlamında neler yapıldığı şeffaf bir şekilde bilinmemektedir. Özellikle siber güvenliğin emniyet, askeri ve güvenlik güçlerinin tek elinde olması çıkarılmalıdır. Siber güvenliğin tam anlamıyla sağlanması için; siber saldırılara karşı etkin tedbir alınması, kurumların sosyal medyada yaratılan algı operasyonlarına karşı duyarlı olması, siber güvenlik farkındalığının geliştirilmesi, siber güvenliği sağlamada birimler arası koordinasyon ve

işbirliğinin arttırılmaya çalışılması, siber altyapıların gelişimi için hem teknik hem de siyasi kararlılığın olması gerekmektedir.

Çalışmanın Konusu

Bu çalışmanın temel konusu, siber güvenliğin sağlanması açısından yeni tehdit algılamalarının Türkiye'nin güvenlik politikalarına etkilerini incelemektir. Böyle bir konunun seçilmesinin nedeni ise teknolojinin insan ve toplum yaşamının merkezine yerleşmiş hale gelmesi ve bu yeni ilişki biçimlerine karşılık bilimsel incelemelerin istenilen seviyede bulunmamasıdır. Türkiye'nin güvenlik politikalarında siber güvenliğe ve teknolojiye ne kadar önem verdiği araştırılması için bu konu seçilmiş olup siber güvenliğin, siber saldırıların ve siber hukukun durumu bölümler dâhilinde araştırılıp sunulmuştur. Araştırmalarda sadece Türkiye değil Dünyadan da örnekler verilmiştir.

Bu konunun seçilmesinin başka bir sebebi de siber güvenlik alanında yapılan bu çalışmanın sosyal bilimler alanındaki literatüre katkı sunması ve bu konunun sosyal bilimler alanındaki çalışmaların arttırılması gerektiği yönündeki kanaattir.

Çalışmadaki Amaç

Bu çalışmanın temel amacı, siber güvenlik açısından yeni tehdit algılarının Türkiye'nin güvenlik politikalarına etkilerini incelemektir. Bu sebeple siber güvenlik politikalarının güvenlik anlamında risk olarak algılanıp algılanmadığı araştırılmak istenilmiştir. Siber güvenliğin uluslararası güvenlik içindeki yeri ve önemi araştırılmış olup siber suçların insan haklarını ihlal etmemesi için herkese görevler düştüğü anlaşılmıştır.

Çalışmanın Sınırlılıkları

Bu çalışma siber güvenlik alanında farkındalık algısı anlamında ölçüm yapmayı amaçlamıştır. Bu ölçümü yaparken belli bir kesim veya kişiler merkez alınarak yapılmamıştır. Örnek vermek gerekirse son bölümde anket yapılmıştır ve bu anket internet ortamında Google Docs- Google Formlar üzerinde anket oluşturulup paylaşım yoluyla kişilere ulaştırılmıştır. Anket cevapları sırasında isim-soy isim alınmamış olup katılımcıların etki altında kalmadan rahat bir şekilde cevaplamaları istenilmiştir. Anket sorularının cevapları analiz edilerek yorumlanmaya çalışılmıştır. Çalışmada teori düzlemde bireysel, kurumsal, ulus devletler ve uluslararası sistem bağlamlarında incelemelerde bulunulmuştur.

Çalışmanın Yararı

Bu çalışma, siber güvenliğe verilen değerin ve önemin artması için pozitif bir yararı olduğu söylenebilir. Çünkü siber güvenliğe verilen değeri yetersiz görüp ilgili kişilere, kurum ve kuruluşlara uyarı mahiyetinde bilgiler sunmuştur. Özellikle teknolojinin gelişmesiyle yeni tehdit algıları ortaya çıkmış olup bu tehdit algılarının siber güvenlik anlamında Türkiye'nin güvenlik konsepti veya güvenlik politikalarında sonuç doğurarak etkileyip etkilemediği araştırılmıştır. Bu etkinin yeterli düzeyde olmadığı vurgulanmış ve daha etkili politikaların, farkındalık projelerinin ve somut adımların ihtiyaç olduğu sonucuna varılarak uyarılarda bulunulmuştur.

Çalışmadaki Varsayım

Bu çalışmadaki hipotez, Türkiye'de siber güvenliğin ve siber farkındalığın yeterli olmadığıdır. Siber güvenliğe gereken önemin verilmediği sonucunu varsaymaktadır.

Çalışmanın Sorusu

Türkiye'de güvenlik politikaları oluşturulurken siber tehditlerin bir güvenlik meselesi olarak algılanıp algılanmadığı meselesi sorusu tartışılmıştır. Siber güvenlik konusu ne derecede politikaların oluşumunda etkilidir konusu irdelenmiştir.

Çalışmanın Akışı

Siber güvenlik bağlamında yeni tehdit algılamalarının Türkiye'nin güvenlik politikalarına etkileri konulu olan bu çalışma; beş ana bölüme ayrılarak incelenmiştir. İlk olarak giriş ile başlanarak çalışmanın tanıtımı yapılmıştır. İkinci bölüm, kavramsal olarak "siber güvenlik" kavramı ve "siber uzay" kavramlarının incelenmesi ile başlanmış olup uluslararası ilişkiler teorilerinin güvenlik yaklaşımları ile devam ederek uluslararası güvenlik içindeki siber güvenliğin durumu ulusal ve uluslararası boyutlarda incelenmiştir. Üçüncü bölümde siber suçların hukuki boyutları incelenmiş siber zorbalık konusu irdelenmiştir. Dördüncü bölümde siber saldırılar incelenmiştir. Siber saldırıları araştırıp incelenmesinde mantık ise siber saldırılara karşı güvenliği sağlamak için öncelikle siber saldırının anatomisinin bilinmesi gerekmekte olduğudur. Saldırı bilinmesi gerekir ki önlem ve tedbirler alınabilsin. Buradan da saldırılara karşı savunma gücü arttırılması için teknik olarak hazır olunmasının şart olduğu sonucu çıkmıştır.

Beşinci ve son bölümde anket çalışması yapılarak siber güvenlik alanında farkındalık algısı anlamında ölçüm yapmayı amaçlamıştır. Anket araştırması sonucunda günümüzde ciddi bir oranda siber suça veya siber zorbalığa maruz kalındığı, siber güvenliği ve siber farkındalığın yeterli olmadığı, çok büyük bir oranda cep telefon ve bilgisayarlarında bir önlem olmadan kullanan kişilerin olması ve bu sebeple bu alanın istismara açıklığını göz önüne sermiştir. Özellikle ankette katılımcıların çok büyük bir oranında çocuklarına eğitim verilmemiş olması bu alana verilen önemin eksikliğini gözler önüne sermiştir. En önemli bulgulardan biri ankete katılımcıların siber suçla karşılaştıklarında yeterli farkındalığa sahip mi ve suça maruz kaldıklarında ne yapacaklarını bilip bilmedikleri sorulduğunda ne yapacaklarını bilmeyenlerin oranının yüksek çıkması dikkat çekicidir.

Çalışmada akıcı bir dil kullanılmaya özen gösterilmiş olup yoğun ve ağır teknik anlatımdan kaçınılmıştır.

2. KAVRAMSAL ÇERÇEVE

2.1. Siber Güvenlik Kavramı

Siber güvenlik (cyber security), genel hatları ile siber alanda olan bilginin
1.mahremiyetinin (confidentiality),
2.bütünlüğünün (integrity),
3.ulaşılabilirliğinin (availability) korunması şeklinde tanımlanabilmektedir(Güvenlik Terimleri Sözlüğü, 2017: 621).

Günümüze kadar siber güvenlik genellikle teknik sorunların ve aksaklıkların giderilmesi olarak anlaşıldı. Ancak siber güvenlik ile sadece teknik sorunlar değil insan hatası veya kullanıcı müdahalesi sonucu problemlerin giderilmesini de içermektedir. Hem teknik hem sosyal boyutuyla değerlendirilmesi gerektiğinden de disiplinler arası bir işbirliği zorunlu hale gelmektedir. Siber güvenliğin üç ana hedefi bulunmaktadır: Bilginin gizliliği, bütünlüğü ve erişilebilirliğini korumaktır. Bilgiye kim ulaşabilecek, kim değiştirebilecek ve kim istediği zaman erişebilecek sorularına cevap aranmaktadır (Akyeşilmen,2018:13-14).

Siber güvenlik, bir bilişim sistemi kullanarak sağlıklı bir iletişim kurulması ve bu iletişimin içeriği de dâhil olmak üzere güvenliğini kapsamaktadır. Daha detaylı olursa sadece iletişimin sağlıklı ve güvenli olması değil, iletişimin içeriğinin ses, mesaj vs. ne ile iletişim kuruluyorsa üçüncü kişilere karşı güvenliğini de içerir. Verilerin bütünlüğü, gizliliği, saklanması, paylaşılacaksa ulaşacağı kanallar günümüzde önemli hale gelmiştir.

Dijital dünyanın büyümesi sonrasında kamu-özel fark etmeksizin elektronik işlem hacmini arttırmıştır. Uzun süredir siber güvenlik alanına yatırım yapan ülkeler siber tehditlerden ve siber saldırılara müdahale kapasiteleri açısından her zaman önde olacaklardır. Siber saldırılar karşısında önlem almayan veya dijitalleşen dünyada siber yatırım yapmayan ülkeler kaybeden taraf olacaklardır.

Siber güvenlik alanında da yerli ve milli ürün ve cihazların geliştirilmesi, siber güvenlikte bulunan çözümlerin güvenilirliği adına büyük önem taşımaktadır. Yurt dışından alınan ürünlerin, cihazların ve programların istismar edilme olasılığı veya güvenilirliği tartışmalı olmakla birlikte ekonomik olarak külfiyet getirmektedir. Oysa yerli ürünlerin, cihazların ve programların yapılması hem ekonomik hem güvenilirlik açısından yararlı olacaktır.

Siber güvenlik günümüzde tek bir ürün veya tek bir kurum aracılığıyla sağlanması imkânsız gibi görünmektedir. Bu sebeple Savunma Sanayi Bakanlığı, Emniyet ve Türk Silahlı Kuvvetlerin ilgili Siber Başkanlıkları, Bilgi Teknolojileri Kurumu ve ilgili birimlerin koordineli olacak şekilde çalışmaları gerekmektedir. Yapay zekâ, robot teknolojileri ve büyük data (veri) teknolojilerinde bilgi paylaşımı ve ortak plan ve programlara olan ihtiyaç geçen zamandan daha çok artmıştır.

Havacılık sektöründe gelişen İHA ve/veya SİHA araçları ile başarılı sonuç alındıysa; Uydu teknolojileri, siber güvenlik, yazılım ve simülasyon alanlarında da yerli teknolojilerin ve bunların yerli ürünlerinin gelişimine ihtiyaç vardır. Bunun için de yeterli insan kaynağının da yetiştirilmesi ve mümkünse ilkokul veya ortaokul çağından itibaren eğitim verilmesi gerekmektedir. Sadece devletin değil özel teşebbüs ve firmalarında doğmasına izin verilmeli ve dünyadaki rekabete katılması gerekmektedir. Özellikle Türk firmaların öncelikle Asya, Afrika, Balkanlar ve Orta Doğuda yarışabilir olması sağlanmalı, daha sonra da sektörün büyük devletlerin firmasıyla rekabet edebilir olması gerekmektedir.

2.2. Siber Uzayın Tanımlanması

İnsanoğlunun tarihsel gelişimini bakacak olursak avcı toplayıcılıktan yerleşikliğe geçip tarım çağına geçmiştir. Tarım çağı sonrası sanayi çağına geçen insanoğlu günümüzde bilimin ve teknolojinin gelişimi ile birlikte bilgi çağına geçmiştir. Bu bilgi ve teknoloji çağında bilgiye ulaşma ve bilgi edinme hızı artmıştır. Siber saldırılara karşı savunmanın iyi olması gerekmektedir. Bunun için de araştırma ve bilgi edinme ayrı bir öneme sahiptir. İçinde bulunduğumuz çağa "Dijital Çağ" veya "Bilgi Çağı" olarak adlandırmalar çok sık karşılaşılan durumdur. 21. yüzyıl beraberinde teknolojik gelişmeleri beraberinde getirmiştir. Bilimin ilerlemesiyle teknoloji gelişmiştir.

İnternet sadece dijital bir dünyayı ifade etse de siber uzay ifadesinin altında insan olmaktadır ve insanı kapsamaktadır. Siber uzayın yapısı gereği sistemi ve teknolojisi insan ürünü ve insan yapımıdır (Akyeşilmen,2018: 53).

Siber Uzay oluşumunu fiziksel alandan sanal alana yaklaştıran katmanlardan biri olan kodlar katmanı ile gerçekleşmektedir. Fiziksel katman unsurları olan ana kartlar, işlemciler,

RAM'ler kodlar ile kullanılır hale gelmektedir. "Doğru-Yanlış" ve ya "1-0" olacak şekilde programlama dilleri vasıtasıyla işlemcinin nasıl çalıştırılacağı belirlenir (Bıçakçı, 2014: 108).

Siber uzay sadece sanal bir yapıyı değil fiziki ve sosyal boyutları barındıran bir alandır. Siber uzayda asıl olarak dört ana bileşen bulunmaktadır. Bunların neler olduğuna önem sırasına göre bakıldığında öncelikle kullanıcı yani insan gelmektedir. İkinci olarak dijital olarak depolanan, değiştirilen, kullanılan yazılar, resimler, videolar, tablolar ve diğer ürünleri içeren Bilgi'dir. Üçüncü olarak dijital işleri ve işlemleri mümkün kılan kodlar, programlar ve protokollerden oluşan software yani yazılım olarak adlandırılan mantıksal çerçevedir. Son olarak ise donanım yani hardware denilen fiziksel alt yapılardır (fiziksel alt yapı ile bilgisayarları, kabloları, hizmet sağlayıcılar dâhil olmak üzere tüm küresel ağları da kastedilmektedir). Siber uzay denildiğinde insanı, bilgiyi, yazılım ve donanımı birlikte düşünülmesi ve değerlendirilmesi gerekmektedir (Akyeşilmen, 2018: 12-13).

Siber uzay tıpkı fiziksel uzay gibi derinliği ve boyutu bilinememektedir. Diğer taraftan siber uzay aynı fiziksel uzay gibi sürekli genişlemekte ve büyümektedir. Buna bir örnek verecek olursak her saniye, dakika, gün ve zaman insanlar internet âlemine yapmış olduğu veya çoğalttığı resim, video, yazı, ses veya her türlü bilgi yükleyerek siber uzayın genişlemesi ve büyümesine katkı sağlamaktadır.

Siber güvenliğin ve siber alanın son yıllarda gelişmesine rağmen hala işin başında olduğu bir gerçekliktir. Bunun siber uzayın doğası gereği sürekli gelişen teknolojinin olması kadar siber ile ilgili durumların tanımlanmasının ve kavramsallaşmanın güçlüğü de etkilidir. Siber uzay interaktif bir alan olup kullanıcılar ondan yararlanmakla birlikte ona katkı da sağlamaktadır. Bu sebeple siber uzay ile ilgili kavramlar ve literatür sürekli değişmekte ve gelişmektedir.

İnternet günlük hayatımızda önemli bir yer tuttuğundan beri tüm işlerimizi ve işlemlerimizi onunla yapar hale geldik. İhtiyaçtan bir tehdit haline geldiği tartışılır oldu. Bu sebeple internetin dengesi kurulamazsa insanlığın cehennemi haline de gelebilir. İşte bu sürekli büyüyüp gelişen internet dünyasına, fiziksel uzayın büyüyüp gelişmesi gibi, siber uzay denilmektedir.

Siber uzay; kullanıcılardan, yazılımlardan, küresel ağlardan oluşan ve elektronik veri kaynaklı sanal bir dünyadır. Şeffaf bir alan olsa da sırları içerisinde barındırmaktadır. Bilinmezlikler ve muğlaklıklar çok fazladır. Bu nedenle tehlikeli ve riskli olup yönetilmesi ve kontrolü zordur (Akyeşilmen, 2018: 58).

Dijital çağ özellikle teknolojinin gelişimi ile birlikte çok sık kullanılmaya başlanmıştır. Dijitalleşme, Dijitalleşen dünya, dijital kütüphane, dijital gazete gibi birçok alanda kullanıldığını ve birçok alanı etkilediği görülmektedir.

Dijital çağ ile kast edilenin veri odaklı ve bire bir ilişkinin ön planda olduğu dönemi ifade eder. Dijital öncesi kitlesel medya odaklı olup post-dijital çağ veya sibernetik çağ ile ise birden anlara ve olana odaklanacağımız dönemi ifade eder (Çetin, 2018: 32).

Dijital öncesi çağda gazete kültürü hâkimdi. Bir mesaj gazeteye basılarak milyonlarca kişiye iletilebiliyordu. Dijital çağda bir mesaj anında milyonlarca kişiye iletilebilmektedir. Artık post-dijital çağ veya sibernetik çağ literatürde geçmekte ve anlık olarak olaylar insandan bağımsız olarak değişebilmekte ve bu olayların takibine odaklanma konusu hâkimdir. Sibernetik, insani müdahale gerekmeksizin dış dünyada kaynaklanan ihtiyaçlara ve olaylara karşı kendini düzenleyebilen sistemleri araştıran ve incelemekte olduğu bir bilim dalıdır (Çetin, 2018:38).

Günümüzde teknolojinin ileri boyuta ulaşmasının sonucu olarak yapay zekâ konuşulmakta, robotların kendi otokontrollerini sağlaması ve insansız araçlar geliştirilmeye çalışılmaktadır. Teknolojinin gelişmesi insan haklarını olumlu anlamda geliştirmesi beklenir. Çünkü teknoloji insanlığın refahını ve yaşam standardını arttırmaktadır. Ancak insana güvenin kalmaması ve her işi robotlara yaptırmanın insanı küçük düşürme yanı göz ardı edilmemelidir. İnsanın hata yapabilen yanı artık hatasız iş yapabilen makinelere yeni robotlara tercih edilmektedir.

2.3: Siber Uzaya ve Siber Güvenliğe Kuramsal Yaklaşımlar Var mıdır?

Uluslararası ilişkiler teorilerinin güvenlik yaklaşımları genel itibari ile incelenecek olursa siber uzay ve siber güvenlik anlayışları da anlaşılabilir. Siber ile sosyal bilimler arasında olan ilişki genellikle sorunlu olmuştur. Bunda sosyal bilimcilerin uzun zaman siber çalışmaları göz ardı etmelerinin yeri büyüktür. Siber alanı daha çok teknik bir disiplin olarak

yorumlayıp kodlar, programlar ve yazılımlardan ibaret sanmışlardır. Siber alanın sosyal, ekonomik ve hatta siyasal boyutu olduğunu yakın bir zamana kadar sosyal bilimciler tarafından fark edilememiştir.

İdealizmin temellerinde Hugo Grotius, Immanuel Kant, John Lock, Jeremy Bentham, John Stuart Mill gibi düşünürler tarafından atılmış olup Birinci Dünya Savaşı sırasında Woodrow Wilson önderliğinde savaş sonrası düzenin akılcı şekilde düzenlenmesi ve uluslararası kurumsallaşmaya öncülük etmiştir. Burada "kolektif savunma" yerine "kolektif güvenliğe" vurgu yapılarak eski tarihlerdeki güç dengesi yaklaşımı ortadan kaldırıp barışçıl bir dünya düzeni kurulmasına öncülük etmiştir. İdealizme göre insan doğası iyi olup yardıma ve iş birliğine yatkındır. Doğru bir hukuksal düzenleme yapılırsa insanın kötü ve çatışmacı kimliği kalkacaktır. Uluslararası kaosun kaldırılıp güvenliğin sağlanmasının en etkili ve yararlı yolu, uluslararası hukuku tesis etmek ve uluslararası örgütler kurmaktır (Karabulut, 2015: 52-54).

Realizmin temelleri incelendiğinde Yunanlı tarihçi Thucydides'in Peloponnesiya Savaşlarının Tarihi (M.Ö 431) isimli eserine kadar uzanmaktadır. Realist yaklaşımın önemli kaynaklardan kabul edilip Yunan şehir devletleri arasında olan "göreceli güç" (relative power) kavramına önem vermiştir. Atina'nın güçlenmesinin Sparta'da yaratmış olduğu güvenlik kaygısına yol açmıştı. Bir başka realizmin temellerini atan düşünür olan Niccola Machiavelli'nin Prens adlı eserinin katkısı da unutulmamalıdır. İtalyan prenslerin iktidarda kalma savaşı ve savaşa önem vermeleri gerektiği ileri sürülmüştür. Machiavelli'ye göre siyasal hareketler "güç politikası (power politics)" dır (Karabulut, 2015: 55-56).

Realist düşünürlere göre güç ve güvenlik arasında doğrusal ve paralel bir ilişki vardır. Bunun anlamı ne kadar güç elde edilirse veya güç biriktirilirse o kadar güvenlik elde edilecektir. Bu güç birikiminin temel amacı barışı sağlamlaştırmaktır.

Neorealist güvenlik anlayışına bakıldığında Kenneth Waltz'ın analizlerine bakılması gerekir. Waltz, devletlerin uluslararası politikada esas aktör olduğunu kabul etmekle birlikte sistem olarak analiz yapmaya çalışmıştır. Uluslararası siyasi yapıyı incelemiştir. Waltz, analiz düzeylerinin ilişkisi yerine uluslararası sistemin yapısal bileşeninin nasıl olduğuna odaklanır. Güç dengesinin düzen anarşik olursa ve varlığını sürdürmek isteyen birimler olursa geçerli

olacağını savunur. Bu sebeple iki kutuplu düzenin üç ve daha fazla kutuplu düzenden daha istikrarlı olduğunu savunur (Griffiths & Roach &Solomon, 2011: 58-60).

Soğuk Savaş sonrası uluslararası ilişkiler teorilerinin düşünüş şekli ve özet mahiyetinde aşağıdaki tablo incelenebilir:

Siyasal Düşünce Yapıları	**Birincil Analiz Düzeyi**	**Birincil Analiz Seviyesi**	**(Anahtar) Açıklayıcı Unsurlar**	**(Esas) Konu veya Odak**	**İdeolojik Gelenek**
Realizm (Gerçekçilik)	İnsan grupları	Gruplar arası/ Devletlerarası seviye, düzey	Askeri güç/ kudret dengesi	Çatışma, anarşi ortamında düzen	Muhafazakârlık
Rasyonalizm (Akılcılık)	Rasyonel aktörler	Bireysel (Bireylerarası) düzey	Müzakere, uzlaşma, çıkarlar	Rasyonel iş birliği	Liberalizm
Revolüsyonizm (Devrimcilik)	Kapitalist dünya sistemi	Dünya sistemleri düzeyi	Yapısal güç, baskı işletme	İktisadi gelişme, siyasi bağımsızlık	Radikalizm

Tablo 2.1: Uluslararası İlişkilere dair üç önemli paradigma. (Knutsen, 2006: 342).

Soğuk savaş sonrası güvenliğe genel olarak bakış açılarında değişiklikler olmuştur. İdealizmin "barışı tesis etme" bakış açısı, realizmin "güç" temelli bakış ve neoralizmin "anarşik güç dengesi" merkezli bakış açıları eleştirilmeye başlanmış ve günümüz dünyasını açıklamada yetersiz kalmıştır. Geleneksel güvenlik anlayışları tam anlamıyla reddedilemez ancak yeni bir bakış açısına temel olarak yeniden düşünmeye ve tartışmaya zemin hazırlar.

Uluslararası ilişkiler alanında güvenlik çalışmalarında realist yaklaşımlarda savaşlar doğal bir olgu olup devletler kendi güvenliklerini sağlamayı amaç edinirler. Realistler devleti temel alan bir güvenlik anlayışına sahip olup güvenlik kavramını "sürekli bir güvensizlik ortamı" olarak tarif etmektedirler. Neorealizme göre devletlerarası işbirliği mümkün olsa bile devletlerarası işbirliği sınırlıdır. Neorealistlere göre güç mücadelesi ve rekabet devam eder. Liberalizm de ise uluslararası kurumlar, çokuluslu şirketleri, sivil toplum kuruluşları önem arz etmekte olup devlet dışı aktörlerin analiz birimi olduğu görülür. Realizmin tersine işbirliği merkezli bir güvenlik anlayışı olan liberalizmde bir ideal ve hedefler, aktörler arası ilişkiler önemlidir (Goyushov, 2019: 696-697).

Geleneksel güvenlik anlayışlarına tepkiler 1970'lerde başlamakla birlikte güvenlik kavramının yeniden sorgulanması gerekliliği ortaya çıktı. Bunun iki önemli nedeni Soğuk Savaşın bitişi ve küreselleşmenin uluslararası ilişkilerin her alanını etkisine almasıdır (Karabulut, 2015: 78-79).

Özellikle 1970'li yıllarda devlet odaklı analiz yapan düşünce okullarına karşı tepki olarak doğan Plüralizm, artan karşılıklı bağımlılık ve karşılıklı etkileşim sebepleriyle geleneksel güvenlik anlayışına tepki olarak çıkmıştı (Arı, 2011: 331).

John J. Burton'un dünya toplumu (world society) yaklaşımınca uluslararası ilişkiler sadece devletlerarası ilişkilerden ibaret değildir. Devletlerarası ilişkiler ekonomik, toplumsal ve siyasi ilişkileri de kapsamaktadır. Burton'a göre uluslararası ilişkilerde iki ayrı model vardır. Bunlar bilardo topu (billiard ball) modeli güç yaklaşımını temel alıp devletleri kapalı bir yapı olarak görürken örümcek ağı(cobweb) gücün göreceli olduğunu ve devlet merkezli olmayan uluslararası iş birliğine, fonksiyonel örgütlenmelere ve karşılıklı iletişime vurgu yapar (Arı, 2011: 331-332).

Barry Buzan, İngiliz Okulu'na ve uluslararası güvenlik çalışmasına katkısı önemlidir. Güvenlikleştirme ile sadece askeri tehditleri ele alan dar bakış aşısıyla değil AIDS ve çevresel konular başta olmak üzere geleneksel olmayan sorunların niçin güvenlik riskini arttırdığını sorgulamıştır. (Griffiths & Roach &Solomon, 2011: 220-221). Güvenlikleştirme eylemi, güvenlikleştirici bir konuyu ele alarak güvenlik tehdidi olarak algılar ve olağan üstü tedbirler alır. Başarılı olan bir güvenlikleştirme ise, hedef kitlenin konuyu tehdit olarak görmesi ve konunun bir güvenlik sorunu olarak kabulüyle mümkündür (Baysal ve Lüleci, 2015: 76). Siber güvenlik pek ala güvenlikleştirilip olağan üstü tedbirler, internette yasaklamalar getirilerek yapılabilir olsa da onun vatandaşlar ve dinleyiciler tarafından bir tehdit olarak algılanması da gerekmektedir.

Güvenlik çalışmalarında Amerikan egemenliğine alternatif Kopenhag Okulu, literatüre "güvenlikleştirme", "güvenlik sektörleri" gibi birçok kavram kazandırmış olup, güvenliği ekonomik, politik, çevresel, toplumsal ve insani güvenlik sektörlerini incelemiştir. Özellikle geleneksel devlet merkezli güvenlik anlayışına eleştiri olarak çıkan Eleştirel güvenlik anlayışı, bireylerin de çalışılması gereken konular olduğunu söyler. Sosyal İnşacı, Feminist ve Post-

modern teorilerde de devlet merkezli güvenlik anlayışına eleştiri vardır (Goyushov, 2019: 697).

Güvenlik teorilerinin tarihine bakıldığında devlet merkezli güvenlik anlayışından bireyi ve kurumları önceleyen güvenlik anlayışlarına doğru bir yol izlemiş olup bunun siber güvenlik anlamında da ayrı bir önemi şüphesiz olacaktır. Günümüzde sadece devletin siber güvenliği değil; kurumların, kuruluşların ve bireylerin siber güvenliği önem kazanmıştır.

Kopenhag Okulu yazarlarına göre "güvenlik" içinde yıkıcı özellikler barındırmaktadır. Özellikle Ole Waever'a göre, amaçlananın "güvenlik-dışılaştırma" olması gerekmektedir. Güvenlik-dışılaştırma ile kastedilen ise konuların "aciliyet" hâlinden çıkması ve siyasi alanda normal görüşmeler düzeyine taşınmasıdır (Baysal ve Lüleci, 2015: 66).

Kopenhag Okulu ekolüne göre güvenlikleştirme kavramı ile değerli sayılan bir şeyin tehdit olarak tanımlanarak inşa edilir ve sonrasında askeri tedbirler başta olmak üzere üst düzey önlemler alınır. Siber güvenliğinde Türkiye için "aciliyet" kapsamına alınıp ciddi tedbirler alınması elzemdir.

Siber güvenliğin güvenlik-dışına ötelemek mi yoksa güvenlikleştirilmesi ve üst düzeye çıkarmak devletlerin politikalarına bağımlı olsa da politika yapıcıların tehdit ve risk algılama düzeylerine göre değişkenlik göstereceği aşikârdır. Ancak günümüzde siber güvenliğin önemli hale gelmesi tartışılmaz bir gerçeklik olup siber alandan ve teknolojik gelişmelerden geri kalınmaması için güvenlik politikalarının yeniden gözden geçirilmesi gerekmektedir.

2.4: Siber Uzayda Çatışma ve Ulus Devletlerin Siber Savaşı

Devletler, siber saldırıları askeri bir çatışmaya gerek olmaksızın kullanılabilecek bir yöntem olarak görebilmektedirler. Siber uzayda saldırganın kimliğinin gizlenebilir oluşu ve siber suçun tespit-isnat (attribution) konusunun karmaşık olması devletlere cazip hale gelebilmektedir (Darıcılı, 2018: 324).

Günümüzde yeni yeni ulus devletlerarasında siber savaş tehdidi algılanmaktadır. Ancak siber savaşlar tarihsel olarak birçok kez yaşanmıştır. Bunlardan bilinen en dikkat çekici olanı casus program olan Promis'tir. Promis konusunu ele alan dosyalarda Dünya Bankası ve IMF'nin, CIA ve Mossad yararına bilgi sızdırdığı ileri sürülmüştür. ABD'nin bu tip program

aracılığıyla hedef ülkelerin banka sistemlerini kilitleme ve kontrollü mali krizlere yol açtığı ileri sürülmüştür (Kuzu, Ağustos 2019:188-189).

Gelecek dönemlerde bilgisayar ağlarına saldırılar, askeri operasyonlar için mühimmatların veya araçların sahaya ulaştırılması kadar önemli hale gelecektir. Askeri operasyonların önemli özelliğinde bilgisayar ağlarına saldırlar ve siber savaş yer alacaktır. 1995 yılında Çin Ordusu finans sistemlerine saldırıyı yararlı bir asimetrik silah olarak değerlendirip 1997 yılında "Bilgisayar Harbi" olarak tatbikatlar yapmıştır (Kuzu, Eylül 2019: 24).

Çinli uzmanlar, bilgisayar virüsleri ile hedef sistemleri izlemek ve yönlendirerek rakip füzelerinin kendine geri döndürerek kullanabileceğini ifade etmişlerdir. Çinli güvenlik uzmanlarınca bir bilgisayardaki bir gram entegre yani bütünleşmiş devre sistemi bir ton uranyumdan daha faydalı olabilmektedir (Kuzu, Eylül 2019: 24).

11 Eylül sonrasında uluslararası arenada en çok konuşulan meselelerden biri NATO üyelerinden bir devlete gerçekleştirilebilecek siber saldırı ve ya "Dijital Felaket" (diğer adı dijital 9/11) senaryosuydu. Muhtemel bir dijital Pearl Harbour beklentisi artmıştı. Devletlerin siber sistemlerine saldırı ile kritik alt yapıları ve ekonomisine ciddi zararlar verilmesi ve bunun güvenliklerini sarsacağı korkusu oluşmuştu. Bu korku sebebiyle birçok ülke ulusal güvenlik belgelerine siber güvenlik stratejilerini eklediler (Bıçakçı, 2014: 119).

Siber terörizmi ciddi tehdit olarak yaşayan en ilginç örneklerden biri Estonya'dır. Soğuk Savaşın sona ermesi ile birlikte Rus kökenli vatandaşlarının artışı ile Ruslarla Estonlar arasında gerginlikler vardı. Rusya kaynaklı internet site ve forumlarında Estonya'daki adresler hedef gösterilmiş ve birçok siber saldırı yapılmıştı. Estonya Savunma Bakanı, NATO teşkilatına ve NATO üyesi ülkelere yardım talebinde bulundu. Uluslararası güvenlik anlamında Estonya'ya yapılan siber saldırılar bir milat olmuştur (Bıçakçı, 2014: 119-121).

2015 tarihinde Rus Hacker grubu olan CyberBerkut, Alman Parlamentosu ve Şansölye olan Angela Merkel'in internet sitelerine saldırılar gerçekleştirmiştir. Siber saldırılar sadece web sayfalarına erişim engeli ile kalmayıp yaklaşık 20.000'i bulan politikacılara, destek personeli ve memurlara ait bilgisayarlara erişim ve veri akışı sağlamıştır (Eren, 2017:62).

Avrupa Birliği'nin siber saldırılar ile siber güvenliğin önemi ile yüzleşmesinde Estonya saldırıları ve Alman Parlamentosuna saldırılar kadar bir başka referans kaynağı TV5 Monde Örneğidir. TV5 Monde siber saldırısını IŞID örgütü üstlenmiş olup kanalın Facebook ve Twitter hesaplarına da saldırı düzenlenmişti. Konu ile ilgili Paris Savcılığı siber saldırılar ile "Terör soruşturması" açıldığını duyurmuştu(www.bbc.com).

2015 yılında Paris'te Fransız dergisi olan Charlie Hebdo'ya gerçekleştirilen silahlı saldırı sonucu 12 kişi yaşamını yitirmiştir. Saldırı sonrası Anti-İslamcı yaklaşımlar sergilenmiştir. Sonrasında radikal İslamcı grup olarak bilinen CyberCaliphate TV5 Monde'ye siber saldırılar gerçekleştirmiştir. Kanal hizmet veremeyecek duruma gelip web ve sosyal medya hesapları ele geçirilmiştir. TV5 Monde örneği devlet dışı aktörlerin de iyi bir şekilde organize olup siber saldırılar yapabileceğini ve özellikle Avrupa Birliği'nin sınırlı yetkilere sahip olduğunu yüzleştirmiştir (Eren, 2017:663-64).

Bireysel hakların sınırları ve meşru hükümet müdahalelerin sınırlanması hakkında uluslararası ve ulusal tartışmalar süregelmiştir. Wikileaks olayı davasında, hassas ve hükümetlerin gizli dokümanlarının yayınlanması ayrıca gizli belgelere erişilmesi sebebiyle ağır bir suç olarak yargılama yapılmıştı. Bazı Avrupalı ülkeler başta olmak üzere Wikileaks internet adresine erişim yasağı getirmiş olsa da bu bilgilere birçok kişi erişebilmiştir (Bendiek, 2012:8).

Avrupa Birliği üye ülkelerde siber güvenlik politikaları minimum düzeyde standartlar getirmiş olsa da haksız yere bireysel hakları ihlale ve demokratik ilkelere aykırı düzenlemelere izin vermemektedir. Birliğe üye devlet önce kendi siber güvenliğini almalı ki Avrupa Birliği siber güvenliğine katkı yapabilsin. Demokratik ilkeler gözetilerek oluşturulan bir siber güvenlik politikaları oluşturulmaya çalışılmakla birlikte Birlik güvenliğine zarar gelmemesi için belirli bir birliktelik sağlaması açısından önemli bir aşama kaydetmiştir. Üye ülkeler hem kendi ulusal düzenlemelerini hem de uluslararası düzenlemeleri yapması gerektiği için çok seviyeli küresel bir politikayı ifade etmektedir. Birliğin içinde özel güvenlik şirketlerinin de bu politikalarda etkin bir olmaya çalıştığı da görülmektedir. Enerji, sağlık, ulaşım şirketlerinin bu yapıda yerini alacağı kuşkusuzdur. Avrupa Birliği siber güvenlik politikaları iyi yönetişim olarak formüle edilen şeffaflık, hukukun uygulanması, sorumluluk ve ortak yönetim ilkeleriyle hareket etmektedir (Bendiek, 2012:5-6).

Günümüzde ulus devletler bilgisayar korsanlığı ve siber güvenliklerini sağlamak amacıyla hackerler yetiştirmekte veya kullanmaktadırlar. Sadece kendi güvenliklerinin sağlanması konusu değil rekabet etme amacıyla da etkinliklerini arttırmaya çalışmaktadırlar.

Dünya da bilinen büyük hackerlarından biri olarak bilinen ve tutuklanmış Kevin Mitnick ABD'de gizli şirket bilgilerini çalmış ve Amerikan Ulusal Güvenlik ağını çökertmiştir. Bir başka hacker Jonathan James daha henüz 16yaşında iken NASA'nın sistemine girmiş ve 1.7 milyon Amerikan doları değerinde program/yazılım indirmiştir. Tüm bu eylemlerin arkasında terörist örgüt veya devlet olmadan gerçekleşse de devletin savunmasına tehdit olmak isteyenler için örnek alınabileceğinden güvenlik anlamında önemlidir (Çakmak & Altunok, 2009: 89).

Rusya, kendi kontrolünde bulunan ancak belirli bir kuruma bağlı olmayan ve bağımsız hacker gruplarının siber güvenlik alanındaki faaliyetleri ve eylemleri desteklemektedir. Rusya siber güvenlik alanında etkili politikalar geliştirmiş ve siber alanda sayılı ülkeler arasına girmiştir. Ayrıca siber güvenlik politikalarını geliştirip yaygınlaştırmasıyla Rusya dış politika çıkarlarında kazançlı çıkmış ve bundan çok yararlanmıştır (Acar ve Pekcandanoğlu, 2020: 166-167).

Rusya siber güvenlik politikalarını 1994 yıllarında gözden geçirme kararı vermiştir. Buna sebep olan olay ise 1994 Rus-Çeçenya arasında geçen savaştır. Çeçenler bu savaşta bilgi teknolojilerini çok iyi kullanmışlardır. Çeçenler kendi self-determinasyon hakkını ilan ederken ve Rusya'nın insan haklarını ihlal ettiğini belgelerle ilan ederken Batı'ya çok iyi propaganda yapmışlardır. Böylece Rusya savaş stratejilerinde büyük değişikliğe gitmiş ve Medya organizasyonlarını, görsel ve yazılı teknolojiyi kontrol altına almaya çalışmıştır (Acar ve Pekcandanoğlu, 2020: 169).

Rusya 2007 Estonya, 2008 Gürcistan ve Litvanya, 2009 Kırgızistan ve 2014 Ukrayna ile olan savaşlarında Siber saldırı kapasitesinin arttığı görüldü. Örneğin Estonya'nın Parlamentosu başta olmak üzere bankaları, siyasi parti siteleri, telekomünikasyon şirketlerinin hacklenmesinde Rus Hackerler başarılı olmuşlardır. Daha sonra Estonya'nın NATO ve ABD'den destek alması ve siber güvenlik önlemlerini alması süreci siber güvenliğin önemini göstermiştir (Acar ve Pekcandanoğlu, 2020: 179-180).

Rusya'nın dış politika problemlerinin çözümünde de siber saldırıları ve sabotajları bir argüman olarak sunması ve masada bir tehdit seçeneği olarak göstermesi yeni tip bir mücadele alanını ortaya çıkarmıştır. Rusya'yı tehdit olarak gören tüm ülkeler Rusya tarafından siber saldırılar düzenlenebileceğine yönelik tehdit algısı algılayıp bu alanda güvenliklerini arttırmaya ve tedbir almaya çalışmışlardır.

NATO Genel Sekreteri Jens Stoltenberg'in 2019 yılında yapmış olduğu açıklama dikkat çekicidir. Açıklamaya göre ittifakın fiziki dünyada olduğu gibi siber dünyada da sürdüğünü ve üye ülkelere yapılacak bir siber saldırının NATO kurucu anlaşmasının 5. Maddesini tetikleyebileceğini belirtmiştir. Özellikle siber dünyanın yeni bir alan olduğu ve yeterli kaynak ve donanımın hazırlanması gerektiği birinci öncelikleri olduğunu belirtmiştir (www.sabah.com.tr). NATO'nun siber saldırıları güvenlikleştirip tehdit boyutunu arttırması NATO kuruluş anlaşmasındaki 5. Madde ile ilişkilendirilmiş olup tehdit algıları yeni bir boyut kazanmıştır.

Siber uzayın karanlık yüzü olarak adlandırılan Deep-weeb kısmında yasadışı faaliyetlerin olduğu sınırsız bir alanı ifade etmektedir. Uyuşturucu ticareti başta olmak üzere insan kaçakçılığı, kiralık katiller, çocuk pornosundan organize suçlara kadar birçok suçun işlendiği ve en az cezalandırıldığı alan olup büyük bir kısmı bitcoin ve sanal paralarla yapılmaktadır. Ulus devletler bunlarla mücadelede de yetersiz kalmaktadır. Uluslararası işbirliğine ihtiyaç duyulduğunda ise devletlerin rekabet algısıyla hareket ettiği görülmektedir.

Kara, deniz, hava ve uzaydan sonra siber savaşı harbin beşinci boyutuna geçilmiştir. Savunma ve radar sistemleri başta olmak üzere, İnsansız hava araçları, internete bağlı veya internete bağlı olmayan kapalı devre sistemlere sahip siber araçlar, füzeler, nükleer sistemler siber savaşların olması durumunda yıkımların ne boyutlarda olabileceği hakkında bilgi verebilmektedir.

Siber terörizm, teknolojinin terörist gruplar tarafından kullanılarak bilgisayar sistemleri ve telekomünikasyon alt yapılarında saldırı düzenlenmesidir. Siber savaş ise ulus devletlerarasında network ve ağ yapılarını zarara sokması veya erişilmez gizli bilgilerine erişilmesi olarak adlandırılabilir (Nandhini & Seemma & Sowmiya, 2018: 125).

Uluslararası ilişkilerde siber suç mu siber terör mü ve ya savaş mı olduğu konusunda kafa karışıklığı olsa de genel hatları ile şöyle bir ayrım ve ana hat bulunmaktadır:

Eylemin	**Siber Suç**	**Siber Terör**	**Siber Savaş**
Niteliği	Doğrudan	Sembolik	-Doğrudan - Sembolik
Şiddeti	Az yoğun	Yoğun	En yoğun
Motivasyonu	Kişisel kazanç	Siyasi	-Siyasi -Doğrudan savaş kabiliyetini azaltmak -Casusluk
Failleri	-Bireyler -Organize suç örgütleri -Anonim	-Terörist örgütler -Hangi örgüt olduğu tahmin edilebilir.	-Failin kim olduğu tam olarak bilinmese de kaynaklandığı devletler bilinir.
Hedefleri	Kazanç sağlanacak hedefler	-Kritik tesisler -Güvenlik birimleri -Hükümet temsilcilikleri	-Kritik tesisler -Ekonomik ve endüstriyel altyapılar -Güvenlik birimleri -Hükümet temsilcilikleri -Askeri altyapılar
Kaynağı	Ülke içinden ya da dışından	Ülke içinden ya da dışından	Ülke dışından

Tablo 2.2: Siber Suç, Siber Terör ve Siber Savaşın Temel Özellikleri (Çakmak & Altunok, 2009: 49).

Yukarıdaki tablodan da anlaşılacağı üzere bazıları benzerlikler içermektedir. Ancak farklılığın motivasyondan kaynaklı olduğu görülecektir. Suç, terörizm ve savaşların amaçları farklı olsa bile siber kelimesi bir sıfat gibi önlerine geldiğinde bu kavramlara yüklediği anlam özünde değişiklik yaratmasa da etkiler açısından asimetriye işaret eder (Çakmak & Altunok, 2009: 49-50).

Teknolojinin gelişmesi her şeyi değiştirmekte ve dönüştürmektedir. Bu değişikliğe ve dönüşüme ayak uydurulması gerekmekte ve takip edilmesi gerekmektedir. Aksi halde takipten düşülürse onarılmaz zararlar ve teknolojik gerilik ile karşılaşılacaktır. Teknoloji ve siber güvenlik literatürü takip edilemezse her türlü siber tehlikelere açık olunacak ve saldırılar kaçınılmaz olacaktır. Özellikle bu saldırıların askeri ve ekonomik sonuçları ağır olacaktır.

2.5: Ulus Devletin Siber Uzay karşısındaki tutumu: Siber Diplomasi ve İşbirliğinin Önemi

Soğuk Savaş döneminde Amerika ile müttefikleri arasında teknoloji kullanımı ve bilgisayar kullanımı artmıştır. Özellikle Avrupa Birliğinin getirmiş olduğu ithalat rejimi kuralları gereği Varşova Paktına üye ülkelere nükleer silahlar sistemlerinde kullanılabileceği gerekçesiyle bilişim sistemleri satılmıyordu. Soğuk Savaşın bitmesi ve yasağın kalkmasıyla birlikte hem internet kullanımında artış oldu hem de ülkeler ekonomik, politik ve askeri alanlarda kullanmaya başlamışlardır (Bıçakçı, 2014: 102-103).

1957 yılında Sovyetler Birliğinin ilk yapay uyduyu dünya yörüngesini yerleştirmesi ile iki kutuplu dünyada rekabet gereği teknolojik rekabet yaşanmıştır. ABD'nin rekabet gücünü desteklemeye yönelik 1958 yılında İleri Araştırma Projeleri Ajansı(ARPA) kurulmuştur. O yıllarda bilgisayar işlemcileri çok sayıda kullanıcının bilgisayara girişini desteklemiyordu. İşlemci teknolojisinin gelişimi ile ve bilim insanlarını tek bir ağda toplamak için 1962 yılında ise İleri Araştırma Projeleri Ajansı Ağı (ARPANET) kurulmuştur. ABD müttefikleri ile ticari ve araştırma amacıyla ARPANET'i paylaşımı ile birlikte uluslararası bilgisayar ağlarının oluşumu gerçekleşmiştir. Soğuk Savaşın sonunda ise kullanıcıların ve tehditlerin artması ile birlikte ABD askeri verilerini taşıyan farklı bir ağ oluşturma kararı vermiştir. Böylece ARPANET ağı sivil araştırmalar için kullanılmaya devam etti ve sivil siber uzayın temeli oldu (Bıçakçı, 2014: 104-106).

Çin ve ABD hackerlarının siber savaşı ve siber yüzleşmesi olarak bilinen ve 'Birinci Siber Dünya Savaşı' olarak adlandırılan 2001 yılındaki saldılar birçok devleti etkilemiştir. ABD keşif ve casus uçağı Çin jeti ile çarpışması sonucu Çin ve ABD hackerları saldırılar düzenlemiştir (Cavelty, 2015: 408).

Günümüzde ulus devletler için siber güvenliğin ve teknolojinin önemi artmıştır. Devletler diğer devletler hakkında istihbarat elde edinirken dahi klasik yöntemlere başvururdu. Günümüzde ise bir teknolojik malzeme veya imkân ile insan dahi olmadan birçok bilgi ve malumat edinilebilmektedir. Buda karşımıza siber espiyonaj kavramını karşımıza çıkarmaktadır.

Siber espiyonaj, gizli bilgi ve belgelere teknolojinin kullanılarak elde edilmesidir. Büyük stratejik, ekonomik, askeri bilgi ve belgelere kötü amaçlı yazılım kullanılması veya teknoloji kullanımı ile elde edilmesidir (Nandhini & Seemma & Sowmiya, 2018: 125).

Devletler kendi çıkarlarını attırmak için komşuları veya rakip devletler hakkında istihbarat toplama veya casusluk faaliyetleri yapmaktadırlar. Bunu yaparken siber casus yazılımların tercih edildiği görülmektedir. Bunun olmasında ki en temel sebepler; yakalanma ve tespitinin zor olması, hızlı sonuç alması, ekonomik olması, iz bırakmaması gibi sebeplerdir.

Günümüzde 'siber caydırıcılık' olarak adlandırılan yaygın bir konsept gelişmiştir. Buna göre saldırının önünü kesmek için hükümet ağları, askeri ve kritik kurumların güvenliğinin sağlam bir kapasitede olmalıdır (Cavelty, 2015: 411).

Gelecekte sosyal medya devriminin etkisi ile bireysel ve toplumsal düzeyde yeni kimlik biçimleri ortaya çıkacaktır. Ulus devletler ve inşasında etkili olan ulusal kimlikler yeni durumdan etkilenmekte olup aynı zamanda da gelişmektedir. Bir başka örnek olarak ulusal kimliğin oluşumunda etkili olan dil dahi etkilenmektedir. Sözcüklerin kısalması veya emoji diye tabir edilen ifadelerin kullanılarak iletişim kurulması gibi trendler gelişecektir. Kimliksel dönüşümler, tarihin dijitalleşmesi ve hızlanması olgusu, sanal veya yeni tekno inanç sistemlerinin ortaya çıkma olasılığı, yeni sosyal kültürün oluşacağı gibi öngörüler yapılabilmektedir (Cihangir, 2020: 193-194).

Dünya politik ve siyasi düzeninde ulus devletlerarasında çekişmelerin önemli bir kısmı siber alanda ve dijital ortamda geçmektedir. İnternette yapılan saldırıların kaynağının bilinmemesi konusunda özellikle devlet destekli olup olmadığının bilinmemesi sebepleriyle siber saldırılar sonrası devletlerarasında karşılıklı tartışmalar ve suçlamalar olmaktadır.

Siber suçların etkileyiciliği bireysel olabileceği gibi bazen bir kurum, şirket veya devlet gibi uluslararası bir aktörü de etkileyebilmektedir. Bu sebeple siber suçların küresel olarak tartışılma boyutu etkilediği aktöre göre değişkenlik gösterebilmektedir. Klasik bir terör faaliyetinde silah ve bomba kullanılması ile belli bir bölge, alan veya insanlar zarar görürken siber terör faaliyetlerinde bilgisayar ve bilgi sistemi kullanılması marifetiyle devlete ekonomik, sosyal ve siyasal sonuçları büyük ölçüde ve milyonlarca kişiyi etkileyebilecek

zararlara sebep olabilmektedir. Üstelik terörü kontrol altına alma veya minimize etmek mümkün iken siber terörist grupları ve hackerları tespit ve yok etmek çoğu zaman imkânsızdır.

Devletler bu sebeplerle analizcisinden büyük veri yöneticisine, programcısından yazılım geliştiricisine kadar gerekirse fiziksel ordusu gibi bir bilgi teknoloji (IT) ordusu kurması artık zorunluluktur. Devletlerin petrol, doğalgaz veya nükleer santral kurması kadar artık güçlü bir bilgi sistemi ve alt yapısının kurmasının önemi artmıştır. Hatta gerekli kurumları kurmadan önce bir bilgi sistemi oluşturulması ve bunun üzerine inşa edilmesi önem kazanmıştır. Aksi halde bir nükleer tesis kontrolden çıkabilir, elektrik şebekesi çökebilir, uydu sistemleri ele geçirilebilir, uçukların kontrol sistemi kaybedilebilir, metro veya tren kazalarına yol açacak güvenlik ihlalleri ile karşılaşılabilir.

Uluslararası arenada siber güvenlik yatırımları ve çalışmaları hız kazanmışken Türkiye'nin duyarsız kalması beklenemez. Terör örgütleri, çıkar grupları ve sınır aşan suç işleyen örgütler siber saldırıları her an kullanabilmektedirler. Bu açıdan Türkiye yurt içi veya yurt dışı kaynaklı siber saldırılara karşı her daim hazır olmak zorundadır. Ayrıca Türkiye sadece kendi resmi kurumlarını değil ekonomik çıkarları gereği ticari şirket ve özel sektör girişimcilerini de korumak zorundadır.

Tüm bu sebeplerle Türkiye siber uzay kapasitesini geliştirmek zorundadır. Türkiye; siber güvenlik stratejisi, siber güvenlik eylem planları, siber güvenlik durum raporları ve eksiklileri belirleyerek gereksinim duyulacak her türlü önlemelerin alınması zorunluluktur. Türkiye hem siber akademik düzey hem de pratik uygulamalar açısından ABD, Rusya, Japonya, Kore ve Çin ile karşılaştırıldığında zayıf olduğu görülecektir. Bu sebeple kendisini önce bu ülkelere karşı geliştirmesi ve bu ülkelerden gelebilecek siber tehditlere karşı korumaya almalıdır.

Türkiye'nin siber anlamında kendini geliştirmesinde önüne engel olan durumlar vardır. Özellikle jeopolitik öneminden kaynaklı askeri ve güvenlik alanına çok ciddi para harcanmaktadır. Bu sarfiyatın siber güvenlik kısmına ciddiyetle ve samimi aktarım yapılmalıdır. Özellikle iç politikada değişen sürekli gündemler ve politikalar, yapılması gerekenlerin önüne geçmemelidir.

3. SİBER HUKUK VE SİBER SUÇLAR

İnsanoğlunun tarihsel gelişimini bakacak olursak avcı toplayıcılıktan yerleşikliğe geçip tarım çağına geçmiştir. Tarım çağı sonrası sanayi çağına geçen insanoğlu günümüzde bilimin ve teknolojinin gelişimi ile birlikte bilgi çağına geçmiştir. Bilgi çağına geçerken insan haklarının tarihsel gelişimi de sürmüştür. İnsan haklarının tarihsel gelişimi insanlığın gelişimi kadar önem arz etmektedir. İnsan haklarının tarihsel gelişiminde en önemli şey iktidarın veya egemen olan kralın yetkilerinin sınırlandırılması meselesidir. Böylelikle insan hakkına ve özgürlüğüne dokunulmayarak düşünsel ve tarihsel olarak gelişme göstermiştir.

"İnsanlık onuru" fikri ve düşüncesi insanlık tarihi kadar kadim olup tüm din ve kültürlerde farklı şekillerde vardır. İnsan haklarının korunmasının özünde de "İnsanlık onurunu" korumak esastır. Afrika felsefesinde insana verilmiş en yüksek değer olan "ubuntu", İslamiyet'te yabancılara verilen haklarda da gözlemlenir. İnsanın kendisine nasıl davranılmasını istiyorsa aynı şekilde başka insanlara davranması ile ortaya çıkan "altın kural" diğer dinlerde de görülecektir. Fakat tam anlamıyla insan hakları fikrinin yerleşmesi rasyonalizm ve aydınlanmacılık felsefesinin gelişimi ayrıca liberalizm, demokrasi ve sosyalizmin temelinde inşa edilmiştir. Modern bir kavram olan "insan hakları" kavramı Avrupa kaynaklı olsa bile özgürlük ve sosyal adalet kavramları açısından diğer din ve kültürlerin ortak parçasıdır (Benedek, 2006:39).

İnternetin hayatımıza girmesiyle insan hakları yeni bir mecraya taşındı. Bu sebeple yeni düzenlemeler yapılması ve bazı hakların daha çok korunması veya müdahale edilmemesi gerekliliği doğmuştur. Örnek olarak dijital çağa uygun olmayan vergi sistemi getirilirse internet üzerinden alışverişlerde vergi usulsüzlükleri olabilir veya dış ticaretin büyük çoğunluğu günümüzde internetten de olabilmekte ve dış ticarette vergi adaletsizliği önlenemezse bu da insan haklarına aykırı olabilir. Bir başka örnek olarak insanların internet sitesine erişim hakkının engellenmemesi gerekmektedir. Haberleşme özgürlüğüne saygı duyulması ve gereksiz kısıtlamalar yapılmamalıdır. Bir başka örnek olarak internetten alışveriş yapılırken güvenli yapılabilmeli ve bunun yanında kişisel verilerinin üçüncü şahıslarla paylaşılmamasını isteme hakkına sahip olunmalıdır.

Günümüzde internet üzerinde kişilik hakkına saldırı çok kolay hale gelmiştir. Ayrıca basın, televizyon, haber siteleri ve sosyal medya yolu ile geniş kitlelere kolayca kısa zamanda ulaşılabilmektedir. Bir internet sitesinde özel hayatın gözler önünde olması ve gerçek dışı olan

yayınlar ile şeref ve haysiyeti zedeleyici ihlaller olup internette kişilik hakkı ihlallerindendir. İnternet yoluyla işlenen İnsan hakları ihlallerinin olmaması için hem kamu sektörü hem özel sektöre önemli görevler düşmektedir.

Teknolojinin gelişmesi insan haklarını olumlu anlamda geliştirmesi beklenir. Çünkü teknoloji insanlığın refahını ve yaşam standardını arttırmaktadır. Ancak insana güvenin kalmaması ve her işi robotlara yaptırmak insana verilen değeri azaltır.

3.1: Ulusal Siber Hukuk ve Siber Suçlar

İnternet yoluyla işlenen siber suçların ve hak ihlallerinin olmaması için hem kamu sektörü hem özel sektöre önemli görevler düşmektedir. İnternetin hayatımıza girmesiyle insan hakları yeni bir mecraya taşındı. Bu sebeple yeni düzenlemeler yapılması ve bazı hakların daha çok korunması veya müdahale edilmemesi gerekliliği doğmuştur. İnternette gerçekleşen insan hakları ihlalleri teknolojinin gelişimi ile birlikte artmıştır. Bu ihlallerin toplum üzerindeki etkisi yadsınamaz. Siber zorbalık, yetkisiz erişim, özel hayatın gizliliğini ihlal, internette çocuk istismarı, banka bilgilerinin ele geçirilmesi ve diğer siber suçlar internet yoluyla gerçekleşen insan hakları ihlalleridir. Bu ihlallerin önlenmesi ve yaptırımların etkili olması gerekmektedir.

Günümüzde sadece Türkiye'de değil tüm dünyada insanlar bir siber tehdit veya bir siber suç ile karşılaştıklarında ne yapacaklarını bilmemekte ve en önemlisi de haklarını bilmediğinden mağduriyet yaşayabilmektedirler.

Hukuk dinamik olup sosyal, kültürel, siyasal boyutları olmaktadır. Siber hukuk ta dinamik olup bunlardan bağımsız olamaz. Her ülke kendi örf ve kültürü, teknolojik gelişme düzeyi ve yaşama standartlarına göre siber hukuk anlamında düzenlemelere gitmiştir. Her ülkenin siber suç tanımları ve yaptırımları farklıdır. Bir ülkeye göre siber suç olabilecek bir eylem başka bir ülkeye göre olmayabilmektedir. Ayrıca siber suç kabul görülen eylemlerin yaptırımları ve infaz rejimleri de farklı olabilmektedir. Küresel bir oydaşmanın olmaması bir yana siber suçlar üzerinde bile anlaşma veya konsensüs yoktur. Durum böyle iken ulusal düzenlemelerin yetersiz kalacağı açık olup uluslararası veya sınır aşan suçlarda etkili çözümler elde edilememektedir.

Uygulanan şiddet tiplerine göre yapılan sınıflandırmada şu alt başlıklar ile karşılaşılmaktadır(Polat, 2017: 17)

1.Fiziksel Şiddet

2.Cinsel Şiddet

3.Duygusal Şiddet

4.Ekonomik Şiddet

5.Siber Şiddet

Siber suçlar bir "şiddet eylemi" olarak kullanılabilir. Bu sebeple toplumsal, psikolojik ve duygusal olarak insanları ciddi boyutta etkilemektedir. İnsanların birbirlerine yaptıkları zorbalıkların internet vasıtasıyla siber ortamda yapılmasıyla karşımıza "siber zorbalık" kavramı çıkmaktadır.

Siber suç denildiğinde akıllara hemen "siber zorbalık" gelmektedir. Siber zorbalık konusunda da günümüzde artış olmuştur. Siber zorbalık olarak literatürde çok çeşitli tanımlamalar vardır. Ortaklaşmış bir tanım olmamakla birlikte teknoloji aracı kılınarak gerçekleştirilmesi ve zorbalık veya zarar verici rahatsız eylemler olmasında ortaklaşmış olduğu görülebilir.

Tokunaga (2010)'nın toplu değerlendirmesine göre:

Belsey (2009)	Başkalarına zarar vermek amacıyla iletişim teknolojileri kullanılarak birey veya grup tarafından, tekrarlanan, kasıtlı ve düşmanca davranışlar,
Finkelhor ve ark. (2000)	Çevrimiçi taciz. Cinsel kışkırtma haricinde tehdit veya saldırgan davranışların başkalarının görmesi için çevrimiçi (olarak) gençlik gurubuna yayınlanması
Juvoven ve Gross (2008)	İnternet veya diğer modern elektronik cihazları kullanarak başkasını tehdit veya hakaret etmek
Li (2008)	Kişisel elektronik malzeme, anlık mesajlaşma, internet veya elektronik iletişim gereçleriyle yapılan zorbalık
Patchin ve Hinduja (2006)	Elektronik yazışma ortamında isteyerek tekrarlanan zarar verici davranışlar
Slonje ve Smith(2007)	Modern teknolojik gereçlerle, özellikle mobil telefon ve/veya internet üzerinden yapılan saldırgan davranışlar
Smith et al. (2008)	Kolayca kendini savunamayan kurbana karşı elektronik formlar kullanarak, art arda veya zaman içinde, bir grup veya birey tarafından süreklilikle yürütülen, isteyerek yapılan bilinçli saldırganlık
Willard (2007)	Zararlı veya zalimane metin veya görüntüleri internet veya dijital iletişim ortamlarında kullanımı

Tablo 3.1: siber zorbalık tanımını Alan yazınında Teknolojik Yorumları (Tamer& Vatanartıran, 2014: 3)

Teknoloji ve bilimin ilerlemesiyle özellikle günlük hayatta insan yaşamını kolaylaştırmıştır. Ancak teknolojik araçların insan hayatında çok fazla kullanımı, mahremiyet hakkının ihlal edilebileceği konusunda kaygılar doğurmuştur. Sağlıklı bir şekilde

kullanılmayan teknoloji topluma zarar getirir. Eğer yasalar ile denetlenmezse sadece kişinin ruh veya fiziksel sağlığını değil toplumun bütünlüğü ve barışını tehlikeye düşürebilecektir.

Devletin yanı sıra birçok kurum ve kuruluş bireyler hakkında bilgi toplayarak özel hayatın gizliliğini ihlal etme imkânını bulabilmektedirler. Örnek vermek gerekirse özel veya kamu hastanelerinde Parmak izi kaydı alınması, GSM operatörlerinin reklam için veya bir başka sebeple kullanıcısı olmayan bireylerin telefonuna ulaşıp ürün veya reklam tanıtımı için arama yapması, özel ve kamu iş yerlerinde kameralar ile denetim gibi birçok örnek verilebilir. Yapılacak düzenlemelerinde sadece kamuyu değil özel kurumları ve kuruluşları da içerecek şekilde düzenlemeler yapılması gerekir.

Teknoloji suç işlemeyi kolaylaştırdığı gerçeği de göz ardı edilmemelidir. Suçlular, suç işlemeyi ve işledikleri suçları gizleme konusunda teknolojik yeniliklerden faydalanmaktadırlar. Bu sebeple suç ve suçlularla mücadelede güvenlik güçlerinin başarılı olabilmesi için teknoloji ve teknik donanım kullanımı tercih değil zorunluluk meselesi olmuştur.

Güvenlik ve emniyet güçlerinin teknoloji kullanımı, klasik metotlardan daha verimli olmaktadır. Sadece suçların aydınlatılması meselesinde değil görev suiistimallerinin olmasını engellemekte ve insan hakkı ihlali olabilecek durumları azaltmaktadır. Suç ile mücadelede zorunluluk olan teknoloji ve teknik donanım kullanımı, gerekli yasal düzenlemeler yapılarak kontrol altına alınması da gerekir. Aksi halde suiistimaller ve insan hakkı ihlalleri kaçınılmaz olur.

Güvenlik ve emniyet güçlerinin teknolojiyi kullanacak personellerine gerekli profesyonellik eğitimi vermesi gerekir. Ayrıca bu profesyonellik eğitimi yanı sıra meslek etik ve ahlakı vermesi gerekir. Aksi halde gerekli eğitim ve kültür verilmediğinde teknolojiyi kullanan personel keyfiyet için veya kendi çıkarı için teknoloji ve yetki kullanımı yapabilecektir.

Gelişmiş teknoloji ve son model cihazların kullanımı devlet güvenliği için elzem olup kullanılması gerekirken yani konunun teknik ve yasal boyutu hayata geçirilirken insan haklarının ihlal edilmemesi ve suiistimallere karşı gerekli tedbirlerin alınması açısından etik ve sosyal boyutu göz ardı edilmemelidir.

M.Foucault' a göre hapishanelerin, ıslahevlerinin, tımarhanelerin amacı sadece güvenliğin sağlanması değil aynı zamanda toplumda disiplin mekanizması işlevi görmesidir. Hapishaneler özellikle işçi sınıfının denetlenmesinde ve bir disiplin müessesesi gibi "hapishane takımadası" oluşturulmuştur. Sakinlerini gözetleyerek, topluma tehdit oluşturmayacak "uysal bedenler" yapmayı hedefliyordu (Zedner, 2015: 39-40).

Modern devlet, sanayi öncesi toplumdan daha çok bireyi kontrol imkânına sahiptir. Modern devlet, bireyin sadece fiziki varlığını değil; duygularına, düşüncelerine ve gelecek planlarına müdahale ve kontrol imkânına sahiptir. M.Foucault'a göre Modern devlet bireyleri iş yaşamında değil ev ve özel yaşamlarında da izleme ve fişleme imkânına sahiptir. Tasarımı Samuel Bentham ve düşünsel temellere Jeremy Bentham'a ait olan Panoptikon'un özelliği, insanların gözetim altında tutulmasını amaçlamaktaydı (der Çoban & Ataman, 2016: 3).

İnternette her eylemin veri olarak saklanabilme olanağının olması piyasa ve güvenlik güçlerinin gözetlemesini olanaklı kılmakla birlikte bu toplanan verilerin yönetimi de güçleşmektedir. Verilerin birikimi özellikle tam ve anlamlı bilgiye dönüştürülme evresinde "veri yönetimi paradoksuna" sebebiyet vermektedir (Ergur, 2016: 7). Herkesin gözetim ve denetim altında olduğu büyük hapishanede olduğu gibi düşüncesi bir tür paranoya dönüşse de teknolojik imkânların kullanımı ile birlikte artan bir şekilde gözetleme ve kayıt altına alma devam etmektedir.

Yeni gözetim teknolojilerinin gelişmesi vatandaş olsun olmasın bazıları şüpheli sıfatıyla daha sıkı izlenebilmektedir. Teknolojide düşen maliyetler sebebiyle daha kolay ve yaygın olarak kullanılabilmektedir. MOBESE ve uydu izleme metotları, veri gözetlemelerinin bilgisayar programları yardımıyla veri madenciliği, tasnifi ve iletişim kayıtlarının depolanması, parmak izleri, göz bebeği yani iris taramaları ve DNA fişleme yollarıyla gerçekleştirilmektedir. Bu teknolojik gelişmeleri etkili polislik ve kapsamlı toplumsal koruma aracı olarak görenler ile "totaliter" ve baskıcı bir topluma doğru gidişin habercisi olarak görenler kutuplaşmışlardır. Bir de kamu yararına hizmet edildiğine inanan orta bir görüş de vardır (Zedner, 2015: 80-81).

Dikkat çekici bir başka nokta ise teknolojinin güvenlik anlamında kullanımı sadece emniyet ve güvenlik güçlerinin tek elinde olmaktan çıkmıştır. Yani sadece "resmi" değil

"sivil" ve "özel" kurumların güvenlik hizmeti veren birimleri bilişim teknolojisinin imkânlarından yararlanmaktadır. İster kamu kurumları, hastaneler, okullar gibi devletin sorumluluğunda olan konumların korunması olsun ister sivil kurumlar, şirketler ve bireysel mülklerin korunması olsun gerekli donanım ve teknolojinin nimetlerinden faydalanmaktadır.

Teknolojinin yaygınlaşması ile bir takım klasik suçlar daha kolay işlenmekte olup, yeni tipte suçlar ortaya çıkarmıştır. Sadece sansasyonel ve büyük etki yaratabilecek olaylarda kendini gösteren siber suçlar, günümüzde hemen hemen her bireyin karşılaşabileceği suç mağduru olma olasılığını arttırmıştır.

Siber Suç tanımına bakılırsa, bir bilişim sisteminin güvenliğine ve bu güvenliğe bağlı verileri ve/veya kullanıcısını hedef alan ve özellikle de bir bilişim sistemi vasıtasıyla işlenebilen suçlardır (https://www.egm.gov.tr).

Siber suç, bir bilişim sistemi kullanılarak işlenmekte olduğu bilinmektedir. Teknolojinin gelişimi ile birlikte artık tüm suçların bilişim sistemi kullanılarak işlenebileceği görülmektedir ancak her bilişim sistemi kullanılarak işlenen suçun da siber suça girmeyeceği unutulmamalıdır.

İnternette işlenen siber suçlar denilince Türk Ceza Kanunu'nun özellikle 243. 244. ve 245. Maddeler akıllara gelse de hepsine bakmanın konunun anlaşılması ve siber suçları bilmek için elzem olduğu görülür.

-Haberleşmenin engellenmesi (Bilişim Sistemleri Kullanmak suretiyle) (Türk Ceza Kanunu madde 124)

-Haberleşmenin gizliliğini ihlal (Türk Ceza Kanunu madde 132)

-Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması (Türk Ceza Kanunu madde 133)

-Özel hayatın gizliliğini ihlal (Türk Ceza Kanunu madde 134)

-Kişisel verilerin kaydedilmesi (Türk Ceza Kanunu madde 135)

-Verileri hukuka aykırı olarak verme veya ele geçirme (Türk Ceza Kanunu madde 136)

-Verileri yok etmeme (Türk Ceza Kanunu madde 138)

-Nitelikli Hırsızlık (Türk Ceza Kanunu madde 142/2-e)

- Nitelikli interaktif dolandırıcılık (Türk Ceza Kanunu madde 158/1-f)

-Bilişim sistemine girme (Türk Ceza Kanunu madde 243)

-Sistemi engelleme, bozma, verileri yok etme veya değiştirme (Türk Ceza Kanunu madde 244)

-Banka veya kredi kartlarının kötüye kullanılması (Türk Ceza Kanunu madde 245)

-Yasak cihaz veya programlar (Türk Ceza Kanunu madde 245/A)

- Çocuk Pornografisi (Türk Ceza Kanunu madde 226/3)

- Online Örgütlü Kumar (Türk Ceza Kanunu madde 228 ve Futbol ve Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkındaki Kanuna Muhalefet 7258 SKM)

-Elektronik İmza Oluşturma Verilerinin İzinsiz Kullanımı ve Sertifikalarda Sahtekârlık (Elektronik İmza Kanunu madde 16-17)

-Ticarî sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması (Türk Ceza Kanunu madde 239/1-2)

-Bilişim Sistemlerini Kullanarak Devlet Sırlarına Karşı Suçlar (ör: Devlet sırlarından yararlanma, Devlet hizmetlerinde sadakatsizlik Türk Ceza Kanunu madde 333, Devlet Sırlarına Karşı Suçlar ve Casusluk suçları Türk Ceza Kanunu madde 326,327,328,329,330)

Siber suçlara literatürde bilgisayar suçu, internet suçu, internete özgü suçlar veya bilişim suçları gibi adlandırmalar yapılmaktadır. Birçok suç bilişim sistemi kullanılarak işlenebilir. Ancak yukarıda da dikkat edileceği üzere bilinmesi gereken siber suçu diğer suçlardan ayıran en önemli özellik bilişim sistemi kullanılarak işlenmesidir.

Teknolojinin gelişmesiyle suçlular her türlü teknolojik gelişmeden yararlanmaktadır. Örnek vermek gerekirse tam anlamıyla bir siber suç olmayan ancak bilişim yoluyla işlenen asayiş suçları vardır. İntihara Yönlendirme (TCK madde 84), Tehdit (TCK madde 106), Şantaj (TCK madde 107), Hakaret (TCK madde 125), Fuhuş (TCK madde 227), Kumar Oynanması İçin Yer ve İmkân Sağlama (TCK madde 228) gibi suçlar asayiş suçları olup bilişim yoluyla ve teknolojik imkânları kullanılarak işlenebilmektedir. Günümüzde her suç teknolojik olarak işlenebilmektedir. Terör örgütü propagandası ile terör suçu işlenebilecekken Cumhurbaşkanına hakaret (TCK madde 299), Devletin egemenlik alametlerini aşağılama (TCK madde 300) veya Türk Milletini, Türkiye Cumhuriyeti Devletini, Devletin kurum ve organlarını aşağılama (TCK madde 301) ile devletin güvenliğine karşı suçlarda bilişim yoluyla ve teknolojik imkânları kullanılarak işlenebilmektedir.

Günlük hayatta olan suçlar ve suç tipleri dijital ortamda da görülmektedir. Kredi kartı dolandırıcılığı, banka hesabından izinsiz para harcanması, internette yasa dışı yayınlar, çocuk pornografisi, sosyal medya hesabın hacklenmesi, şirket veya kurumsal bilgisayarların sunucularının hacklenerek sonrasında fidye istenmesi, siber zorbalık faaliyetleriyle rahatsızlık verme çok sık karşılaşılan vakalardır. Sanal ortamda müstehcen yayınlar toplumsal ahlakı etkilemektedir. Tüm bunlar yasal bir düzenlemenin ve denetimlerin sağlam olmasını şart koşmaktadır.

Bilişim suçları denilince temelde ikili bir ayrıma gidilebilir: Kanunda tanımlanan bilişim suçları ve Bilişim sistemleri kullanılarak işlenen suçlar. Tablo olarak genel hatları ile bakıldığında:

Kanunda Tanımlanan Bilişim Suçları:	**Bilişim Sistemleri Kullanılarak İşlenen Suçlar**
-Bilişim Sistemine Girme, Sistemi engelleme, bozma, verileri yok etme veya değiştirme TCK 243, 244 -Banka veya kredi kartlarının kötüye kullanılması, Kart Kopyalama TCK 245 -Bilişim Sistemleri Kullanılması Suretiyle Nitelikli Hırsızlık TCK 142/2/e - Nitelikli interaktif dolandırıcılık (Türk Ceza Kanunu madde 158/1-f) -Elektronik İmza Kanununun 16 ncı ve 17 nci maddeleri -Banka Kartları ve Kredi Kartları Kanununun 23 üncü maddesi Banka Hesaplarını Boşaltma (TCK142/2/e) -Devlet Sırlarına Karşı Suçlar -İnternet üzerinden Çocuk İstismar Görüntü Paylaşımı- Çocuk Pornografisi (Türk Ceza Kanunu madde 226/3) -Özel Hayatın Gizliliğini İhlal (sahte facebook hesabı), - Online Örgütlü Kumar (Türk Ceza Kanunu madde 228 ve Futbol ve Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkındaki Kanuna Muhalefet 7258 SKM)	-Silah Ticareti, Uyuşturucu Madde Ticareti, gibi. -Yasadışı Yayınların Neşredilmesi, Bölücü Terörist Faaliyetler. v.s -Tehdit, Şantaj, Hakaret, -Örgütlü Olmayan Sanal Kumar -Müstehcenlik, Porno Görüntüler -Dolandırıcılık Olayları (sahibinden.com gibi kaparo dolandırıcılığı), Ara-Kazan Dolandırıcılığı, -Elektronik Cihaz kullanılmadan ATM'lerden sıkıştırma yöntemiyle ve fiziksel olarak kredi kartı veya banka kartının çalınması -Devlet Büyüklerine, Dine, Peygambere ve Atatürk'e Hakaret.

Tablo 3.2: Kanunda Tanımlanan Bilişim Suçları ve Bilişim Sistemleri Kullanılarak İşlenen Suçlar

Türkiye'de işlenen bilişim suçlarında 2000 yılında 60 suç işlenmişken, 2004 yılında 317, 2005 yılında 214, 2006 yılında 299 suç işlenmiştir (Sargın & Temurçin, 2011:30).

		Açılış yılına göre 2018 Yılında Karara Bağlanan Davalardaki Suç Sayıları											
İsnat Edilen Suç	TCK Madde No	2014 ve öncesi	%	2015	%	2016	%	2017	%	2018	%	Toplam	%
Malvarlığına Karşı Suçlar	141-169	38819	7,4	32370	6,1	67963	12,9	202860	38,5	184620	35,1	526632	21,6
Vücut Dokunulmazlığına Karşı Suçlar	86-93	19013	4,0	30 432	6,4	67 413	14,2	194445	40,9	163649	34,5	474952	19,5
Hürriyete Karşı Suçlar	106-124	11243	3,3	18955	5,5	48411	14,1	145904	42,3	120039	34,8	344552	14,1
Şerefe Karşı Suçlar	125-131	5001	2,3	12382	5,6	34681	15,6	95544	43,1	74205	33,5	221813	9,1
Anayasal Düzene ve Bu Düzenin İşleyişine Karşı Suçlar	309-316	1148	0,8	1274	0,9	8823	6,4	75989	55,5	49700	36,3	136934	5,6
Kamunun Sağlığına Karşı Suçlar	185-196	2705	2,0	1915	1,4	7390	5,4	52895	38,8	71511	52,4	136416	5,6
Genel Tehlike Yaratan Suçlar	170-180	1194	1,0	1641	1,4	5212	4,5	41 898	36,1	66174	57,0	116119	4,8
Kamu Güvenine Karşı Suçlar	197-212	11671	11,8	6780	6,9	12708	12,9	34300	34,8	33149	33,6	98608	4,0
Hayata Karşı Suçlar	81-85	3597	4,2	3137	3,7	5200	6,1	64910	75,8	8738	10,2	85582	3,5
Adliyeye Karşı Suçlar	267-298	2516	3,8	1901	2,9	6033	9,2	26323	40,2	28754	43,9	65527	2,7
Kamu İdaresinin Güvenilirliğine ve İşleyişine Karşı Suçlar	247-266	5079	10,1	4229	8,4	7155	14,3	17974	35,8	15704	31,3	50141	2,1
Cinsel Dokunulmazlığa Karşı Suçlar	102-105	1023	2,8	1066	2,9	3321	9,0	16073	43,7	15336	41,7	36819	1,5
Bilişim Alanında Suçlar	**243-246**	**2919**	**9,4**	**1614**	**5,2**	**4492**	**14,5**	**11349**	**36,5**	**10706**	**34,4**	**31080**	**1,3**
Genel Ahlaka Karşı Suçlar	225-229	1395	5,6	1395	5,6	2689	10,8	10159	40,7	9323	37,4	24961	1,0
Kamu Barışına Karşı Suçlar	213-222	5854	35,1	950	5,7	1287	7,7	3562	21,4	5025	30,1	16678	0,7
Özel Hayata Karşı Suçlar	132-140	237	1,5	1653	10,4	2590	16,3	7617	47,9	3819	24,0	15916	0,7
Çevreye Karşı Suçlar	181-184	382	2,8	614	4,5	2084	15,3	6575	48,3	3963	29,1	13618	0,6
Ekonomi, Sanayi ve Ticarete İlişkin Suçlar	235-242	2885	38,8	960	12,9	1061	14,3	1173	15,8	1355	18,2	7434	0,3

Göçmen Kaçakçılığı ve İnsan Ticareti	79-80	723	9,8	363	4,9	999	13,6	2639	35,9	2636	35,8	7360	0,3
Aile Düzenine Karşı Suçlar	230-234	185	2,7	361	5,3	991	14,7	2936	43,4	2286	33,8	6759	0,3
Devletin Egemenliğine Karşı Suçlar	299-301	10	0,2	73	1,2	627	10,5	3103	51,8	2173	36,3	5986	0,2
Devletin Güvenliğine Karşı Suçlar	302-308	40	3,0	75	5,6	360	26,6	384	28,4	492	36,4	1351	0,1
Devlet Sırlarına Karşı Suçlar ve Casusluk	326-339	7	0,8	187	21,9	72	8,4	239	28,0	348	40,8	853	0,0
İşkence ve Eziyet	94-96	67	7,9	82	9,6	96	11,3	361	42,4	245	28,8	851	0,0
Ulaşım Araçlarına veya Sabit Platformlarına Karşı Suçlar	223-224	11	2,0	195	36,2	75	13,9	217	40,3	41	7,6	539	0,0
Koruma, Gözetim, Yardım veya Bildirim Yükümlülüğünün İhlali	97-98	2	0,7	11	3,8	54	18,7	141	48,8	81	28,0	289	0,0
Milli Savunmaya Karşı Suçlar	317-325		0,0		0,0	6	2,1	235	82,2	45	15,7	286	0,0
Çocuk Düşürme, Düşürtme veya Kısırlaştırma	99-101	9	8,0	8	7,1	10	8,9	47	42,0	38	33,9	112	0,0
Yabancı Devletlerle Olan İlişkilere Karşı Suçlar	340-342	1	20,0		0,0		0,0	2	40,0	2	40,0	5	0,0
TCK Kapsamındaki Diğer Suçlar		251	2,0	374	3,0	1062	8,6	5338	43,5	5263	42,9	12278	0,5
TCK Toplamı		117987	4,8	124997	5,1	292855	12,0	1025192	42,0	879420	36,0	2440451	100,0

Tablo 3.3: Açılış yılına göre 2018 Yılında Karara Bağlanan Davalardaki Suç Sayıları (www.adlisicil.adalet.gov.tr/)

Bilişim alanındaki açılış yıllarına göre 2018 yılında karara bağlanmış olan davalardaki suç sayılarına bakıldığında 2018 yılına kadar artan bir şekilde dava sonuçlandığı çıkarılabilir. Bunun böyle olmasında hem davaların sayısının artmasının hem de o yıl içinde dava sonuçlanmayıp bir sonraki yıllara davaların kalmasının sebebi olduğu anlaşılabilir. Bilişim suçlarının hemen sonuçlanması doğası gereği beklenmez. Bunun sebebi yetkisiz erişim konularında sunucu veya ip yurt dışı kaynaklı bir site olduğunda gerekli yazışmaların sürmesi ve dosyanın toplanması dosyanın büyüklüğüne göre yıllar alabilmektedir.

Bir başka yorum yapılırsa 2018 yılında bilişim suçlarında 10.706 karara bağlanmış suç varken, toplam karara bağlanmış 31080 karar vardı. Bunun anlamı 2018 yılında işlenen

suçlarda bir azalma değil, 2018 yılında işlenmiş olup daha sonraki yıllarda devam edecek daha çok davanın olduğunun habercisidir. İşlenen bir bilişim suçu aynı senesinde sonuçlandırılamamaktadır. Bu diğer suçlarda da bu kadar olmayabilmektedir. Örnek vermek gerekirse; Anayasal Düzene ve Bu Düzenin İşleyişine Karşı Suçlar, Hürriyete Karşı Suçlar, Malvarlığına Karşı Suçlar veya Vücut Dokunulmazlığına Karşı Suçlarda dava sonuçlandırılması hem şüphelisi müştekisi belli olması hem de toplumda infial yaratmaması amacıyla daha çabuk sonuçlandırılmaya çalışıldığı ancak Bilişim suçları gibi suçlarda şüphelilerin tespiti, infial yaratmaması ve başka sebeplerle davaların sonuçlandırılmaları gecikebilmektedir.

Teknoloji kullanımı giderek artmaktadır. Buna örnek olarak aşağıdaki tablo 4 verilebilir. Tablo incelendiğinde sabit olarak kullanılan telefon abone sayısı azalmakta olup cep telefonu kullanan abone sayısı ise düzenli bir yükseliş olmasa da artış olduğu görülmektedir. İnternet abone sayısında ise yükselişin olduğu 2004 sonrasında hiç azalmadan devamlı yükselmiştir.

YIL	Sabit telefon abone sayısı	Cep telefonu abone sayısı	İnternet abone sayısı
1996	14 286 478	692 779	-
1997	15 744 020	1 483 149	-
1998	16 959 500	3 382 137	229 885
1999	18 054 047	7 562 972	436 610
2000	18 395 171	14 970 745	1 629 156
2001	18 904 486	19 502 897	1 619 270
2002	18 914 857	23 323 118	1 309 770
2003	18 916 721	27 887 535	906 650
2004	19 125 163	34 707 549	1 474 590
2005	18 978 223	43 608 965	2 248 105
2006	18 831 616	52 662 709	3 180 580
2007	18 201 006	61 975 807	4 842 798
2008	17 502 205	65 824 110	5 804 923
2009	16 534 356	62 779 554	8 849 779
2010	16 201 466	61 769 635	14 443 644
2011	15 210 846	65 321 745	22 371 441
2012	13 859 672	67 680 547	27 649 055
2013	13 551 705	69 661 108	32 613 930
2014	12 528 865	71 888 416	41 272 940
2015	11 493 057	73 639 261	48 617 291
2016	11 077 559	75 061 699	62 280 191
2017	11 308 444	77 800 170	68 869 578

2018	11 633 461	80 117 999	74 500 089
2019[(1)]	11 542 548	82 896 108	77 048 026

Tablo 3.4: Sabit telefon, cep telefonu ve internet abone sayısı (http://www.tuik.gov.tr/)(not:1 Veriler Eylül ayı sonu itibarıyladır.)

Yukarıdaki tablo incelendiğinde internet ve cep telefonu abone sayısı artış göstermişken eski bir teknoloji olan sabit ev telefon abone sayısı azalmıştır.

Teknoloji kullanımının arttığı çağımızda bilişim ve siber suçlarda artış olacağı da açıktır. Suçu önleme açısından devletin gerekli kurumlarının da teknoloji kullanımını arttırması gerekmektedir. Bu sadece güvenlik için değil acil ve sağlık meselelerinde de geçerlidir.

ABD de kullanılan 911, İngiltere de kullanılan 999 ve Türkiye'de 112 olarak kullanılan acil servis hizmetlerinin ileri teknoloji ile donatılması aciliyet ve elzem olmuştur. Keza 155 ve 156 gibi polis ve jandarma ihbar hatlarının, Mobesse sistemlerinin kurulması gibi acil müdahale etme imkânı veren teknolojilerin kullanımı insan hayatı için önem arz etmektedir.

Teknolojinin gelişmesi ile birlikte sanık ve suçlular hakkında bilgi toplanması, bu bilgilerin saklanması ve gerektiği zaman kullanımı kolaylaşmıştır. Özellikle kriminal suçlulardan alınan parmak izi ve fotoğraflama olay aydınlatmalarda etkili olmaktadır. Her suçlunun bir iz bırakabileceği ve izin kriminal laboratuvarında araştırma ve incelemelerle anlamlandırılması ile suçlar aydınlatılabilmektedir.

Demokratik toplumlarda devletin toplumu izleme ve kontrol etmesi yerine kendisine hizmet edecek, vatandaşların refahını ve demokrasisinin seviyesini yüceltecek olan özgürlük değerlerini yerleştirmek ve devletin kendi kurumlarını kontrol etmesi gerektiğine inanılır. Yani vatandaşların kontrolü yerine devletin kontrolü elzemdir. Devlet, toplum üzerindeki kontrolü yine toplumun menfaatine olmalıdır. Toplumun büyük bir kısmı devletin kendilerini gözetlediğini veya izlediğini düşünürse sağlıklı bir toplum yapısı oluşmayacaktır.

Dikenli teller, gözetleme araçları, güvenlik güçleri tam anlamıyla güvenliği sağlamada yeterli değildir. Güvenliğin tam anlamıyla sağlanması vatandaşların kendilerini güvende hissetmeleri ile doğru orantılıdır. Bu sebeple güvenliğin psikolojik ve algısal tarafı da göz ardı edilmemelidir.

Sosyal Medya, yeni arkadaşlarla tanışmak ve bilgiye ulaşmakta faydaları olmuştur. Ancak kişisel bilgilerin paylaşılması konusu ve mahremiyet hakkının ihlal edilebileceği konusunda kaygılar doğurmuştur. İnternette gerçekleşen insan hakları ihlalleri teknolojinin gelişimi ile birlikte artmıştır. Bu ihlallerin toplum üzerindeki etkisi yadsınamaz. Siber zorbalık, yetkisiz erişim, özel hayatın gizliliğini ihlal, internette çocuk istismarı, banka bilgilerinin ele geçirilmesi ve diğer siber suçlar internet yoluyla gerçekleşen insan hakları ihlalleri olup bu ihlallerin önlenmesi ve yaptırımların etkili olması gerekmektedir.

20. yüzyılın sonlarına doğru medya tarafından kuşatılan ve yalnızlaşan bireyin iktidar karşısında direniş alanının azaldığı bir dönüşüme zorlanmış olup 21. Yüzyılın başlarında sessiz yığınların internet haberciliği, teknoloji ve siber ağları kullanarak ayağa kalktığını söylemek için erkendir. Ancak şurası bir gerçektir ki insanların önemli bir çoğunluğu sosyal medyayı kendi görüşlerini insanlarla paylaşmak, taraftar bulmak, topluluk oluşturmada kullansa da küreselleşen ancak bir o kadar da homojenleşen "yenidünya" düzeninde var olma çabası içerisindedir (Kaplan ve Ertürk, 2012: 11).

Matbaanın ortaya çıkması ile halka ulaşan bilimsel bilgi sayesinde nasıl ki insanlar aydınlanma çağına girmiş ise teknoloji bu hızla giderse ve sibernetik ilerlerse insanlığın tarihi de değişecektir. Değişen durumlara özgü yeni haklar çıkacaktır. Yeni hakların ihlal edilmemesi için de düzenlemelere ihtiyaç duyulacaktır. Mahremiyet Hakkı, internette ihlali durumunda insanı çok sıkıntılara sokabilecek ve özgürlük alanının çok ciddi tehditlerle karşılaşılması gibi sonuçları ağır olabilmektedir.

Mahremiyet hakkının ihlali konusunda genellikle devletin rolüne odaklanılır. Ancak günümüzde özel kişi ve kuruluşlar tarafından da özel yaşam alanına veya mahremiyet alanına tehditler olabilmektedir. Siber uzay çağında mahremiyet alanının korunması için güncel hukuki düzenlemeler yapılması gerekmektedir. Günümüzde telefon görüşmelerin dinlenmesinden, kişisel elektronik posta ve maillerin okunmasından, kişisel bilgi ve fotoğrafların gazete sayfaları, televizyon veya internet sitelerinde paylaşılmayacağından, kişisel mali durumlarla ilgili bilgilerin başka kişi veya kuruluşlara pazarlanmayacağından emin olunmamaktadır (Yüksel, 2003:183).

Mahremiyet hakkı, klasik haklardan olan birinci kuşak haklardandır. Bu hakların en önemli özelliği bireyi koruması ve devleti sınırlandıran negatif statü haklarındandır. Bu haklar

kişinin devlet, toplum ve üçüncü kişilerin dokunamayacağı özel alan yaratır (Fırat, 2015: 105).

Liberal görüşlerde insanı odak olarak alma ve devletin müdahale edemeyeceği özgür alanı koruma önem arz etmektedir. Liberal yaklaşımların tersine sosyalist yaklaşımlar toplum çıkarına vurgu yapıp kişisel hakların ve özgürlüklerin arka plana atılması tehlikesini barındırmaktadır. Mahremiyet hakkı olgusu dokunulmaması gereken ve özellikle de devletin müdahale olmaması için gerekli tedbirleri alması gereken bir haktır. Mahremiyet hakkı olgusu içinde özel hayatın gizliliği hakkını da içermektedir. Ancak özel hayatın ihlalinin alt bileşenleri ile daha geniş bir içeriğe sahiptir. Bu sebeple kişinin özel hayatının mahrem kabul edilmesi gerekir ve saygı duyulması istenilir.

Tüm insanlar internet ortamında da mahremiyet veya özel hayatın gizliliği hakkına ve korunma hakkına sahiptir. Söz konusu bu haklar ile gözetlenmeme, şifreleme hakkı ve internet ortamında anonim olabilme ve gizlenme hakkına sahiptir. Günümüzde internette kişilik hakkına saldırı çok kolay hale gelmiştir. Ayrıca basın, televizyon, haber siteleri ve sosyal medya yolu ile geniş kitlelere kolayca kısa zamanda ulaşılabilmektedir. Ayrıca bir kişinin elektronik postası kişisel verisi olup hem haberleşme özgürlüğünün hem de özel hayatın bir unsuru olabilmektedir. Bir internet sitesinde özel hayatın gözler önüne serilmesi ve gerçek dışı olan yayınlar yapılarak şeref ve haysiyeti zedeleyici ihlaller olup internette kişilik hakkı ihlallerindendir (Fırat, 2015:107-110).

Anayasamızın 20. Maddesinde geçen herkesin özel hayatı ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu belirtilmiştir. Ayrıca özel hayat ve aile hayatı gizliliğine dokunulamayacağı ifade edilmiştir ve güvence altına alınmıştır (www.mevzuat.gov.tr).

Avrupa İnsan Hakları Sözleşmesi 8. Maddesinde geçen her insanın özel hayatına, aile hayatına, özel konutuna ve haberleşmesine saygı gösterilmesi hakkına sahip olduğu belirtilmiş olup devletin bir birey için teminat altına alması gerek hakları saymıştır. Ayrıca Avrupa İnsan Hakları Mahkemesine göre özel hayat tanımlanamayacak derecede geniş bir kavram olup mahremiyet hakkından daha geniş olan bir haktır. Çünkü özel hayat özgür olarak kişiliğin oluşması ve gelişmesini sağlayan alanı ifade eder. Kısaca Özel hayat, insanın diğer insanlarla olan ilişki geliştirme hakkını da kapsamaktadır (Kilkelly, 2001:9-17).

Özel hayatın alt unsurları içinde şahsi verilerin, haberleşme, konut ve aile hayatına saygı gösterilmesi gerekliliği ilkesi vardır. Özel hayat hakkı, insanın özel hayatının müdahalelerden uzak ve özgür bir şekilde yaşama hakkıdır. İnsan toplumda yaşamaktadır ve özel hayat denildiğinde sadece kişinin özel yaşamıyla sınırlı olmamaktadır. İnsanın toplumsal yaşamdaki ifade, tasavvur, düşünce, din ve vicdan özgürlüklerini de kapsamaktadır. Yani Özel hayat hakkına verilen değer ve önem, temel insan haklarından olup güvence altına alınmış haklardandır (Korkmaz, 2014:100 ve 102).

Özel hayatın gizliliği ve korunması konusu tüm Demokratik rejimler ve devletlerin mutlak olarak koruma altına alması gereken haklardandır. Özel hayatın gizliliğini ihlal hakkı çok iyi korunması gerekmektedir. Çünkü diğer birçok hakkın özgürlüğü ve selameti için bu gereklidir. Kişinin seçme bilincinin gelişmesi için özel hayatın gizliliği korunmalı, din ve vicdanının getirdiği düşünceleri ifade etmesi veya dinini yaşaması için özel hayata saygı duyulmalıdır.

İfade özgürlüğü, klasik haklardan olan birinci kuşak haklardandır. Bu hakların en önemli özelliği daha önce Mahremiyet hakkını anlatırken ifade ettiğim gibi bireyi koruması ve devleti sınırlandıran negatif statü haklarındandır. Bu haklar kişinin devlet, toplum ve üçüncü kişilerin dokunamayacağı özel alan yaratır (Fırat, 2015:105).

"İnternette ifade özgürlüğü" kavramı yeni çıkmış bir özgürlük değildir. Mevcut olan bir insan hakkının yeni bir mecrada genişlemesi anlamına gelir. Aynı durum aslında internette anonim olma hakkında, toplantı yapma ve dernek kurma özgürlüğü veya eğitim hakkı gibi özgürlüklerin internette kullanılması ve gerçekleştirilmesi için de geçerlidir (Benedek ve Kettemann, 2013:166).

İnternet mecrası yeni olsa da insan hakları tarihsel olarak çok eskiye gitmektedir. Bu açıdan düşünüldüğünde dahi insan haklarının yeni bir mecrada sürdürülmesi gerekmektedir. Ayrıca gelişerek devam eden insan hakları tarihi, teknolojinin insanlar arasında yaygınlaşması ile farklı bir şekilde kendini geliştirmek zorundadır. Artık insan hakları sadece fiziksel olarak insan hakkı ihlal edilmemekte, internet ve sanal ortamda da insan hakları ihlal edilebilmektedir. Bu sebeple insan hakkı ihlallerinin önlenmesi için gerekli düzenlemeler interneti de kapsayacak şekilde yapılmalıdır.

Türkiye de internet alanında insan hakları ihlallerinin önlenmesi için etkin bir kurumsallaşma yapılması gereklidir. Bunun yapılması için Dünya ülkelerinden örnek alınmalı, Dünya da bu alan iyi takip edilip düzenlemeler bu çerçevede yapmalıdır. Siber dünyada en büyük problemlerden biri saldırının kaynağının ve kim tarafından gerçekleştiği meselesini aydınlatmaktır. Saldırganın bulunması insan haklarının önlenmesi açısından da önem taşımaktadır.

Siber güvenlik uyumluluğu oluşturulma adımları şu şekilde izlenebilir:

1.Uyum ekibi geliştirme: Burada organizasyonun büyük veya küçüklüğüne bakılmaksızın IT departmanı veya siber alanda çalışacak ekip ve takımlar oluşturulmalıdır.

2.Risk analizi belirlemek veya oluşturmak: Bunu yaparken tüm bilgi sistemlerini, varlıkların, ağların ve veri erişimlerinin tanımlamaları kontrol edilmelidir. Erişilebilen, saklanan ve toplanan yüksek riskli bilgilerin belirlenip tüm seviyelerde risk analizi yapılması gerekmektedir. Riskler belirlendikten sonra da riskler formüle edilerek düzenlenmelidir. Daha sonra da risklere nasıl önlem alınacağı ve neler yapılabileceği belirlenmelidir. Özellikle riskin sürüp sürmediği takip edilmeli ve bazılarının reddedilmesi sağlamak gerekmektedir.

3. Düzenli kontroller: Güçlü parola ve şifre politikaları, Güvenlik duvarlarının (Firewall)düzenlenmesi, iki faktörlü kimlik doğrulama koruması, sigorta, çalışanların eğitimi gibi konularda analiz edilen riske dayalı olarak risk denetleyicisi kurma ihtiyacı karşılanmalıdır.

4.Politikalar Oluşturmak: Faaliyetlerin ve yapılan kontrollerin uyumluluğunu kontrol eden ve bunlardan haberdar olan politika belgeleri veya yol haritası oluşturulur.

5. İzleme ve cevap verme: Zaman zaman tüm uyum programı izlenmeli, tehditler ve her türlü güvenlik açıklarıyla başa çıkmanın yeni yolları araştırılıp bulunmalıdır (Meharanjunisa, 2020: 5).

İnternet üzerinde en önemli suç kategorilerinden biri sanal ortamda işlenen çocuk istismarı suçu olup teknolojik gelişmeler arttıkça çocuk istismarı da internette yaygınlaşmıştır. Ayrıca bu suç emniyet kayıtlarında "çevrimiçi çocuk istismarı" olarak adlandırılmıştır. Çocuklara yönelik istismar konusunu ele alan araştırmalar tıp alanında yoğunlaştığı görülürken sosyal bilimlerde özellikle "çevrimiçi çocuk istismarı" konusunda eksiklik görülmektedir (Çalışkan, 2019: 122-123).

Çevrimiçi çocuk istismarı suçunun işlenmeden önlenmesi amacıyla şu gibi önlemler alınabilir:

1. Bir çocuk odasına uyumak amacıyla gittiğinde sanal ortamla iletişim kurabileceği telefonu var ise sanal kullanıcıların olduğunu ve yalnız olmadığı bilinciyle telefonları ile birlikte odaya gitmemeleri gerektiği konusunda anlaşma yapılması faydalı olacaktır.
2. Sanal tehditlere karşılık evde ortak telefon kullanma alışkanlığı geliştirmek ve aile bireyleriyle ortak karar alınma yararlı olabilecektir.
3. Çocuğun girebileceği web siteleri hakkında anlaşmaya varılması yararlı olacaktır.
4. Çocuğun girebileceği web sitelerinin yaşına uygunluğuna bakılmalı ve zararlı içerikleri olan web sitelerinden koruma sağlayan filtre programlar veya yazılımlar kullanılmalıdır.
5. Eğitim amaçlı olarak internet kullanılmalı, vakit geçirmek veya oyalayıcı aktivite olarak kullanımı azaltılmalıdır.
6. Çocukların internette arkadaşlık kurduğu çocuklar veya kişilerde yaş farkı gözetilmelidir. Ayrıca çocuk sosyal medya kullanıyorsa fiziki çevrede bilinen teyit edilebilir kişiler olmasına dikkat edilmelidir.
7. Çocukların kişisel ve şahsi bilgilerinin kendine özel olduklarının bilincine vardırılması gerekmektedir.
8. Çocuklara sanal ortamda istenmeyen ve kötü bir olay veya durumla karşılaştıklarında ebeveynlerine anlatmaları ifade edilip onları suçlayıp kötülememeli ve çocuklara güvence verilmelidir.
9. Çocuğun internet kullanımı fiziki çevreden çok koparıyor hale geldiyse profesyonel yardım olarak uzmana başvurulması gerekmektedir.
10. İstismar konusundan şüphe duyulması halinde eldeki bilgiler ile güvenlik güçleri ile paylaşılmalı ve gerekli yardımlar alınmalıdır (Çalışkan, 2019: 129-130).

Son olarak devletlerin genel hatları ile siber hukuk anlamında yapabilecekleri ve yapması gerekli noktaları genel hatları ile maddeler halinde özet olarak belirtecek olursak:

-Her devlet kendi yasalarında geçen siber suçları güncellemeli ve mevcut yasalarını değiştirmesi gerekmektedir. Teknik bilgi ve teknolojiler geliştiği için suçlar da değişkenlik göstermekte, mağduriyet tipi ve oranları artabilmektedir.

-Devletler küresel oydaşma veya konsesüs sağlayarak bir hukuk sistemi oluşturmalılar. Bu mümkün gözükmüyor ise ikili veya çok taraflı anlaşmalar yaparak siber suçlara yaptırım konusunda mutabakat yapmaları gerekmektedir.

-Uluslararası örgütler, özel şirketler ve hükümet dışı kuruluşların da üzerine düşeni yapması için devletlerin politika geliştirmeleri gerekmektedir.

-Devletler savaş hukukunu ve insan hakları hukukunu geliştirmişken siber hukuk anlamında temel etik ilkeler geliştirmeli ve bunu yazılı hale dökmeleri gerekmektedir.

3.2: Uluslararası Siber Hukuk: Küresel ve Bölgesel Mekanizmalar

Uluslararası ilişkiler literatüründe ortak bir siber tanımı olmadığı gibi, ortak bir siber hukuk da bulunmamaktadır. Bölgesel olarak NATO ve Avrupa Konseyi gibi bazı kurumlar sınırlı olsa dahi işbirliği ve/veya anlaşmalar geliştirme başarısı gösterseler dahi, Birleşmiş Milletler nezdinde küresel düzeyde herhangi bir anlaşma yapılamamıştır (Akyeşilmen,2018: 60-61).

NATO 2008 yılında Bükreş Zirvesi sonrasında yayınladığı bildirge ile üye ülkelerin siber saldırılara karşı güçlendirilmesi kararlığı vurgusu yapmıştır. NATO'nun siber güvenlik politikasının savunma olduğu, tecrübe paylaşımı ve birbirlerine yardım konuları vurgulanmıştır. Zirve sonrası gelişmelere bakılırsa NATO Siber Savunma Yönetimi Otoritesi'nin Brüksel'de kurulması kararı ve Estonya'da bulunan Tallinn merkezli Siber Savunma İşbirliği Mükemmeliyet Merkezi kurulması dikkat çekicidir (Bıçakçı, 2014: 121).

Karadeniz Havzası'ndaki kıyı ülkeler için çok büyük bir kriz olmasa da her şeyin yolunda da denilemez. Rusya'nın yapmış olduğu Gürcistan'a ve Estonya'ya yapmış olduğu siber saldırılar, diğer Karadeniz'e yakın devletleri tedirgin etmiş olup bölgesel işbirliğini de zedelemiştir. Bu saldırılar sonrası Karadeniz ülkelerinin çoğu harekete geçmiş olup siber alanda gerçekleştirilen istihbarat operasyonları yapma ve böyle yapılan operasyonlara karşı koyabilme çarelerini ve yollarını araştırmaya başlamışlardır (Güntay, 2015: 481-483).

Akdeniz bağlamında kıyısı olan ülkeler açısından bakıldığında stratejik önem itibariyle yük ve ticari gemilerin geçiş noktalarını barındırmaktadır. Doğu Akdeniz bölgesini ele alacak olursak bazı NATO ülkelerine üye devletlerin kıyısı olmakla birlikte uluslararası çıkar gruplarının, özellikle kıtasal ve küresel güçlerin menfaatlerinin kesiştiği bir bölgedir (Güntay, 2015: 481-483).

NATO'nun Siber Savunma Mükemmeliyet Merkezi adında ve Belçika'da Siber Uzay Operasyon Merkezi adında yapılar kurarak üyelerinin siber savunma programlarını geliştirmeye çalışmıştır. Bunu yaparken ulusal, ikili ve çok yapılı bir savunma birlikteliği kurarak siber savunma çalışmaları ve eğitimleri yapmıştır. İttifak üyeleri bölgelerinde kontrollerini arttırabilmeleri için eğitim ve çalışma yapmaları sağlanmakla birlikte operasyonlar ve taktikler geliştirerek NATO'nun da siber güvenliğine katkı sağlayacak bir ortam bulmuşlardır (Efthymiopoulos, 2019:8).

NATO'nun siber savunma politikasının neler olduğu temelinde Mart 2011 tarihinde NATO Siber Savunma Konsepti ile oluşmuştur. Bu politikalar genel olarak şunlardır:

a. NATO'nun ana görevleri olan kolektif savunma ve kriz durumlarının yönetimini yapmak için NATO plan süreçlerine siber savunma hususları dâhil edilecek,
b. NATO ve üye devletler için kritik siber alt yapıların korunması ve savunulmasına çalışılacak,
c. Güçlü bir siber savunma oluşturulmaya çalışılacak ve bu sağlanırken NATO'nun ağlarının korunması merkezileştirilecek
d. Üye devletlerin kritik altyapılarının açıklarını kapatmak ve eksikliklerini gidermek için Müttefiklere yardım edilecek,
e. Müttefik ülkeler, uluslararası kuruluşlar, özel şirketler ve akademik çevreler birlikte çalışacaklar,
f. Siber savunma gereksinimlerinin tespit edilmesi ve eksikliklerin giderilmesi sağlanacak (NATO Defence Planning Process yoluyla yapılacak)
g. Siber farkındalık geliştirilecek olup özellikle NATO tatbikatlarına siber bileşkeler eklenecek
h. NATO ve üye müttefik ülkeler Tallin'deki Kooperatif Siber Savunma Mükemmelliyet Merkezi'nden uzmanlık ve teknik destek alacaklar (Defending the networks, The NATO Policy on Cyber Defence 2011).

Akdeniz de siber anlamda alt yapıların güvenliği, petrol boru hatlarının ve istasyonlarının güvenliği ve gemi geçişlerinde taşıtların güvenliği dikkat çekici konulardandır. Bu sebeple gelişen teknolojide bölgenin siber anlamda güvenliği de önem arz etmektedir. Özellikle Akdeniz'e kıyısı olan Avrupa Birliği üyesi ülkelerin sayısı fazladır. Avrupa Birliği'nin siber güvenlik politikaları incelendiğinde ciddi çalışmaların olduğu görülecektir.

Kurumsallaşma çalışmalarına örnek olarak 5 Haziran 2003 tarihinde Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA) kurulma kararı alınması sonrasında 14 Mart 2004 tarihinde fiilen kurulmuştur. Amaç olarak Avrupa Birliği ülkelerinin siber güvenliğinin sağlanması için koordinasyon yapması amaçlanmaktaydı. Kurulduğundan beri bir bilgi akış merkezi de olmuştur (Eren, 2017: 73).

Avrupa Birliği'nde üye ülkelerin bazıları özgürlük alanlarına müdahale olarak gördüklerinden çatı kuruluşlara önyargılı yaklaşmaktalar. ENISA kurumuna böyle önyargılı mı yaklaşmışlar uygulamalara ve örneklere bakmak gerekmektedir.

ENISA, Avrupa Birliği üye ülkeleri enerji ve ulaşım altyapısında devletlerin siber direnç kapasitesini geliştirmek için çalışmalar yapmıştır. Bu çerçevede 2013 yılında Avrupa Birliği için "Endüstriyel Kontrol Sistemleri ve Bilgisayar Güvenliği Olaylarına Müdahale Birimi (ICS-CSIRTs)" kurulmuştur. Böylece Avrupa dışından gelebilecek tehditlere ve saldırılara karşı siber güvenliğin sağlanması için aktif rol almıştır. Avrupa Birliğince bu yeterli görülmemiş olup ulus devletlerinde politikalarını kapsayacak yasal düzenlemelerin olması gerektiği görülmüştür. Ulusal otoriteleri kapsayacak şekilde 2012 yılında Brüksel'de CERT (Bilgisayar Acil Müdahale ekibi) oluşturulmuştur. AB kurumlarındaki problemlerle ilgilenmesi için de CERT-EU olacak şekilde ayrı bir mekanizmada yapılmıştır. Bu CERT ve CERT-EU ile olası kriz durumu ve olaylarda AB ve üye devletlere etkili bir ağ ve bilgi güvenliği politikası oluşturmaktır (Eren, 2017: 74 ve 78).

Avrupa Birliği acil müdahaleler konusunda stratejiler belirlemiş, ekipler ve mekanizmalar kurmuştur. Diğer devletlerde örnek alacak şekilde gerekli tedbirleri ve düzenlemeleri yapabilmelidir. İnsan hakları ihlallerinin önlenmesinde devletler yeterli olmayabilir. Bu sebeple uluslararası kuruluşların, kurumların, devletlerin katkı sunacağı küresel çatı bir yürütme organına ihtiyaç vardır. Aksi halde her devlet veya kurum kendi alacağı kararlar ile insan haklarına ne kadar saygı duyacağı merak ve tartışma konusudur.

Uluslararası kuruluşlar denildiğinde ilk dikkat çekilenleri çokuluslu şirketlerdir. Çok uluslu şirketler ve kendi ülke hükümetleri olan ilişkileri çoğu zaman çıkar çatışmaları ile tartışılsa da çoğu zaman ev sahibi ülkenin ekonomik gücünü arttırmışlardır.

Çok uluslu şirketin basit tanımı; iki veya daha fazla ülkede ekonomik birimi olan ve veya bu birimleri yöneten firma şeklindedir. Bu firmalar çoğu zaman çeşitli ülkelerdeki firmalara doğrudan yatırım yaparlar. Bu yatırımlar uluslararası işlemler anlamına geleceğinden liberalizmle uyumlu olup ekonomik milliyetçilik veya ekonomiye müdahale eden sistemlere karşıdır (Gilpin, 2011:283-284).

Bir Çokuluslu Şirketin doğası gereği üretim yaparken dünya pazarlarına en düşük maliyetli ürün sağlamaktır. Diğer ülkelerde üretimin yardımcı kuruluşları olsa da tepe yönetimi bir ülkededir. Bu şirketler eşgüdümlü bir küresel strateji ile yönetilirler. IBM, Exxcon, General Motors, Mitsui, Toyota, Fiat ve Nestle en bilinen örnekleridir (Gilpin, 2011:285).

Amerikan çok uluslu şirketleri bazı durumlarda Amerikan hükümetince diğer hükümetleri kendi emirlerine uymaya zorlamada kullanıldığı da olmuştur. Örnek vermek gerekirse Henry Kissinger döneminde ticaret ve yatırımlar ile Rusya ile dış dünya arasında bağımlılık yaratarak Sovyet davranışlarını dönüştürmeyi hedeflemiştir (Gilpin, 2011:297).

Uluslararası ilişkilerde sadece devletlerin değil çok uluslu şirketlerin, hükümet dışı kuruluşların da gücü yadsınamaz. Bu sebeple uluslararası kuruluşların siber hukuka katkısı elzemdir. Örnek olarak Facebook milyonlarca kullanıcı olan bir şirkettir. Siber suçlarda devletler ile iş birliği yapması ve elindeki kanıt veya bilgileri paylaşma anlamında suçluların yakalanması ve suçların aydınlatılmasında tabiri yerinde ise "elini taşın altına koyması" beklenir.

Hem devlet hem özel sektör, izleme ve gözetleme araçlarının kullanımını arttırmaktadır. Bu anlamda insanların mahremiyet hakkının gözetilmesi için devletin ek düzenlemeler yapması gerekmektedir. Ayrıca Devletin yanında devletin gerekli düzenlemelere yapıp yapmadığını denetleyen veya takip edecek özel kuruluş veya uluslararası kurumların da denetleme yapması gereklidir.

İnsan haklarını dijital çağda korumak için sadece devletlerin değil, bireylerin ve özel şirketler üzerinde bağlayıcı olacak uluslararası bir düzene ve uluslararası anlaşmalara ihtiyaç vardır. Kısaca anarşik uluslararası düzenin doğasının üstüne çıkacak küresel bir yürütme organına ihtiyaç vardır. Siber uzay sınırsız, paydaşı çok olan, mesafelere sığmayan ve anarşik

yapısıyla insan haklarının bir aktörce korunmasını imkânsız kılmaktadır. Siber uzayın tüm paydaşlarını içerecek kapsayıcı bir yaklaşım benimsenirse insan hakları korunabilecektir. Bu uluslararası hukukta yeni öznelerin çıkmasına, devletin egemenliğinin sorgulanmasına yol açacaktır (Akyeşilmen,2018:304-305).

Devletler Meclisi fikri birçok yazar tarafından (Dubois, Cruce, Sully, Sain-Pierre) dile getirilmiştir. Fakat Jeremy Bentham, devletlerarası ilişkilerin düzenlenmesinde cezalandırıcı güçten vazgeçilmesi gerekir. Herhangi bir zorlayıcı güç olmadan insan aklına tabi bir Devletler Meclisinin, en güçlü yaptırımlarının "kamuoyu mahkemesi" olduğunu savunarak daha adil ve makul olabileceğini savunur (Knutsen, 2006: 206).

Bentham, "Uluslararası hukuk" kavramını icat etmiş olup ülkelerin kendi arasında kullanacakları kanunlar ile kendi egemenliği içinde kullanacağı kanunlar arasında ayrıma gitmiştir. Devletler Meclisi veya Devletler Mahkemesi gibi bir oluşum kurmaktaki mantık ise dünya ekonomisinin doğal yasa ilkesiyle yürütülmesi olup serbest ticaretin, sömürge ve korumacı uygulamaların olmamasıdır (Knutsen, 2006: 207).

İnsan haklarına etkin güvence sağlama hedefi ve arzusu İkinci Dünya Savaşından beri sürmüş olup uluslararası mecrada insan haklarının korunması amacıyla kurumlar ve mekanizmalar çoğalmıştır. Bu gelişme devletlere pozitif yükümlülük getirmiş ve devletlerin yükümlülüklerinin yerine gelip gelmediğini denetleyen uluslararası mekanizmaların olması uluslararası hukukun gelişmesine katkıda bulunmuştur (Göçer, 2002: 19).

Tarihsel olarak insan haklarının korunması ile ilgili kurallar antlaşmalarda yer almış olup din özgürlüğü ile başlayıp dinsel azınlıkların korunması ile gelişmiş özellikle Birinci Dünya Savaşı sonrası azınlıkların korunması ile ilgili antlaşmalar artmıştır. İnsan haklarının uluslararası bir boyut kazanımı BM Şartının ile olmuş, uluslararası anlamda insan haklarının korunması ile ilgili antlaşmalar artmıştır (Göçer, 2002: 25-26).

Devletlerin uluslararası ilişkilerde sorumluluk atfedebilmek için iki koşulun bulunması gerekmektedir. Bunların biri uluslararası hukuk uyarınca bir yükümlülüğün ihlali diğeri ise bu yükümlülüğü ihlal eden eylemin o devlete yüklenebilmesidir (Şafak, 2020: 141).

Tespit ve ilişkilendirme olayı siber uzayda çok zor olmaktadır. Siber saldırıları düzenleyenlerin kimlikleri (identity), yerleri (location) ve aracıları(intermediary) belirlenerek ilişkilendirme yapılabilmektedir. Profesyonel saldırganlar için birçok gizlenme ve yanıltma araçları varken tespit edilmesi güçleşmektedir. Eğer saldırılan kurum/şirket içinde bir bağlantı (insider) olduğu takdirde soruşturmalar daha kesin neticeler verebilmektedir (Şafak, 2020: 142).

Uluslararası hukukta "jus ad bellum" olarak bilinen silahlı kuvvet kullanma veya başvurma haklılığını ifade ederken "jus in bello" olarak ifade edilen kavramla da silahlı çatışmada uygulanan hukuka uygun yöntem ve araç kullanımı kurallarını ifade etmektedir. BM 3314 Sayılı kararı madde 1 de genel olarak saldırı tanımlanmış ve kararın 3. Maddesinde saldırı örnekleri sayılmıştır. Özellikle 1.madde de "…Birleşmiş Milletler Antlaşması ile bağdaşmayan diğer herhangi bir tarzda silahlı kuvvet kullanılmasıdır" ifadesiyle "herhangi bir" tarz denilerek siber saldırılar da kast edilebilir. Özellikle fiziki olmasa da ciddi somut zararlara sokan siber saldırılar da bir silah gibi eş değere sahip kabul edilebilir. 2010 yılında ABD'nin İran'a yapmış olduğu nükleer tesislere yapılan siber saldırılar ciddi zararlar vermiştir (Şafak, 2020: 144-145).

Siber saldırılar önlem alınmazsa çok büyük zararlara sebep olabilmektedir. Doğalgaz hatlarına sabotaj düzenlenerek bir ülkeyi hem ekonomik hem de binlerce kişiyi mağdur edebilir. Nükleer sistemlerine zarar vererek işlemez duruma getirebilir veya büyük çevresel felaketlere sebep olabilir. Hava trafiği veya deniz seferleri aksatılarak binlerce kişi mağdur edilebilir. Askeri cihaz veya silahlara siber saldırılar düzenlenerek imha edilebilir veya kendi vatandaşlarına karşı terör eylemi gerçekleştirilebilir. Özellikle bankalara siber saldırılar düzenlenerek ciddi ekonomik zararlara sebebiyet verilebilir. Örnekler çoğaltılabilir. Bu sebeple devletlerin hem gerekli tedbirleri alması hem de uluslararası hukukun getirdiği sorumluluklara uygun davranması gerekmektedir.

Uluslararası sistemde hâkim olan anarşik doğada devletler saldırı yaptığında saldırı yapan belirli olup gerektiği durumlarda yargı organlarında sorumluluk doğabilmekteydi. Ancak siber dünyada saldırının kaynağının belirlenememesi veya kim-hangi devlet tarafından yapıldığının bilinmemesi sebepleriyle devletler siber güvenlik alanına yatırım yapmak zorundadırlar.

Siber savaş, siber saldırı, siber terörizm gibi kavramlar uluslararası hukuk nezdinde kabul görmesi, konu hakkında çalışmalar ve makalelere ihtiyaç duyulmaktadır. Ayrıca Birleşmiş Milletler nezdinde yeni düzenlemelere ve kuralların oluşturulmasına ihtiyaç duyulmaktadır. Kurallar konulurken siber saldırı ve savaş tanımları yapılması haricinde nasıl yaptırımların uygulanacağı da belirtilmelidir.

Uluslararası Adalet Divanı, Uluslararası Ceza Mahkemesi, AHİM veya Avrupa Birliği Adalet Divanı ve diğer uluslararası yargı divanlarında siber saldırı suçunu işlemiş devletler hakkında ve hatta devlet görevlileri hakkında yargılamalar yapılmalıdır. Hüküm verildiği takdirde devletler çıkan sonuca ve yaptırımlara uluslararası hukukun getirdiği sorumluluk gereği uymalıdırlar.

3.3. Siber Zorbalık ve Zorbalık Karşıtı Politikalar Oluşturulması

Zorbalık aslında fiziki olarak bir anlam ifade etse de ilişkilerin internet mecrasına taşınması ile birlikte zorbalığın sanal boyutu da ortaya çıkmıştır. Sanal olarak işlenen suçlarda artış olmuştur. Dünya genelinde bilişim, internet veya siber suçlar olarak adlandırılan suçların işlenme oranlarının çok olması sebebiyle bu suçların mağdurları da fazladır. Mağdurlar arasında özel şahıslarla birlikte özel ve kamu tüzel kişileri de bulunabilmektedir.

Siber zorbalık olarak literatürde çok çeşitli tanımlamalar vardır (Tablo3.1 de olduğu gibi). Ortaklaşmış bir tanım olmamakla birlikte teknoloji aracı kılınarak gerçekleştirilmesi ve zorbalık veya zarar verici rahatsız eylemler olmasında ortaklaşmış olduğu görülebilir.

Siber zorbalığa ilişkin yapılan akademik çalışmalarda geleneksel akran zorbalığından ayıran özelliklerin belirlenmesi çabası vardır. Akran zorbalığı genel olarak güçlü bir öğrencinin güçsüz bir öğrenciye şiddet uygulaması ve acı çektirmesi olarak tanımlanabilir. Tamda bu tanımdan yola çıkarak siber zorbalık tanımlanacak olursa siber zorbalık, teknolojik bilgi gerektirerek ve teknolojik bilgi kullanılarak akıllı telefon uygulamaları, e-posta, SMS, sohbet odaları, forumlar, bloglar ve diğer sosyal ağlarda mağdur etmesidir (Sayımer ve Akça, 2017:4).

Normal bir şaka veya oyun oynama sırasında çocukların birbiri arasında uğraşma ve davranışları rahatsız edici boyutlara gelebilmektedir. Özellikle çocuklar birbirlerine karşı acımasız davranabilmektedir. Fiziki yapılan şakalar internet mecrasına taşınması ile siber

zorbalık yapılabilmektedir. Bunun için aileler ve öğretmenler şakaların büyütülmemesi ve rahatsız edici davranışların sürdürülmemesi için gerekli eğitimleri çocuklara vermesi gerekmektedir. "Dört göz", "cüce", "şişko", "çirkin", "fakir", "tembel", "git buradan", "bizimle oynayamazsın" gibi sözlere ve davranışlara izin verilmemesi, isimlerine lakap takılmaması ve laf atmalara izin verilmemesi gerekmektedir.

Siber zorbalığı akran zorbalığından daha çok tercih edilen ve yaygın olmasının en büyük sebeplerinden birisi yüz yüze olmaması ve sanal ortamda gerçekleşmesidir. Özellikle failin veya şüphelinin takma hesap-anonim hesap ya da sahte hesap kullanılarak yapılması ve gerçek kimliğin gizlenmesi zorbalık yapmayı kolaylaştırmaktadır. Durum böyle iken mağdur ve mağdurun çevresine etkisi çok büyük olabilmektedir. Failin kimliğinin tespitinin zor olması mağdurun psikolojik şiddete daha fazla mazur kalmasına sebep olmaktadır.

Siber zorbalığın akran zorbalığından en büyük ve dikkat çekici farklarından birisi de sürekliliğidir. Akran zorbalığında fiziksel şiddet anlık veya zincirleme işlense bile siber zorbalık kadar uzun süreli olmayabilmektedir. Siber zorbalıkta teknolojinin gelişmesi ve dijital çoğaltımın kolaylıkla olabilmesi sebepleriyle mağduriyet süreklilik arz edebilmektedir.

Siber zorbalığın yapılma nedenleri arasında kimliğin bilinmemesi ve kullanıcı adlarının arkasına saklanması, saldırganın sonuçlarını görmemesi, popülerlik, yaşadıklarından farklı hayatı yansıtma, özgüven düşüklüğü gibi sebepler yer almaktadır. Siber zorba ile saldırıya uğrayan mağdur arasında temas olmasa bile mağdur psikolojik zararlar görebilmektedir. Zorbalığa maruz kalan mağdurlarda hayata küsme, panik, korku, hayal kırıklığı, üzüntü, depresyon, utanç ve daha birçok olumsuzluk olmaktadır. Akran zorbalığı yapmış çocukların birçoğunun da siber zorbalık yaptıkları saptanmıştır. Akran zorbalığı yapanların genel olarak güçlü olan bir ergen-çocuğun güçsüz olan bir ergen-çocuğa yaptığı zorbaca davranışları ifade ederken siber zorbalıkta psikolojik, sosyal, akademik sorunlar olabilmektedir. Yeni iletişim teknolojileri faydayla birlikte yeni problemler getirmiştir. Bu problemlere karşı özellikle ebeveynler olarak anne-babalara ve herkese görevler düşmektedir (Korkmaz, 2016: 75 ve 77).

Bir çalışmada aile, arkadaş ve sosyal çevreden görülen destek düştükçe siber zorbalığa yönelim artmaktadır. Yani algılanan sosyal destek siber zorbalığı önlemede önemli bir değişkendir. Sonuçlardan dikkat çekici olan arkadaştan algılanan sosyal destek tam aracı olup,

öğretmenden algılanan destek ise kısmi aracı rol oynandığı belirtilmiştir (Peker ve Eroğlu, 2015: 772).

Siber zorbalık ile mücadele küçümsenmemeli ve kurumların ciddiyetle önlem almasında fayda vardır. Siber zorbalık ve siber suçlarda dikkat çekici olan bir tek hareket ile binlerce veya milyonlarca kişiyi mağdur olarak etkileyebilmesidir. Doğal olarak bu sebeple kanun uygulayıcılarının işini zorlaştırmaktadır. Özellikle bu tür suçlarda sınır aşma olgusu çok sık karşımıza çıkan bir durumdur. Bu nedenle mücadelesi zor ve devletlerarası iş birliğini de gerekli kılmaktadır.

Çocukların ve özellikle de okul çağındaki çocukların siber zorbalık vakalarında öğretmenlerine, okul yöneticilerine ve ailelerine paylaşım konusunda çekimser olduklarından önemli görevler düşmektedir. Çünkü çocuklar aile, okul ve arkadaş baskılarından dolayı zaten üzerinde baskı varken bir de siber zorba tarafından tehdit, şantaj ve diğer zorbalık türlerine maruz kalınca çok çeşitli sorunlar doğabilmektedir.

Siber zorbalık ile karşılaşıldığı durumlarda okul yöneticileri ilgili okul kural ve politikalarını belirlemeli ve şüpheli durumları polise bildirmelidir. Okul psikologları ve danışmanları, siber zorbalık ile ilgili farkındalık, önleme ve politika geliştirmeli okul, aile ve toplum arasında iş birliği sağlamalıdır (Aksaray, 2011: 426).

Tüm bu olumsuzluklara maruz kalmamak için sadece çocuklar değil her bir ferdin eleştirel medya okuryazarlığı ve bilgilerin kaynağını araştırarak bilinç düzeylerini ve kültürlerini arttırmaları gerekmektedir. Özellikle siber zorba olmasa bile bireyler fazla internet kullanımı ile kendilerine zarar verebilmektedir. Eğer gerekli önlemler alınmazsa ve bilinçlendirme yapılmazsa çocuklar çok kötü etkilenebilmektedir. Çünkü ebeveyn kontrolü olmazsa çocuklar kötü uygulamalara girebilir, oyunlar ile çok fazla zaman geçirebilir, pornografik içeriklere maruz kalabilir.

Yeni medya okuryazarlığı dersi çocukları geliştirecek ölçüde internetin olumlu-olumsuz yanlarını göstererek eğitimler verilmelidir. Bu konu da üniversiteler ile birlikte RTÜK, Bilgi Teknolojileri kurumu, ilgili bakanlıklar ve kurumlar aracılığıyla ortak uzaktan eğitim dahi verilebilir (Özmen, 2018: 965).

Siber zorbalık konusunda mücadele edebilmek için çok çeşitli ortaklık kurulması lazım veya ortak çalışmayı gerekli kılmaktadır. Bu sebeple siber yönetişim kavramını ortaya çıkarmıştır. Siber yönetişimin çok çeşitli tanımları vardır. Ancak hükümetlerin, özel sektörün ve sivil toplumun ortak çalışmasını gerekli kıldığı görülmektedir.

Siber yönetişim Almeida'ya göre, veri bütünlüğünü gerçekleştirmek için devlet ve uluslararası paydaşların sınır aşan faaliyetlerini ve davranışlarını düzenleyen formel ve in formel hukuki mekanizmalar, politikalar ve düzenlemeleri içermektedir (Akyeşilmen, 2018: 263).

Siber zorbalık ve diğer siber suçların cezasız kalmaması ve caydırıcı olabilmesi ciddi hukuki düzenlemelere ihtiyaç duyulmaktadır. Sadece devletin değil devletlerarası iş birliğini ve uluslararası kuruluşlarla iş birliğini gerekli kılmaktadır. Örnek vermek gerekirse ABD menşeli bir özel uluslararası kuruluştur. Facebook şirketinden herhangi bir bilgi talebi için sadece ABD devletinden değil Facebook şirketiyle yazışma yapılarak talep edilmesi gerekir. Siber suçlar ile mücadele için NGO'lar (Non-Government Organization) yani Hükümet dışı kuruluşlar ile ortak çalışmayı dahi gerekli kılmaktadır.

Çocuklar özellikle internet kullanma veya bilgisayar, cep telefonlarını kaybetme korkusuyla ailelerine siber zorbalığa maruz kalsalar bile söylemeyebiliyorlar. Buna birde yasakçı uygulamalar koyan aile bireyleri eklenirse çocuğun psikolojisi de bozulabilmektedir. Psikolojisi bozulan çocukların dersleri kötü olabiliyor veya aile, arkadaş ilişkileri bozulabilmektedir. Özellikle saldırgan davranışlar veya içe kapanık davranışların altında yatan sebepler siber zorbalık olabilmektedir. Siber zorbalık mağduriyetleri azaltılabilirse çocuklar daha sağlıklı eğitim ve daha iyi bir psikoloji ile yetişebilirler. Bunun için anne babalar çok dikkatli olup siber zorbalıkta yasaklayıcı tavır ve baskıcı tavırlardan kaçınmalıdırlar. Bunu yaparken psikolojik destek ve diğer ilgililerden destek almalıdırlar.

Türkiye'de siber zorbalık sonrası psikolojik destek verecek bir merkez kurulmuş değildir. Önleyici çalışma yürüten kurumlar, üniversiteler ve STK'ların görüşü alınarak böyle bir merkezin kurulması ciddi bir girişim olacaktır. Mağdurun desteklenmesi ve eski itibarının sağlanması için neler yapılabileceği konusunda merkez ve birimler olmalıdır. Böylece çok çeşitli kurumların yürüttüğü çalışmaların merkezde toplanması sağlanacaktır. (Akca, Sayımer, Salı ve Başak, 2014:28).

Zorbalık karşıtı politika (Anti-bully Policy) oluşturulması öğrencileri fiziksel ve psikolojik olarak güvende hissetmeleri açısından önemlidir. Okullar her öğrencisini kapsayacak şekilde bir eylem ve mücadele programı oluşturmalıdır. Zorbalıkla mücadele politikası oluşturma ve uygulamaya geçirirken taraflardan programa uyacakları yönünde yazılı belgenin alınması tarafların mücadeleyi ciddiye almalarını sağlayacaktır (Yaman & Eroğlu & Peker, 2011: 215).

Ebeveynler zorbalık karşısında çocuklarını eğitmeli ve siber güvenlik konusunda eğitim vermesi gerekmektedir. Özellikle kendisine sanal ortamda kötü davranan, aşağılayan, tehdit ve küfür kullanan profilleri engellemesi gerektiği, nasıl engelleyeceğini, suç ile karşılaştığında delilleri nasıl edinip saklayabileceği konusunda, gerekli yerlere şikâyet edilmesi konusunda ve özellikle kişisel profil hesabını gizli tutarak tanımadığı hesapların arkadaşlık isteği ve/veya mesaj isteklerini reddetmesi gerektiği konusunda eğitim ve bilinç verilmelidir.

Psikolojik Etkileri	Sosyal Etkileri	Akademik Etkileri
Üzüntülü olma	Öz saygının düşmesi	Okula gitmekten korkma
Yoğun bir stres yaşama	Akran ilişkilerinde çatışma	Öğrenmede sorun yaşama
Kendini değersiz hissetme	Başkalarına güvenmeme	Okuldan kaçma
Kendisi hakkındaki bilgilerin öğrenilmesinden utanma	Arkadaşlık ilişkisi kurmada güçlük yaşama	Ders başarısının düşmesi

Tablo 3.5: Siber Zorbalığa Maruz Kalmanın Psikolojik, Sosyal ve Akademik Etkileri (Yaman & Eroğlu & Peker, 2011: 192).

Sosyal medyada kişisel profil hesapların herkesin görebileceği şekilde açık olmaması ve özel resimlerin paylaşılmaması konusunda çocuklarla birlikte ebeveynlere de verilmesi gerekmektedir. Özel montaj programları veya fotoğraf düzenleme araçları ile asıllarından çok farklı içeriklere sahip fotoğrafların şantaj veya aşağılama amaçlı kullanılabileceği unutulmaması gerekmektedir.

İnterneti güvenli kullanım ve işlevsel kullanım çok değerli kabiliyetlerdir. Kendi kendine bilgisayardan videolar veya sitelerden dil öğrenenler, yararlı ve kişisel becerileri geliştirenler azımsanmayacak kadar vardır. Bilgi kaynakları doğru kullanılıp sağlıklı ve sınırlı kullanım yapılmalıdır.

Siber Zorbalığa maruz kalan veya Çocuklara Öneriler	Ailelere Öneriler	Kurumlara Öneriler
Siber zorbalığa mağdur kalan öğrencilerin öz saygıları düşük olacağından kendilerine güvenmeli ve olumsuzlukları unutma ve tedbir almaya yönlenmelidirler	Siber zorbalığa mağdur kalan çocuklarına destek olmalı ve onlara güvenmeliler, onları suçlamamalılar ve bir daha olmaması için tedbir almalılar.	Devletin eğitim kurumları başta olmak üzere müfredat ve konularına siber farkındalık konusunda dersler ve eğitici bilgilendirmeler konulmalıdır.
Her anı ve durumu sosyal medyada paylaşmamak gerekmektedir	Aileler çocuklarına disiplin etmeye çalışırken cezalandırma yaparken kesinlikle şiddete başvurmamalıdır	Devletin çocuk istismarı veya akran zorbalığına karşı sosyal bilinçlendirme ve reklam yaparak duyurular yapması gerekir.(Çocuk susar, sen susma gibi söylemler)
Siber zorbalığa mağdur kalan kişiler mutsuz olmamalı ve hayattan kopmamalılar	Siber zorbalığa mağdur kalan çocuklarını mutlu etmeli ve mutsuzluktan kurtulmalarına yardım etmeliler	Siber zorbalık ve siber suçların işlenmemesi için gerekli tedbirlerin alınması ve başvuru mercilerin kolaylaştırıcı ve etkin mücadele için eğitimi ve desteklenmesi
Siber zorbalığa mağdur kalan kişilerin arkadaşlık ilişkileri zedelenmiş olabilir, yeni arkadaşlar edinmeli ve çevresiyle olumlu ilişkiler geliştirmeliler	Siber zorbalığa mağdur kalan çocuklarının yeni arkadaşlar edinmesine yardım etmeli ve çevresiyle olumlu ilişkiler geliştirmesi için çaba sarf etmeliler	Öğretmenlerin siber zorbalık konusunda eğitilmesi ve öğrencileri ile empati kurmaları ve yardımcı olmaları sağlanmalıdır
Madde/Alkol/Sigaraya başlama eğilimi içine girmemeliler	Madde/Alkol/Sigaraya başlama eğilimi içine girmesine izin vermeliler	Okul çevrelerinde gereken güvenlik tedbirleri alınmalı ve öğrencilerin Madde/Alkol/Sigaraya başlama eğilimi içine girmesine izin vermeliler veya gördüklerinde müdahale etmeliler
Duygusal ve psikolojik olarak kendilerini yenilemeliler	Özellikle ailelerin duygusal ve psikolojik olarak çocuklarının yanında olmalı ve bunu çocuklarına da hissettirmeliler, çocuklarına gereken ilgi ve sevgiyi göstermeliler	Gerek okul yöneticiler gerek Gençlik ve Spor Bakanlığı öncülüğünde spor ve yararlı aktiviteler yapmaları konusunda yardımcı olunmalıdır
Akademik ve okul hayatlarına önem vermemeliler	Akademik ve okul hayatlarına önem vermeleri konusunda yardımcı olunmalıdır	Zorbalıkla mücadele programı gibi bir süreç oluşturup uygulanması gerekmektedir.
Spor ve yararlı aktiviteler yapmalılar	Spor ve yararlı aktiviteler yapmaları konusunda yardımcı olunmalıdır	İnternet güvenliğine ilişkin gerekli yasal düzenlemeler yapılmalı ve suçlarla etkin mücadele

		edilmelidir.
İntikam alma duygusu önlenmelidir	İntikam alma duygusu önlenmelidir	Dünyadaki yasal düzenlemeler takip edilmeli
İnternette filtre programlar kullanmalıdırlar	Çocuklarına örnek olmalılar	Siber suçlarda caydırıcılık arttırılmalı ve yaptırımların miktarında arttırılma yapılmalıdır
İnternetten zorba kişiler veya yabancı kişilerle mesajlaşıp görüşmemeliler	Çocuklarının filtre programlar kullandığına emin olmalılar	Siber önlemlerin alınması için yardım mekanizmaları ve mercilerin oluşturulması
İnterneti bilinçli kullanmalılar ve zaman kontrolü, içerik kontrolü yapmalı ve küçük düşürücü eylem, davranış ve isteklerden kaçınmalıdırlar	Nasıl ki küçük çocuklara kaybolma eğitimi verilmesi ihmal edilmemesi gerekiyorsa internette çocukların kimlerden yardım alabileceği konusunda eğitim verilmeli (3. Kişilere güvenmemeyi öğretmeliyiz)	İhbar web ve internet mecrasında ihbar ve şikâyetlerin değerlendirilip işlem yapılan mecraların daha aktif kullanılması gerçekleştirilmelidir.

Tablo 3.6: Siber Zorbalığa maruz kalan veya Çocuklara Öneriler, Ailelere Öneriler ve Kurumlara Öneriler

4. SİBER SALDIRI

4.1: Siber Saldırıların Anatomisi

Siber saldırılara karşı güvenliği sağlamak için öncelikle siber saldırının anatomisinin bilinmesi gerekmektedir. Saldırı bilinmesi gerekir ki önlem alınabilsin. Saldırıya karşı savunma gücü arttırılması için teknik olarak hazır olmak şarttır. Saldırganların genel olarak yaptıkları belli başlı ortak çalışmalar vardır. Bunun en bilinen yöntemi ve ilk aşaması Bilgi toplamaktır. Özellikle internette açık kaynaklarda edinilin en ufak bir bilgi dahi saldırgan için önemli olabilmektedir. Bu bilgiyi kullanarak başka bilgilere ulaşmak kolay başvurulan yollardan olup maliyeti yoktur.

Terörist örgütler tarafından siber faaliyetlerle eylem yapma çekici bulunur. Geleneksel terörist metotlardan az maliyetli oluşu, silah ya da patlayıcı temin etmek zorunda olmayışı, saldırganın kimliğinin gizlenebilir oluşu, özellikle hedef seçilebilecek noktaların (silahlı kuvvetler, kuruluşlar) fazla oluşu ve uzaktan kumanda edilebilir olması gibi sebepleriyle çekici olur (TASAM, 2004: 5-6).

Saldırgan açık arayarak sistem hakkında yeterli düzeyde bilgiye sahip olduğunda sistemin açıkları hakkında bilgi toplamak amacıyla tekrar internet araştırmasıyla bu iş için kurulan site ve formları tarayacaktır. Gereken bilgiye ulaştığında test saldırıları yapmaktan çekinilmez ve hedefine ulaşana kadar çalışılır.

Saldırıda bulunan bir cracker (çökertici) hedef makinedeki loğlarını (sunucuların oluşturduğu günlük kayıtlar ve dijital hareketlerin kayıt edilmesi) da inceleyerek hedef tarafta saldırı ile ilgili kayıtları anlayabilir ve bu izleri bilir. Her sistemin değişik "logging" işlemleri olmaktadır ve "log" dosyalarının saldırı hakkında kayıt tutacağını da bilmesi gerekmektedir. Saldırıda bulunanın kayıtları incelemesi veya erişmeye çalışmasındaki en büyük neden ise ele geçirdiği sistemden çıkarken geride iz bırakmak istememesi ve izleri yok etmek istemesidir (Güven, 2004: 52).

Türkiye Cumhuriyeti vatandaşları hedef alan phishing (oltalama) yöntemiyle gerçekleştirilen ve vatandaşların kredi kartı bilgilerini elde etme amacıyla "skimming" saldırıları ile kart bilgilerini satıyor olabileceği değerlendirilen gayrı resmi olarak "Cimer Duyuru Grubu" olarak adlandırılan saldırganlarda vardır. Bu grubun yöntemleri genel olarak kredi kartı ve başka bilgileri elde etmek için sahte web siteleri hazırlama, zararlı

sayfalara yönlendiren bağlantılar oluşturma, Twitter ve başka sosyal medya mecralarında reklam verilerek geniş kitlelere ulaşma ve başkalarına ait sosyal medya hesaplarını ele geçirerek bu hesaplardan paylaşma gibi yöntemleri olmuştur (Thinktech STM Teknolojik Düşünme Merkezi Siber Tehdit Durum Raporu, 2020: 5).

Saldırganların asıl amaçlarından biri inandırıcılık sağlamaktır. Bu amacı gerçekleştirdiği ve mağdura istediği eylemi yaptırınca başarıya ulaşmaktadır. Bu sebeple vatandaşların daha çok güvenebileceği kurumlar ve/veya şahıslarla irtibat kurmaları gerekmektedir.

Kötü niyetli veya suç işlemeye meyilli kişilerin kazancınızı yasal olmayan yollardan ele geçirmelerine müsaade etmemeli ve gerekli tedbirlerin alınması gerekmektedir. Kendisini kamu görevlisi olarak tanıtıp, hattınızın veya cep telefonunuzun terör örgütü tarafından kullanıldığı, bu örgütten ve adının karışmaması için mağdurlardan para, altın ve kıymetli eşya istemeleri yaygın bir yöntem olup özellikle yaşlı insanları çok kolay kandırabilmektedir. Savcı, polis veya herhangi bir kamu görevlisinin para veya altın istemeyeceği unutmamalı bununla ilgili bilinçlendirici reklamlar ve seminerler verilmelidir.

Evlere ve binalara nasıl ki güvenlik kameraları takılıyor önlemler alınıyorsa internet ve dijital âlemde de güvenlik önlemi alınmalıdır. Siber suçlar işlenirken birçok suç ve birçok hak ihlali birlikte işlenebilmektedir. Bu sebeple tedbirin ve siber güvenlik önlemlerinin gecikmeksizin alınması önem arz etmektedir. Etkilenen hesapları kapatmalı, şifresini değiştirmeli ve şikâyetçi olunan konular ile ilgili Cumhuriyet Savcılığı veya kolluk birimine şikâyette bulunulmalıdır.

Siber uzayda savunma, saldırıya karşı üstün olduğu iddia edilebilir. Örnek olarak İran gibi kritik altyapılarının önem arz ettiği ve mekanik yöntemler kullanılan bir devlet, ağ teknolojilerini yoğun olarak kullanan ABD'ye göre siber savunma açısından avantajlıdır. Diğer taraftan İran küresel güç olmasa bile siber saldırı kapasitesine ciddi olmasa da düşük bütçeli yatırımlar yaparak ekonomik ve teknolojik açıdan büyük olan ABD ile siber uzayda rekabete girebilmektedir (Darıcılı, 2018: 324).

Siber uzay yeni bir muhabere ve rekabet alanı getirmekle kalmamış, stratejik ve hassas bir konu haline gelmiştir. Savunma alanından ekonomiye, ticaretten sağlık alanına kadar birçok sektörde kritik alt yapıların korunması siber güvenliğin sağlanması açısından önemli hale gelmiştir. Sadece Türkiye değil hemen hemen birçok ülkeye siber saldırılar düzenleyen uluslararası hacker grubu olan Anonymous çok etkili olmuştur. Saldırılarını hizmet akışını engelleyerek (DDOS) yapmakla birlikte sistem açıklarını kullanarak gizli belgeleri çalmıştır. Sadece kamu sektörüne değil özel sektöre de saldırılar düzenlenmiştir.

4.2: Siber Saldırı Çeşitleri ve Yöntemleri

Siber saldırılar genellikle hacking faaliyetleri olarak bilinmektedir. Bilişim sistemlerine yetkisiz ve izinsiz erişimler olup hukuka aykırı ve sahibinin bilgisi ve/veya rızası dışında erişilmektedir. Birçok ülkede ve Türkiye'de suç olarak sayılmakta ve bu suçla birlikte başka suçların işlenmesine kapı açmaktadır (www.egm.gov.tr).

Siber saldırı çeşitlerinden ve hacking faaliyetlerinin en aktif ve fazla kullanılan yöntemlerinden biri Bot-Net ya da başka bilinen adıyla D-DOS saldırı türüdür. Bot-Net/ D-DOS saldırıları bir bilişim sisteminin erişilmesini engellenmesi amacıyla yapılır. İlk olarak zararlı yazalım yüklenerek ele geçirilmiş ve "BOT" olarak tabir edilen bilgisayar ve sistemlere komut verilerek istenilen web sitesi çok sayıda giriş isteği aldığı için başka kullanıcılara hizmet verememesi ve ulaşımının engellenmesi eylemidir. Genel olarak anlaşılması için verilen örnek aynı anda on kişinin girebileceği bir market kapısına on binlerce kişinin yığılması ve marketin hizmet verememesi örneği açıklayıcıdır. Ticari, siyasi ve terör amaçlarıyla yapılabilmektedir (www.egm.gov.tr).

DDOS (Distributed Denial of Service) saldırıları geleceğin en büyük dijital tehlikesi olarak görülmektedir. Bu saldırılarda çok sayıda makine kullanılmaktadır. Hacker'lar tarafından zombi yazılımlar kullanarak daha önce güvenlik açığı olup ele geçirdiği bilgisayarları kullanarak tek komutla hedefe saldırı yapabilmektedirler. Uzaktaki makineleri saldırı için yönlendiren TFN (Tribe Flood Network) programları ve üst versiyonu TFN2K ve Trino programları gibi çek çeşitli programlar kullanılabilmektedir (Yılmaz, 2005: 329-333).

Hacker gruplarının özellikle ilgilendiği konuların başında verilere yönelik suçlar olmaktadır. Özellikle bir sistemdeki veriyi yok etme veya sisteme girerek veri ekleme,

veriyi değiştirme, şifreleme, çalma veya veriye tümden erişimi engelleme eylemleridir (www.egm.gov.tr).

Siber saldırılarda saldırganlar port tarama yaparlar ve en popüler keşif yoludur. Port tarama ile saldırgan hedef sistemin belirli portlarına bağlantı kurar. Daha sonra gelen cevaplara göre sistemin açık, kapalı veya filtrelenmiş olup olmadığını öğrenir. Port tarama ile saldırgan hedef sistemin çalışan servislerini ve işletim sisteminin detaylarını öğrenir. Saldırganın amacı, çalışan servislerdeki zayıflıkları bulup bundan istifade etmektir (Burlu, 2013: 41-42).

Genel olarak siber saldırı yöntemlerinin bilinmesi tedbirlerin alınmasında ve güvenliğin arttırılmasında yararı olmaktadır. Herhangi bir suç bilgisayar veya internet ortamında işleniyorsa ve hukuka aykırı olarak da tanımlanıyorsa bu siber suç olarak tanımlanabilme olasılığı bulunsa da bilgisayarda işlenen her suç siber suç değildir. Siber suç, ağ veya bilgisayar sistemleri aracılığıyla bilgisayar veya ağ sistemlerine karşı işlenebilen suçlardır.

Bilgisayar ile ilgili suçlar basit internet dolandırıcılığından başlayıp sahteciliğe, programların telif haklarına aykırı olarak paylaşımı ve dağıtılmasına, Telekomünikasyon sistemlerinin çökertilmesine, internetten çocuk istismarına ve banka hesapları vurgununa kadar çok çeşitli olarak yelpaze de işlenebilmektedir.

Genel olarak yapılan siber saldırı çeşitleri:

4.2.1: Şifrelere saldırı yöntemleri: Çeşitli yöntemlerde yapılmaktadır. Belirlenen kelimeleri şifre üzerinde denenmesi ile yapılan sözlük saldırısı (Dictionary Attack), olabilecek olasılık ve kombinasyonların şifre üzerinde denenmesi olarak bilinen Brute Force yöntemi, önce sözlük içindeki kelimeleri daha sonra brute force saldırı yaparak çalışmakta olan Hybrid yöntemi ve insani ilişkiler kullanılarak şifreler elde edilmeye çalışılan sosyal mühendislik yöntemleri ile şifreler elde edilmeye çalışılır (Burlu, 2013: 71).

4.2.2: Zararlı Yazılımlar (Malware): Bilgisayar sistemini kötü emellere ulaşmak için erişme ve ya bilgisayara ciddi zarar veren kötücül programlardır. Zararlı yazılım

genel ifade olup virüsler, solucanlar, rootkitler, Truva atları ve casus yazılımları içerir (USOM Siber Güvenliğe İlişkin Temel Bilgiler, 2014: 9).

4.2.3: Virüsler: Bilgisayar sistemine bulaşmak için dosyalara tutunup kendini çoğaltan programlardır. Virüslerin aktif hale gelmesi kullanıcının çalıştırması ile olmaktadır. Özellikle "otomatik çalıştır" (Autorun) özelliği bilgisayarda virüslerin aktif olmalarını kolaylaştırıcı etkendir. Virüslerin en yaygın ortamı internet siteleri olup internetten dosya veya program indirirken p2p yazılımları gibi virüslere davetiye çıkarır (Büyükçapar, 2018: 55).

4.2.4: Rootkitler: Bilgisayara bulaşıp aktif işlemler sırasında kendini gizleyen uzaktan bilgisayarın tam hâkimiyetini ele geçirmesidir. Kötü niyetli kişilerce sistemde varlığını gizlemeyi amaç edinir (USOM Siber Güvenliğe İlişkin Temel Bilgiler, 2014: 11).

4.2.5: Trojanlar (Truva Atları): Mitolojide geçen Truva atının armağan gibi sunulup aslında Troyayı istila eden Yunanlı askerleri taşıyordu ise Trojanlarda bilgisayar sisteminde kullanışlı veya eğlenceli görünüp arka planda sistemde gizli bilgilere ulaşıp bunları dışarıya göndermeye yarayan casus yazılımlardır. Trojanlar ile şifrelere, kişisel belgelere, ekran görüntülerine, resimlere, ortamdaki ses ve web kamerası görüntülerine gizlice ulaşılabilmektedir (Burlu, 2013: 125).

4.2.6: Solucanlar (Worms): Solucanlar, bağımsız ve kendi kendine çoğalabilen olup ağda bir bilgisayardan diğer bilgisayara yayılabilmektedir. "Kurt" olarak adlandırılmakla birlikte bir bilgisayarla iletişim kurulduğu anda o bilgisayarda kendini transfer etmekte ve o bilgisayarda saniyeler içinde yayılarak ele geçirebilmektedir (Çifci, 2017: 169). Solucanları virüslerden ayıran özelliğe bakmak gerekirse virüs bir programın çalışması ile bilgisayara bulaşırken wormlar hiçbir müdahaleye gerek duymazlar. Wormlar sistemin açıklarını kullanmakta ve bilgisayar hafızasını kullanıp kendini çoğaltabilir. Virüsler gibi çalıştırılabilir programa kendini bulaştırmaz (Burlu, 2013: 115).

4.2.7: Phishing (Oltalama-Yemleme): Kullanıcıların bir sistemde kullanıcı adı, şifre, kimlik bilgileri, kredi kartı bilgilerinin elde edilmesi yöntemi olup İngilizce password (şifre) ve fishing (balık avlamak) kavramlarının birleşimiyle oluşmuştur. Türkçe olarak düşünüldüğünde ise phishing "yemleyici" olarak bilinen şifre avcıları, eposta

yoluyla kişilere ulaşıp resmi veya güvenilir kurum gibi kredi kartı bilgilerini ister. Bu tip maillere cevap veren veya inanıp bilgilerini giren kullanıcıların hesapları, şifreleri veya kredi kartı bilgileri çalınmaktadır (USOM Siber Güvenliğe İlişkin Temel Bilgiler, 2014: 11-12).

4.2.8: Keylogger ve Screenlogger: Bilgisayar kullananların klavye tuşlarını kayıt altına alan keylogger zararlı yazılımı ile ekranda yapılanları kayıt altına alan screenlogger zararlı yazılımı ile kötü niyetli kullanıcılara gönderir. Keylogger ile banka, e-posta, sosyal ağ şifreleri elde edilebilecekken, secreenlogger ile izlenen videolar, gezilen sayfa ve siteler, yazılar görsel olarak kayıt edilip kötü niyetli kişilere ulaşır (Büyükçapar, 2018: 56).

4.2.9: Tarama (Scanning): Terimsel olarak port (giriş-delik) hem fiziksel hem sanal yapıyı ifade eder. Fiziksel anlamda bilgisayarın giriş ve çıkışına bağlanan yazıcı, klavye gibi bilgisayara bağlanma anlamında kullanılmakta ve sanal anlamda ise veri iletişimi anlamında işletim sistemi ve ağ cihazlarındaki iletişimin sanal olarak olacağını anlatır. Güvenlik için bazı girişler açık bırakılabilir. Bu açıklıktan sisteme saldırı yapmak isteyen kötü niyetli kişiler saldırı yapabilirler. Bu açık girişlerin tespiti için tarama (scanning) yapılır (Akarslan, 2015: 99-100).

4.2.10: Sosyal Mühendislik: Bilgisayar kullanıcılarını yönlendirmeler yoluyla şüphe duyurmadan güvenilirliğini kazanarak kullanıcıların gizli veya değerli bilgilerinin elde edilmesi yöntemidir. Genel olarak mağdurun acil durumlarında, korku ve endişeli zamanlarında aktif olunmaktadır. Panik halinde olan mağdurlar tehlike veya acil durumlarda linke tıklama veya virüslü dosyayı indirme gibi hataları kolaylıkla yapabilmektedirler. Mağdur karlı çıkacağı bir senaryoya ikna edilir ve vaat etme yoluyla veya sahte senaryolarla güven kazandırılır (Bayer & Aksoğan & Çoban & Çelik, 2017: 362-364).

4.2.11: Kartlı ödeme sistemleri dolandırıcılıkları: ATM dolandırıcılıkları kart sıkıştırma, para sıkıştırma, fiziki ATM soygunu olarak çeşitleri olsa da en etkili çeşidi ATM'lere zararlı yazılım yüklemektir. ATM'lerde birer bilgisayar içermektedir ve bu bilgisayarın güncellenmemiş işletim sistemine zarar verici saldırılar yapılabilmektedir. Saldırganlar ATM kapağını açtıktan sonra bilgisayara zararlı yazılım yükleyip bir komut

ile tüm parayı alabilmektedirler. Bunun en bilinen örneklerinden biri "Tyupkin" zararlı yazılımıdır. Ayrıca kart kopyalama (Skimming) veya sahte üretilmiş kartlarla da dolandırıcılık yapılabilmektedir. "Skimmer" cihazı ile kartın kopyalanması ve ATM'lere yerleştirilip şifreler edinilip, hesaplardan para çekilebilir (Türkiye Bankalar Birliği, 2015: 59-63).

4.2.12: Sahtecilik: Sahtecilik ile kastedilenin dijital belgelerin sahteciliği olabileceği gibi kimlik hırsızlığı gibi başkalarına ait kişisel bilgi ve belgelerin ele geçirilip kullanılması kastedilmektedir. Kimlik hırsızlığı ekonomik kazanç için yapılmakla birlikte şantaj veya itibar zedeleme amacıyla da kullanılabilmektedir. Bir kişinin itibarını zedelemek için internet üzerinden pornografik materyal siparişi vererek kullanılabilir (Hekim & Başıbüyük, 2013: 139).

4.3: Teknoloji ve İnternet Bağımlılığına Karşı Alınabilecek Önlemler

Teknoloji kullanımı özellikle gençlerde ve eğitim seviyesi yüksek bireylerde fazlalığı bir gerçektir. Teknolojiyi kullanan bireylerin daha çok eğitim düzeyi yüksek olması teknolojiyle ilişkiyi ve zaman geçirme süresini arttırmıştır. Bu da bağımlılığı beraberinde getirmiştir. İnternet bağımlılığı günümüzde çok sık rastlanan ve özellikle ebeveynleri de etkileyen çok önemli bir sorundur.

İnternet bağımlılığı birçok sorunu beraberinde getirmiştir. İnternet bağımlılığından sağlık ve psikolojik hasarlar yanında başka kişilere de zarar verme durumları ile karşılaşılmıştır. Her birey huy ve karakter özellikleri itibarıyla farklı olduğundan internet bağımlılığı kimi bireylerde bağımlılığa kadar gidebilmektedir. Nasıl ki alkol-sigara ve uyuşturucu gibi kötü alışkanlıklarla mücadele ediliyorsa internet bağımlılığı içinde mücadele edilmesi gereklidir.

İnternet öğrencilerin bilgiye ulaşımını kolaylaştırmıştır. Hatta uluslararası kütüphanelere ulaşım gibi bilgiye erişim anlamında yararlar sağlamıştır. İş yaşamında özellikle bankacılık sistemlerinde kolaylıklar ile birlikte anlık işlemler yapılabilmektedir. Bu olumlu durumlar kadar olumsuz durumlarda artış göstermiştir. Özellikle bilgisayar oyun sektörünün gelişmesi ile birlikte gençlerin bilgisayar bağımlısı olması gibi olumsuz sonuçlar ortaya çıkmıştır. Gençler kadar ergenlikten öncesi de çok etkilenmektedir. Anne

babaların bir yaş sonrası çocuklarına susmaları için eline telefon vermesi ile bağımlılık günümüzde çok erken yaşlarda ortaya çıkabilmektedir.

Bilgisayar oyunları ile ilgili araştırmalarda oyun oynama nedeni genellikle; merak, can sıkıntısı, stresten kurtulma, uyarılma isteği, öfke ve kızgınlıktan kurtulma, başarısızlıktan kurtulma gibi sebeplerle oynanmaktadır. En çok tercih edilen oyunlar ise şiddet içerikli oyunlar, fantezi ve şiddet içeren spor oyunlarıdır. İnternet üzerinden oynanan çok oyunculu oyunlar internet bağımlılığının önemli nedenlerindendir (Ögel, 2012: 49).

İnternet bağımlılığı kavramı 1996 yılında Dr. Goldberg tarafından bulunmuş olup daha sonra bilimsel mecrada tartışılmaya başlanmıştır. İnternet bağımlılığının ayrımını yapabilmek için belirli tanı ve ölçütlere de bakılmaktadır. Bağımlılığın olmasında bireylerin fiziksel, toplumsal ve psikolojik özellikleri de etkili olmaktadır. İnternete bağımlı olunmasında çevrimiçi oyun oynama isteği ve bağımlılığı en önemli etkendir. Oyunlarda başka kişilerle iletişim, ekonomik kazancın sağlanması ve sosyallik sağlanmasına yönelik pratikler bağımlılığı arttırmaktadır (Ayhan & Köseliören, 2019: 5-6).

İnternet bağımlılığı literatürde ve yazında farklı şekillerde ele alınmıştır. İnternet bağımlılığı özellikle bir teknoloji bağımlılığı olarak düşünülmekte ve ele alınmaktadır. Teknoloji bağımlılığı, insan makine iletişimini içerecek şekilde kimyasal olmayan bir davranışsal bağımlılık olarak tanımlanmaktadır. Yani davranışları kontrol problemi olarak görülmektedir. Araştırmacılar bu bağımlılığı diğer bağımlılıklar ile akraba olarak görmektedirler. Az uykunun yanı sıra yemek yememe, sınırlı aktiviteler günlük ve iş hayatının bozulması gibi problemlere sebep olduğunu ifade etmektedirler (Taş, Eker ve Anlı, 2014:39-40).

İnternet bağımlılığı, davranışsal bozukluk olarak ele alındığında psikoloji ve sosyal yaşamı etkilemesi açısından önem kazanmaktadır. Günlük hayatı olumsuz etkilemesi ve günün olağan akışının bozulması gibi birçok önemli problemlerle karşılaşılmaktadır. Kişinin kendi kontrolünü kaybetmesi ile başlayan ve onsuz yapamama hali, harcanan zaman ve internet başında giderek daha fazla aktivite ile ortaya bağımlılık çıkmaktadır. İnternet başından kalkınca huzursuzluk ve öfke hali sosyal ve aile çevresi ile ilişkilerini

zedeleyebilmektedir. Başında zaman harcaması sadece bedensel veya sağlık açısından değil psikolojik, sosyal ve hatta adli olarak sorunlara sebep olmaktadır.

Aslında bağımlılıkta kritik eşik bilgisayar başından kalkma kararı alsa bile kalkamama veya nükseden bir durum söz konusudur. Özellikle bilgisayar oyunu oynayamayan arkadaşlarına karşı mahcubiyet yaşamama duygusu ve iyi bir oyuncu olmak için zaman harcamaya itmektedir.

İnternet bağımlılıklarında, klinik bulgu olarak yapılan çalışmalarda, aşırı ve kontrol edilemeyen istek ve dürtülerin olması problematik internet kullanımı olarak tanımlanabilir. İşlevsel ve ılımlı internet kullanımı kişinin psikolojisine katkıda bulunurken ve sosyal ilişkilerini arttırabilirken problematik internet kullanımında sosyal ilişkilerini bozmakla birlikte mesleki, akademik ve ailesel ilişkilerini bozabilir. İnternet bağımlılığı ve ilgili bozukluklar sinsice gelişen bozukluklardır. İnternet kişinin hayatından tamamıyla çıkarılamamaktadır. Bu sebeple tedavisi çok zor olup kişinin küçük yaşlardan önlem alınması gerekmektedir. Burada ailelere de önemli görevler düşmektedir. Ebeveynler internet ve bilgisayarı etkin ve yararlı kullanarak çocuklarına örnek olmalıdırlar (Yalçın ve Karaçetin,2016:2 ve 20).

Türkiye'de internet bağımlılığı problemi teknolojiye hâkim gençlerde ve çocuklarda görülmektedir. Aileler çocuklarının internet kullanımının sebep olduğu sorunlar nedeniyle tedavi yapılabilecek merkezlerin arayışına girmiştir. Türkiye'de internet bağımlılığı sorunu artmaya başladığından klinisyenlerimizin ve doktorlarımızın bu bozukluk konusunda yeterli bilgiye sahip olup uygun tedavi yaklaşımı sergilemeleri önem arz etmektedir (Arısoy, 2009: 66).

İnternet bağımlılığı konusunda cinsiyete göre ayırt edecek olursak erkek öğrencilerin daha fazla desteğe ihtiyacı vardır. Öğrenim düzeyi ne olursa olsun ailelere yönelik bağımlılık konusunda broşür yayınlama, konferans düzenleme, TV programları yapma, rehberlik faaliyetleri oluşturma gibi etkinlikleri önerilmektedir (Gökçearslan ve Günbatar, 2012:22).

Dijital oyun bağımlılığı gerçek oyun ve sanal olmayan oyunlar ile önlenebilir. Okulda ve ev ortamında sosyal etkileşime dayanan oyunlar ön planda tutulmalıdır. İlla

kullanılacaksa zekâ geliştiren uygulamalar ve oyunlar oynanmalıdır. Ailenin kontrol ve yönlendiricilik görevi önem kazanmaktadır. Çünkü okulda öğretmenlerin gözetimi ve müdahalesi sınırlı olabilmektedir. Ailenin gözetimi ve çocukları ile zaman geçirmenin önemi giderek artmaktadır. Kardeşlerin bile günümüzde teknoloji sebebiyle ilişkileri ya minimum ya da bozulmaya doğru gittiği bir çağdayız. Teknolojinin bu olumsuzluklarından korunmak ve kurtulmak için insan iletişiminin önemi giderek artmaktadır.

Günümüzde internet bağımlılığı öyle bir boyuta gelmiştir ki: onsuz yapamama ve korku-hastalık boyutuna gelmiştir. Özellikle literatürde nomofobi olarak akıllı telefonsuz kalma korkusu olarak bilinen bağımlılık türü gelişmiştir. Nomofobi aslında teknolojinin insan hayatında önemli bir noktaya geldiğini göstermiştir. Nomofobi'nin hemen hemen herkeste görülebilme olasılığı vardır ve teknoloji ile temas kuran her insanın potansiyel hasta olabileceğini belirtmek gerekir. Bireyin yaşam kontrolünü etkileyip günlük yaşamına odaklanmasında sorun olabilmektedir. Nomofobinin artık internet bağımlılığı ile ilgili çalışmalardan daha özel olan mobil cihaz bağımlılığına yönelik çalışmalara doğru evrilmiştir.

Nomofobi kavramı ilk olarak İngiltere'de 2008 yılında Posta İdaresince yapılan bir araştırmada meydana çıkmıştır. Bu çalışmada 2100 akıllı telefon kullanıcısı katılmıştır ve katılımcıların yarısından fazlası nomofobiye yakalandıkları tespit edilmiştir. Katılımcıların akıllı telefonlarının batarya bitmesi, kontör bitmesi durumunda, çalınma veya kapsam alanı dışında kalınmasından dolayı endişe duyduklarını belirtmişlerdir. Ayrıca kavram İngilizce "No Mobilephone Phobia" yani "akıllı telefonsuz kalma" fobisinden gelmektedir. Burada cep telefonlarının yerini alan akıllı telefonlar da kastedilmektedir (Erdem, Türen ve Kalkın, 2017: 3 ve 4).

Dijital hastalık olarak görülmekte olan nomofobi kavramı, insanların elektronik veya teknolojik bir aletle bağını kopardığı zaman hissettiği ve/veya kendi içinde duyduğu duygular bütünü şeklinde hayatımıza girmiştir. Kişi stres, sinirli olmakla birlikte saldırgan bir bireye dönüşebildiğinden psikolojik bir rahatsızlık olarak tıpta yerini almıştır. Connecticut Üniversitesi'nden David Greenfield'in yapmış olduğu çalışmada Nomofobi kavramı için akıllı telefon bağımlılığının belirtileri görüldüğünde konulan isim olduğunu

belirtmişlerdir. No-Mobile-Phone ifadesinin kısaltılması ve geliştirilmesi ile Nomofobi ismi karşımıza çıkmıştır (Polat, 2017:165 ve 168).

Nomofobi teriminin haricinde literatürde yeni olan bir başka kavram "Hikikomori hastalığı" olarak bilinen Japoncadan Türkçeye çevrildiğinde ise "dünyadan elini ayağını çekmek, yalnız başına hayat sürme" veya " geri-içeri çekilmek, hapsedilmiş olmak" anlamına gelmektedir. Bu hastalığa göre bireyler hayattan deyim yerindeyse "hayattan el çekerek" ve odalarına kapanarak bilgisayar başında zaman geçirmeyi ifade etmektedir (Batu ve İplikçi, 2019: 644).

Sosyal medyanın aşırı ve bilinçsiz kullanımı ile nomofobi, hikikomori, Youtube Narsisizmi, Blog ifşacılığı ve birçok rahatsızlıklar oluşabilmektedir. Dijital medya kullanıcıları popülerleşme ve takipçi sayısını fazlalaştırma adına kendilerini yeniden tanımlamakta ve kurgulamaktadırlar. Bu durum gerçeklik algısının bozulmasına ve gerçek hayattan zevk almama durumuyla karşılaşılmasına ayrıca sanal alemin muhteşem çekiciliğine bağlanılarak teknolojinin kontrolsüz kullanımına yol açabilmektedir (Batu ve İplikçi, 2019: 639).

Özellikle devlete ve STK'lara akıllı telefonsuz kalma korkusu gibi ve diğer teknolojinin ortaya çıkardığı rahatsızlıklarla ve sorunlarla mücadele konusunda sorumluluk düşmektedir. Devletin 2018 yılında ortaya koymuş olduğu "Bağımlılıkla Mücadele Eylem Planını" kararlılıkla uygulamalıdır. İlkokuldan başlamak üzere teknolojinin doğru kullanımı ve teknolojinin fayda ve zararları anlatılmalıdır. Sürekliliği olan eğitim programları geliştirilmelidir (Akman, 2019: 270).

Mevcut haliyle gençleri ve çocukları teknolojiden soyutlamak veya izole etmek imkânsız gibi görünmektedir. Gerek eğitim dünyasında gelişen teknolojik imkânlar gerek pandemi kaynaklı uzaktan eğitime verilen destek ve önem artmış olup uzaktan eğitim bir seçenek olmaktan çıkıp zorunluluk halini almıştır. Bu sebeple internet bağımlılığı ve Nomofobi gibi rahatsızlıklarda tüm kesimlere görevler düşmektedir. Devlete, STK'lar, Öğretmenler, anne-babalar ve ilgili olabilecek herkese görevler düşmektedir.

Teknolojinin gelişimi bazı durumlarda zamandan tasarruf sağlarken hayatımızı kolaylaştırmış. Artık hız önemsenir olmuştur. Sosyal medyayı yaygın kullanan gençler

arasında adeta "internet dili" denilen bir dil gelişmiştir. Çoğu zaman emojiler gönderilse de "Allaha emanet ol" yerine "aeo", "kendine iyi bak" yerine "kib", "iyiyim" yerine "iim", "sağ ol" yerine "saol" , "Direkt Mesaj" yerine "DM", twitter'da kullanılan "Trend Topic" yerine "TT", İnstagram ve twitter'da kullanılan "throw-back Thursday" kısaltması "tbt" geçmişte çekilmiş olan fotoğraflar paylaşılırken, işteyen bakmayın uyarısı manasında sansür için kullanılan yetişkin içerikli paylaşım yapılacakken"not safe for work" kısaltması "NSFW" gibi daha birçok kullanım görmek mümkündür.

Böyle yukarıdaki gibi kısaltmalara karşı uyarılar ve bilinçlendirme faaliyetleri yapılması gerekir. Aksi halde Türkçe'nin yozlaşması veya tahribata uğraması kaçınılmaz olacaktır. Sanal dünyada artan sosyalleşme ihtiyacı, aidiyet ve topluluğa dâhil olma çekiciliği, kaynaklara erişimin kolay olması, zafer ve kazanma arzusu, toplum denetiminin zayıf olması ve anonim olmanın verdiği rahatlık gibi birçok kolaylık sağlanmıştır. 21. Yüzyılda literatüre giren sibernetik, robot teknolojisi, big data, yapay zeka, nano teknoloji, dijital çağ, siber uzay, globalizm gibi kavramlar yerleşmiş ve tartışılır olmuştur. Teknoloji gelişse de insan oto kontrolünü kaybetmemeli ve eylemlerini bilinçli yapmalıdır.

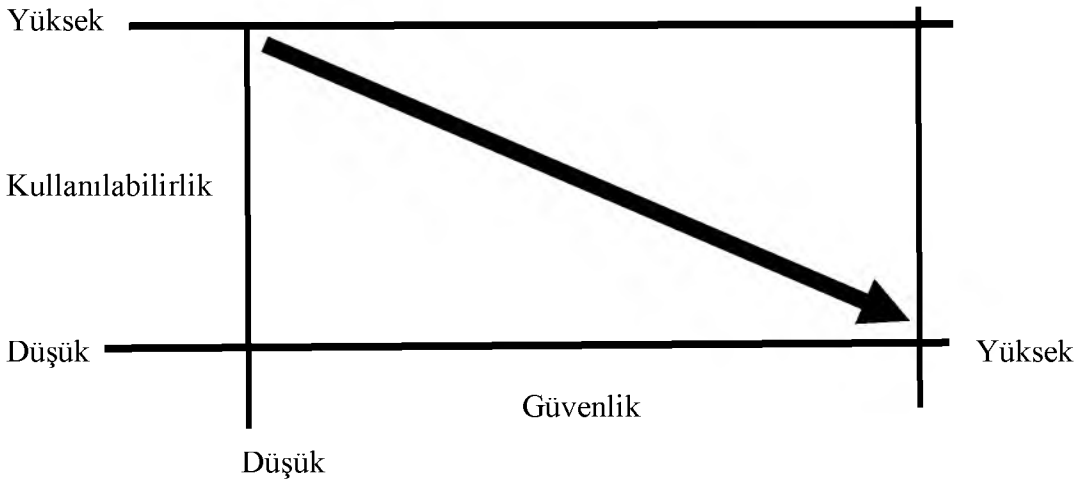
Ebeveynlerin güçlü ve iyi bir aile bağları sağlamaları bağımlılıkla mücadelede önemli bir avantajdır. Aksi halde gerekli sıcaklığı ve samimiyeti bulamayınca oyun arkadaşları ve sanal dünya daha çekici gelebilmektedir. Aile içi ilişkiler açık, uyumlu ve tutarlı olmalıdır. Çocuklara gerekli ilgi gösterilmeli ve çocuk zihnini belirsizliklerden uzak tutmak gerekir. Bilgisayar veya telefon kısıtlamaları gerçekçi ve somut olarak anlatılmalıdır.

Okulda başarılı olması özellikle bağımlı olmaması ve teknolojiyi yararlı kullanımına da bağlıdır. Spor ve kulüpler ile internette zaman harcamaksa zinde ve sağlıklı aktivitelere yönlendirilmelidir. Sadece çocuklar değil aile bireyleri de bilinçli olmalı ve doğru internet kullanım becerisine sahip olması gerekmektedir.

4.4: Siber Güvenlik İçin Alınabilecek Önlemler

Deprem olmadan önce tedbirlerin alınması gerekliyse, Siber saldırılar olmadan önce de tedbirler alınmalıdır. Eğer önlemler sağlam ve yerindeyse veri kaybı olmadan, sistem ve bilgiler zarar görmeden saldırı atlatılabilir. Acil durumlarda karşılık verme ve nasıl müdahale edilmesi gerektiği ve nasıl silsile izleneceği planlanmalıdır. Aslında öyle

tedbirler alınmalı ki acil durum veya siber saldırılarla karşı karşıya olunmasın. Alınacak tedbirler ve ne kadar tedbir alınacağı bir ikilemle karşılaştırmaktadır.



Şekil 4.1: Güvenlik Üçgeni (Burlu, 2013: 3).

Yukarıdaki güvenlik üçgeni şekli güvenlik eğitimlerinde sıkça kullanılmakta olup güvenliğin ne kadar arttırılırsa kullanılabilirliğin o kadar düşeceğini anlatmaktadır. Terazinin iki kefesi gibi, hangisine önem veriyorsak diğerinin önemini azaltıyoruz demektir. En uygunu hem güvenliği sağlamak hem de kullanılabilirliğimizi ve alanımızı daraltmamaktır.

Güvenlik için alınabilecek önlemlerin başında Firewall sistemini kurmak gelecektir. Ev için kullanım veya şirket için olsun bilgisayarın korunması şarttır. Ücretsiz Firewall bulunabileceği gibi fiyat olarak çok pahalı Firewalllarda vardır. Dikkat edilmesi gereken Firewall 'un kullanım zorluğu, performansı ve fiyatıdır. Genel olarak piyasada iki çeşit Firewall bulunur. Bunlar: Application Proxy seviyesinde çalışan Firewalllar ve Stateful Inspection olarak çalışan firewalllardır. İlk olan çeşidinde gelen paketleri içeriye kendisi gönderir. Böylece paketlere müdahale şansı olurken ikinci olanında isi paketlerin hedeflere ulaşması ve cevapların dönüşüne kadar her durumu izler. Yoğun olmayan ağlarda ilki kullanılmakta olup yoğun ağlarda ikincisi tavsiye edilir (Güven; 2004: 32).

Alınabilecek diğer güvenlik önlemi virüs tespit edici ve virüse karşı korumu sağlama amacı taşıyan Anti-Virüs yazılımları ve programlarıdır. Bir başka güvenlik önlemi Saldırı Tespit Sistemleridir. Sistemin hangi saldırılara maruz olduğu ve saldırıların hangi ölçüde engellenebileceğinin tespiti yapılır. Bir başka önlem VPN yan ve Sanal Özel Ağ kullanarak sistemin veri trafiğinin dinlenmemesi için trafiği şifreleme yöntemidir.

Özellikle yöneticilerin işini kolaylaştıracak ve çalışanlarının belli sitelere girebilmesine olanak sağlayan İçerik Filtreleme Yazılımları, Raporlama ve Ağ izleme araçları kullanmak alınabilecek önlemlerdendir (Güven; 2004: 33-34).

Cep telefonları sadece açık olduğunda yapılan konuşmaları kaydetmekle kalmamakta ve konuşma yapılmadığı durumlarda bile yer tespiti veya dinleme cihazı olarak kullanılabilmektedir. Bilgisayarda internet üzerinden bilgi veya veri aktarımlarının yapılması olanak dâhilinde olabilmektedir. Özellikle hangi sitelere giriş yapıldığının veya hangi arama kelimelerinin taratıldığının tespiti ve veri trafiği tutulabilmektedir. İnternette her şeyin izinin olması özellikle hacker ve kötü niyetli kişiler tarafından istenilmeyen bir durum olduğundan dolayı ip gizleyiciler veya VPN diye tabir edilen ip dönüştürücüler çok sık olarak kullanılmaktadır.

Siber dünya gerçek dünyanın sanala uzantısıdır. Çalışabileceğimiz ve oyun oynayabileceğimiz yeni bir boyut. Yararları çok muhteşem olup hız, zaman ve maliyetten tasarruf sağlanması açısından avantajlıdır. İnternet ile insanlar bazı engelleri kaldırmaya vesile olmuştur. Çevrim içi oyunlar veya canlı sohbetlerde takma ad kullanılarak kimliğin gizlenmesi çok kolay olabilmektir. İnsanlar normal hayatından farklı davranmaya çalışır. İnsanlar sanal âlemde yapacağını yapar ancak gerçek âlemde sonuç doğurur (Chilk, 2007:159).

Hacker'lar internette bulunan arama motorları, eposta grupları ve forumlarda açık kaynak araştırması yapmaktadırlar. Bu sayede enteresan ve güvenlik ile ilgili bir şirket veya kişi hakkında bilgiler edinirler. Çoğu sistem yöneticisi bu tür gruplarda rastgele sorular sorup bu soruların güvenlik açıklarını düşünmeden bilgi paylaştıklarından çok riskli olmaktadır. Bu araştırmalar ile hedef şirket hakkında şirket yapısı, irtibat ve iletişim bilgisi, IP ve DNS adresleri, kullanmış olduğu işletim sistemi ve güvenlik mekanizmaları gibi çok çeşitli ve önemli bilgilere ulaşabilmektedirler (Yılmaz, 2005: 130-131).

Siber güvenliğin sağlanması için bazı hususların tam olarak sağlanmasına ihtiyaç vardır. Bunlar genel hatları ile gizlilik, kimlik doğrulama, bütünlük, erişilebilirlik ve inkâr edememe gibi unsurlardır. Gizlilik unsuruyla verilere sadece yetkisi olanların erişmesini ve ilgisiz kişilerce verilere erişimi engellemeyi ifade eder. Bütünlük unsuru ile verilerin doğruluğu ve içeriğin değişmeden gönderilmesini anlatır. Kimlik doğrulama unsuru ile

yetkilendirilmiş kullanıcıların verilere erişimi için kullanıcıların belirlenmesi ve doğrulanmasını ifade eder (elektronik imza kullanımı gibi). İnkâr edememe unsuru ile yetkilendirilmiş kullanıcının mesaj gönderme ve alım işlemlerinin ispatlanması ve inkâr edilmemesi durumunu anlatır. Erişilebilirlik unsuru ile yetkili kullanıcıların sisteme güvenli ve sürekli erişim hakkının garanti edilmesini anlatır (Sağıroğlu, 2018: 41-42).

Siber güvenlik anlamında en önemli öncelik sağlanması gereken konuların başında tabiri doğru kullanmak gerekirse "virüslenmemek"tir. Bu bir internet sitesine girerek veya gerekli güvenlik önlemi almayarak kendi kendimize karşılaşabileceğimiz gibi bir hacker veya kötü niyetli kişi veya kişilerce sabotaj edilerek karşılaşılabilmektedir. Bu konuda bizim sormamız gereken soru şu olmaktadır: Virüslendikten sonra acil müdahalemiz ne olmalı veya neler yapılmalı sorusu olmalıdır. Virüslendikten sonra ilk yardım ve acil müdahaleler önemlidir. Nasıl ki trafik kazasında acil müdahaleler gerekliyse virüslendikten sonra da acil müdahaleler "hayat kurtarıcı" olabilmektedir.

Öncelikle panik olunmaması ve sakin olmak gerekmektedir. Gereksiz yere panik insanın kendisine daha çok zarar verebilmektedir. Çok acil durumda yani virüsün dosyalarınızı sildiğini düşünüyorsanız bilgisayarı doğrudan kapatabilirsiniz. Fakat bilgisayarı doğrudan kapatma eylemi, kaydedilmemiş dosyaları veya açık olan işlemlerin kaybedilmesine ve bazı uygulamaları bozabilmektedir. Bilgisayar kapatılmasa bile dış dünya ile bağlantısını kesmek gerekmektedir. Yapılabiliyorsa bilgisayardan interneti kapatma, yapılamıyorsa network bağlantısını (Ethernet kablosu gibi) çıkarma yapılabilir. Daha sonra eğer anti virüs programı varsa, virüs taraması yapmak, temizleniyorsa virüs temizlemek, temizlenmiyor ise karantina altındaki dosya silinebilir. Bazı antivürüsler dosyanın bir yedeğini almaktadır. Eğer bu dosyanın yedeği alınmış ise virüs silindikten sonra dosyanın zararlı olmadığından emin olduktan sonra da virüslü yedeğin silme işlemi yapılabilir. Eğer anti virüs programı yoksa bir anti virüs programı elde edinilebilir, edinilmezse bile çevrimiçi virüs taraması yapılabilir. Virüs tespit edildiğinde virüsün özelliklerini sorgulama ve antivürüs geliştiricilerin web sitelerinde tespit ve temizleme ile ilgili bilgiler ve programlar ile bilgisayarı kurtarma yoluna gidilebilir (Bahtiyar: 2003: 12-16).

İsim soy isim, doğum tarihi, kimlik numarası, adres, sağlık kayıtları, telefon numaraları, finansal bilgiler, e-posta adresleri, kredi kart bilgileri, sigorta bilgileri ve daha

birçok bilgilere izinsiz erişmek için yaygın olarak saldırı ve hacklemeler yapılmaktadır. Özellikle iş dünyası ve ticari dünya da siber saldırılar yaparak iş dünyasındaki güven ve imajı zedeleme ve ekonomik değerlerini kaybettirerek saldırılar önemli boyutlara gelebilmektedir (Bendovschi, 2015: 27).

Günümüzde tartışılan ve önemli kavramlardan bir tanesi de dijital okur-yazarlık meselesidir. İnternetin doğru kullanımı, etkin kullanımı ve doğru bilgiye ulaşmada doğru kaynak üzerinden ulaşıp emin olunan bilginin paylaşılması aşamalarını kapsamaktadır. Günümüzde tartışılan bir başka kavram olan dijital vatandaşlığın en önemli özelliklerinden biri de internetin etkin kullanılması, doğru kullanılması ve internetin risklerine karşı tedbir alınmasıdır (Büyükçapar, 2018: 267).

Dijital hayatın kazandırdığı en önemli özelliklerden birisi de sorgulayıcılık ve eleştirel bakış akışına sahip olunmasıdır. Son olarak bilinçli internet kullanımı ve siber güvenlik anlamında alınabilecek genel güvenlik önlemleri genel hatları ile maddeler halinde özet olarak belirtilirse:

Kişisel-Bireysel olarak alınabilecek önlemler:

1. Bilgisayar veya sosyal medya şifrelerini güvenlikli hale gelmesi için etkili şifreler kullanılmalıdır. Doğum tarihi, okul numarası, sicil numaraları vb. bilinen numara ve sayılar kullanılmamalıdır. Şifreler kimseyle paylaşılmamalıdır.

2.İnternet kullanıcısı bilmediği kişi veya kurumdan gelen e-postaları hemen açmamalı. Sms veya e-postalardaki linklere güvenmiyorsa tıklamamalıdır. Sahte sitelere karşı duyarlı olmalı, hemen kişisel bilgi verileri girmemelidir.

3. Kişisel ve özel bilgileri sosyal medyada ve internet ortamında paylaşılmaması gerektiği unutulmamalıdır. (Özellikle telefon numaraları, ev-okul-iş adresleri, doğum günü, T.C. Kimlik numaraları, E-mail adresleri, Anne kızlık soyadı, kardeş sayısı ve isimleri, ebeveynlerin kredi kartı bilgileri, sevilen ünlü veya evcil hayvanımızın ismi paylaşılmamalıdır.)

4. Sosyal medyada ve internet ortamında tanımayan kişilerden gelen arkadaşlık istekleri geri çevrilmelidir.

5. İnternette karşılaşılan ve rahatsız edici durum, yazılar, fotoğraflar, mesajlar vb. ebeveynlere haber verilmelidir. Ebeveynlerinde suç olması durumunda ilgili mercilere iletimi sağlanmalıdır.

6. Sosyal medyada ve internet ortamında çok zaman harcanmamalı ve sosyal faaliyetlere yönlendirme yapılması gerekmektedir.

7. İçeriğinden emin olunmayan dosyalar kabul edilmemelidir. Bilgi ve isteğimiz dışında gelen mail veya mesajlara şüphe ile yaklaşılmalıdır. Bilinmiyorsa ve şüpheliyse dosyalar indirilmemelidir.

8. Sosyal medyada ve/veya internette paylaşım yaparken fotoğraf ve videolarının fotoshop ve fotomontaj ile kötüye kullanılabileceğini öngörerek paylaşım yapılmalıdır.

9. Üçüncü kişilere veya tanınmayan kişilere fotoğraf, video ve herhangi bir bilgi gönderilmemelidir.

10. Sosyal Medya profil ayarları yapılmalı özellikle profilin herkese açık yapılmamasına veya herkesin görmesine izin verilmeyecek şekilde yapılmasına özen gösterilmelidir. Bunu paylaşım ayarları için de yapılması gerekmektedir. Özellikle paylaşılan bilgileri istenmeyen kişilerin görmemesi için kapatılmalı veya o profilleri engelleme seçeneği kullanılmalıdır.

11. Herkese açık olan internet ortamından veya bilgisayarlardan sosyal medya hesaplarına veya bankacılık sistemlerine girilmemesi gerekmektedir.

12. Güvenli internet hizmeti alınmalı özellikle virüs saldırılarına karşı güncel bir anti-virüs programı veya güvenlik duvarı (firewall) kullanılmalıdır. Kullandığımız programlarında yazılımı lisanslı olmalıdır.

13. Çocuklar ebeveyn korumalı bilgisayar kullanmalıdır. Her türlü taciz, tecavüz ve siber zorbalıktan korunmak için aileler çocuklarının ulaştıkları siteleri bilmeli ve dikkat etmeleri gerekmektedir.

14. Ücretsiz wi-fi bağlantıları genellikle saldırganların pusuda beklediği yer ve zamanlar olup şifreleriniz kaydedilebilir. Güvenli olmayan internet wifi bağlantılarına bağlanılmamalıdır.

15. İnternet bağlantımız (modem-tablet-cep telefonu vb. fark etmeksizin) herkese açık olacak şekilde olmamalıdır.

16. Girilen internet sitelerinin güvenilirliği de sorgulanmalıdır. Şüpheli internet sitelerine girilmemeli ve dosya indirilmemelidir.

17. Ekonomik olarak menfaat talepleri olan kişi, internet siteleri, mesajlara karşı şüpheyle yaklaşılmalıdır.

18. Kredi kartı ve/veya bankamatik kartı bilgilerini güvence altına alınamamış ve tanınmamış sitelere göndermemelidir.

19. Evde kişisel kullanılan modemin şifresini veya wifi da tanımadığımız kişilere, komşulara ve arkadaşlara verilmemesi gerekmektedir. Her türlü illegal faaliyet yapılıp modem sahibine veya internetin sahibine mağduriyet yaşatabilmektedir.

Kurumsal-Şirket olarak alınabilecek önlemler:

20. Öğrencilerin, anne-babaların, memurların, şirket veya kurum çalışanlarının siber riskler ve güvenlik konusunda eğitimler verilmesi gerekmektedir.

21. Saldırı Tespit servisleri aktif olacak şekilde çalışmalıdır. Örneğin DoS ve DDos saldırılarında ağ trafiğinin kısıtlanması veya saldırının olduğu portların geçici olarak devre dışı bırakılması yapılmalıdır.

22. Kullandığımız verilerin yedeğini almalı ve düzenli olarak yedeklendiğinden emin olunması gerekmektedir. Mümkünse şirket sunucularının dışında bir yerde yedeklemeleri muhafaza edilmesi gerekmektedir.

23. Her çalışana, öğrenciye, kullanıcıya özel ayrı bir şifre verilmesi ve şifrelerin düzenli aralıklarla güncellenmesi ve değiştirilmesi gerekmektedir.

24. Ağ içinde bilgilere erişme ile ilgili sınıflandırma yapılması, limit belirlenmesi ve erişime yetki verilmesi gerekmektedir.

25. Sosyal Mühendislik saldırılara karşı çalışanlar ve kullanıcılar bilgilendirilmesi gerekmekte olup insani zaafların önüne geçmek için önlemler alınması gerekmektedir. Özellikle bilginin kaynağını sorgulamak ve doğruluğunu teyit etmeden hiçbir işlemi yapmamak gerekmektedir.

26. Bilgisayarlarımıza ve özellikle de sunucularımıza kaynağı belirsiz USB flash bellek veya sd cartlar takılmamalıdır. Mümkün olursa tüm sunucular dış bağlantıya ve uzak erişime kapalı olmalıdır.

27. Web sitesi sahipleri ve/veya yönetici adminleri site trafiğini izlemeli, site trafiğinde düzensizlik veya açık gördüğünde müdahale etmelidirler.

28. Halka açık siteler çalıştıran kurum veya şirket web sunucuları, kurum veya şirket içi ağdan ayrı olacak şekilde korunmalıdır.

Devlet olarak alınabilecek önlemler:

29. Siber suçların tazminat ve hapis cezası süreleri arttırılmalıdır. Siber suçlarda mağduriyetleri önleme anlamında cezaların yetersiz olduğu bilinen bir gerçek olup Türk Ceza Kanununda ilgili maddelerin güncellenmeye ihtiyacı vardır.

30. Siber güvenliğin nasıl sağlanacağı konusunda ülkeler vatandaşlarını bilinçlendirmeli, online (çevrimiçi) olarak hak ve özgürlük arama anlayışı öğretilmeli ve gerekli mekanizmaların kurulması gerekmektedir.

31. Siber suçlar sınır aşan suçlar olması ve tüm ülkeler için tehditler oluşturduğundan uluslararası işbirliğini gerekli kılmaktadır.

32. Uluslararası siber rejimler kurulması için tüm aktörlerin çaba göstermesi gerekmektedir. Bu mümkün değilse uluslararası düzeyde işbirlikleri sağlanması gerekmektedir. (Küresel-Bölgesel-Yerel düzeylerde birlikler ve mekanizmalar için girişimler ve çabalar yapılmalıdır.)

33. 5651 sayılı yasanın gereksinimlerini karşılamak, özellikle MAC-IP eşleştirme ve kayıt alma gibi servisler aktif bir şekilde kullanılmalıdır.

Akıllı Mobil Telefonlar için güvenlik tavsiyeleri

34. Mobil Telefona öncelikle şifre konulması ve temel güvenlik ayarları yapılmış olması gerekmektedir.

35. Mobil telefona indirilen uygulamaları indirmeden önce uygulamaya verilecek izinleri kontrol edin.

36. Mobil telefona indirilen uygulamaları güvenilir kaynaklardan ve mağazalardan (Storelardan) indirilmesi gerekmektedir.

37. Uygulama mağazalarında kredi kartı bilgilerinizi girmektense sanal kredi kartı edinilerek alışveriş yapılması daha güvenli olmaktadır.

38. Mobil Telefonlarınızın güncellemelerini düzenli olarak yapılması gerekmektedir.

39. Mobil Telefonlarınızın içindeki verileri, bilgileri düzenli aralıklarla yedekleme yapın.

40. Mobil Telefonlarınızı satacağınız zaman içerisindeki verileri silin veya fabrika ayarlarına geri dönmesini sağlayın.

SAVCILIKLARCA SİBER SORUŞTURMALARDA ÖRNEK TALİMATLAR:

SENARYO 1: Banka veya kredi kartlarının kötüye kullanılması (TCK madde 245) suçu kapsamında Cumhuriyet Savcılıklarınca yürütülmekte olan soruşturmalarda Cumhuriyet Savcılarınca alınması gerekli talimatlar şu şekilde olursa **kredi kartı**

dolandırıcılık veya Banka veya kredi kartlarının kötüye kullanılması (TCK madde 245) suçlarının aydınlatılmasında daha etkili sonuçlar alınabilecektir:

1.İlgili banka ile yazışmanın yapılması

a)Kredi kartının bağlı olduğu hesabın hangi şubeye ait olduğunun,

b) Kredi kartından yapılan işlemin nerede, ne zaman hangi yöntemle gerçekleştirildiğinin,

c)İşlem internet üzerinden yapılmış ise IP adreslerinin sorulması,

d) İşlem müşteri temsilcisi aranılarak yapılmış ise görüşme kayıtlarının istenilmesi

e) İşlem havale ve ATM'den para çekme yöntemi ile yapılmış ise kamera görüntülerinin istenilmesi,

f)Üye işyeri ve yetkilisinin açık kimlik ve adres bilgilerinin sorulması,

g)Şikâyetçinin hesabından çekilen harcamaya ilişkin hesap özetinin ve harcama detaylarının istenilmesi

2.Para çekme işleminin X Şehir Cumhuriyet Başsavcılığı adli yargı sınırları içerisinde gerçekleştirilmiş olması halinde, temin edilen kamera görüntülerinin (CD'nin/DVD'nin) çözümünün yapılarak şüphelinin tespitine çalışılması,

3. Şikâyetçinin, şüpheli/şüpheliler ile iletişime girdiği telefon numaraları abonelerinin açık kimlik ve adres bilgilerinin Bilgi Teknolojileri Kurumundan ve/veya ilgili GSM şirketiyle yazışma yapılarak sorulması,

4. Tespit edilen telefon numarası bilgilerine göre suça telefon numarası X Şehir Cumhuriyet Başsavcılığı adli yargı sınırları içerisinde kullanan tüm şüphelilerin tespit edilen ev veya işyeri adreslerinde arama yapılması hususunda Cumhuriyet Başsavcılığı ile irtibata geçilerek alınan talimat/talimatlar doğrultusunda hareket edilmesi,

5. X Şehirde ikamet eden tüm şüphelilerin atılı suçtan savunma ve delillerinin tespit edilmesi ve bu konudaki beyanların tutanağa bağlanması,

6. Kredi kartı ile cep telefonu faturasının ödendiği veya kontör alındığının belirlenmesi halinde, bu hat sahiplerinin açık kimlik ve adres bilgilerinin tespit edilmesi,

7. Kredi kartıyla yapılan işlemler sonrasında satın alınmış ürünler kime-hangi kişilere teslim edilmiş ise bu kişilerin de şüpheli sıfatıyla ifadelerinin alınması, ayrıca ilgili kargo şirketinden teslimatın yapıldığına dair belgelerin onaylı suretlerinin temin edilmesi,

8. Tüm bu işlemler sonucunda soruşturmanın mevcutlu veya ikmalen gönderilmesi konusunda Cumhuriyet Başsavcılığından alınan talimat gereğince hareket edilmesi şeklinde örnek talimata istinaden işlem yapılırsa daha olumlu neticeler alınacaktır.

SENARYO 2: Bilişim sistemine girme (TCK madde 243) veya Sistemi engelleme, bozma, verileri yok etme veya değiştirme (TCK madde 244) suçları kapsamında olması durumunda: Örnek olarak bir hastanenin veya bir kurumun/şirketin sunucularının **hacklenmesi, verilerinin çalınması, verilerin yok edilmesi veya şifrelenerek akabinde şantaj olarak para istenilmesi.**

1. Söz konusu saldırıyı gerçekleştiren kişi ve/veya kişilerin tespit edilmesine yönelik çalışmalar yapılır.
2. Güvenlik sistemi loğlarından siber saldırıyı gerçekleştiren makineler ve/veya bilgisayarların ip adresleri belirlenmeye çalışılır.(Mümkün oluyorsa sunucunun imajını almak gerekmektedir. Bu mümkün değilse olay gününden itibaren 1 ay öncesi ve sonrasına ait Log kayıtları alınmalıdır:)
3. Kurumun bilgi işlem biriminde çalışanlar ve yöneticiler hakkında bilgi sahibi sıfatıyla ifadelerinin alınması sağlanmalıdır.
4. Veriler silinmişse silinen verilerin kurtarılması için bir çalışma yapılıp yapılmadığı sorgulanmalıdır. Kurtarma işleminde silinen ve yedekleme yapılmayan verinin olup olmadığı sorgulanmalıdır.
5. Veri tabanı sunucusu üzerinde sistem loğları ve analizi yapılmalıdır.
6. Bir mail veya bilgi varsa araştırılmalı, özellikle ilgili mail şirketinin bulunduğu ülke ile savcı talimatı alınarak yazışmalar yapılması gerekmektedir. Mailin bağlı olduğu şirketin ip adresi ve şüpheliyi bulma adına göndereceği her türlü bilgi ve belge değerlendirilmelidir.
7. Siber saldırıda bulunanlar kurum içi veya kurum dışı üçüncü kişiler tarafından destek alıp almadığı sorgulanmalıdır.
8. Zararlı bir kodla yapılmış saldırı var ise kodun bulaştığı yerler tespit edilmelidir. Tespiti mümkün değilse ağ erişimi kesilmelidir.
9. Saldırgan kaynaktan gelmiş tüm e-postalar tespit edilmelidir. Kime-nereden geldiği belirlenmelidir.
10. Şirketin/Kurumun banka hesaplarının güvenliği alınmalıdır. İlgili banka ile iletişim halinde olunmalıdır.

SENARYO 3: A kişisinin Facebook hesabını ele geçiren kişi/kişiler indirim kuponu verme vaadiyle hesaptaki arkadaş listesindeki arkadaş olarak ekli olanlara telefon numarası isteyerek ve cep telefonuna gelen mesajlara "EVET" yazarak hesabından çok

sayıda işlem yapılması/ başka kişilerin faturalarının ödenmesi/alışveriş sitelerinden harcama yapılması gibi dolandırıcılık olayı olması.

1. Hesaba o günden itibaren erişim yapan/ele geçiren kullanıcılara ait İP numaralarının port bilgileri ve kullanıcı/kullanıcılara ait verilen kimlik bilgileri, kurtarma e-posta adresi ve varsa profil/profillere ait tanımlı GSM numaralarının tespit edilebilmesi için Savcı talimatıyla Swarm/Foursquare/ Facebook/İnstagram vb. sosyal paylaşım siteleriyle yazışma yapılır.
2. Savcı talebi yapılırken "http://www." İle başlayan URL adresinde yayın yapan Z isimli profilin yetkisiz kişilerce erişme anından itibaren günümüze kadar giriş yapılırken sisteminizde bırakmış olduğu İp adreslerinin gün/ay/yıl-saat/dakika ve zaman dilimiyle birlikte temin edilmesi için yazışma yapılır.
3. İlgili şirkete ele geçirilen profil ile bağlantı yapan telefon numaralarının, mail adresi bilgilerinin, varsa konum ve kaynak port bilgilerinin tespit ve temin edilmesi için yazışma yapılır.

SENARYO 4: B kişisinin **cep telefonu ve fotoğraflarının** Swarm/Foursquare/ Facebook/İnstagram vb. sosyal paylaşım sitelerinde paylaşılması ve cep telefonunu arayan binlerce kişi tarafından **rahatsız edilmesi olayı.**

1. Sahte hesapların oluşturulduğu günden itibaren erişim yapan kullanıcılara ait İP numaralarının port bilgileri ve bahse konu profillerin oluşturulduğu sıradaki kullanıcı/kullanıcılara ait verilen kimlik bilgileri, kurtarma e-posta adresi ve varsa profil/profillere ait tanımlı GSM numaralarının tespit edilebilmesi için Savcı talimatıyla Swarm/Foursquare/ Facebook/İnstagram vb. sosyal paylaşım siteleriyle yazışma yapılır.
2. Savcı talebi yapılırken alınan talimat içeriğinde şikâyette bulunulan "http://www." İle başlayan URL adresinde yayın yapan Q isimli profilin URL adresinin tam olarak olması, tam olarak hangi bilgilerin istenildiği (İP Bilgileri, kullanıcı bilgileri v.s.), suça konu eylemin gerçekleştiği tarih (oluşturulma anından itibaren günümüze kadar giriş yapılırken sisteminizde bırakmış olduğu İp adreslerinin gün/ay/yıl-saat/dakika ve zaman dilimiyle birlikte) temin edilmesi
3. Talepte MUTLAKA iki tarih aralığı olmasına özen gösterilmelidir
4. Sahte profil ile bağlantılı telefon numaralarının, mail adresi bilgilerinin, varsa konum ve kaynak port bilgilerinin tespit ve temin edilmesi, gerekir.

SENARYO 5: C kişisinin **fotoğrafları kullanılarak farklı adlarla** Swarm/Foursquare/ Facebook/İnstagram vb. sosyal paylaşım sitelerinde birkaç tane **sahte profil oluşturulması** ve C kişisinin telefonunun paylaşılması ile ilgili **birçok kişi tarafından rahatsız edilmesi olayı.**

1. Sahte hesapların oluşturulduğu günden itibaren erişim yapan kullanıcılara ait İP numaralarının port bilgileri ve bahse konu profillerin oluşturulduğu sıradaki kullanıcı/kullanıcılara ait verilen kimlik bilgileri, kurtarma e-posta adresi ve varsa profil/profillere ait tanımlı GSM numaralarının tespit edilebilmesi için Savcı talimatıyla Swarm/Foursquare/ Facebook/İnstagram vb. sosyal paylaşım siteleriyle yazışma yapılır.
2. Savcı talebi yapılırken "http://www." İle başlayan URL adresinde yayın yapan Y isimli profilin oluşturulma anından itibaren günümüze kadar giriş yapılırken sisteminizde bırakmış olduğu İp adreslerinin gün/ay/yıl-saat/dakika ve zaman dilimiyle birlikte temin edilmesi
3. Sahte profil ile bağlantılı telefon numaralarının, mail adresi bilgilerinin, varsa konum ve kaynak port bilgilerinin tespit ve temin edilmesi gerekir.

SENARYO 6: D kişisinin X isimli oyunda item-karakter-özellik gibi değerlerinin çalınması olayı sonrasında hesabının da çalınması olayı.

(Verilerin hukuka aykırı olarak ele geçirilmesi olayı)

1. İlgili oyun hesabına hesabın çalındığı günden itibaren erişim yapan kullanıcılara ait İP numaralarının port bilgileri ve bahse konu profillerin oluşturulduğu sıradaki kullanıcı/kullanıcılara ait verilen kimlik bilgileri, kurtarma e-posta adresi ve varsa profil/profillere ait tanımlı GSM numaralarının tespit edilebilmesi için Savcı talimatıyla ilgili oyun sitelerinin bağlı olduğu şirketlerle yazışma yapılır.
2. Kullanıcı bilgilerinin temini, olay yeri ve saati belirtilerek istenilmesi önem arz etmektedir. Eğer Türkiye'de temsilciliği bulunmuyorsa yazışma yapılarak temin edilmesi gerekmektedir.

SENARYO 7: E kişi sigorta şirketi sahibi/çalışanı olup sigorta yapan kişilerin bilgilerini alıp data oluşturup satma suçu ayrıca ilgili sigorta şirketlerinin bilişim sistemlerine izinsiz ve yasa dışı yollarla giriş yapması, kayıtlı olan bilgilere izin almadan erişilmesi ve satış yaparak

kişisel banka hesaplarında tespit edilen fazladan gelir elde edilmesi suçu olayı. (TCK 243 ve 244 maddeleri kapsamında bilişim suçunu oluşturmaktadır.)

1. İzin almadan erişim yapan ve satış yaparak kişisel banka hesaplarında fazladan gelir tespit edilen K kişisinin açılış tarihinden günümüze kadar olan zaman aralığındaki hesap hareketleri Savcılık talimatıyla istenilir,
2. Bu hesaplara para gönderen ve bu hesaplardan para havalesi yapılan hesap numaraları ve bankalar bünyesinde bulunan hesap sahiplerinin sistemde bulunan açık adres, telefon ve kimlik bilgileri Savcılık talimatıyla istenilir,
3. Başka bankalar bünyesinde ise bankalara ait bilgilere de Savcılık talimatıyla istenilir,
4. TR11 1111 1111 1111 1111 1111 11 IBAN numaralı hesaptan tespiti yapılabilecek son nakit çekim işlemlerine ait kamera görüntüleri ile çekim işlemlerinin nereden ve nasıl yapıldığı bilgilerine, bilgi ve belgelerin excel ve/veya Word ortamında CD ortamına aktarılarak ilgili Siber Şube Müdürlüğü veya birimine gönderilmesi için Savcılık talimatıyla istenilir,
5. Dosya üzerinde ilk inceleme sonrasında gerekirse soruşturmanın gizli yürütülmesi hakkında gizlilik kararı verilebilir.
6. Soruşturma sonucunda üzerlerine atılı suçları işlemiş olabileceği kanaatine varılacak kişi/kişilere eylemlerine uyan yasa maddeleri gereğince cezalandırılması yapılabilmesi için aleyhlerinde fezleke düzenlenip dava açılmasına kadar olan süreç takip edilmelidir.

SİBER ŞUBE PERSONELİNİN SORUŞTURMA AŞAMASINDA YAPMASI GEREKENLER:

-İnternet sitesi ile alakalı araştırma raporu düzenlemeli, site ile alakalı site sahiplerinin adres ve kimlik çalışması yapılmalıdır. (Sosyal medya üzerinden yapılan dolandırıcılıklarda profil ve paylaşım hakkında URL bilgisi ile sanal devriye faaliyeti neticesinde araştırma raporu düzenlenmelidir.)

-Sitenin Türkiye'de olması durumunda kayıtları kimin tuttuğu ve eklediği ve hatta log kaydı bilgi temin edilmelidir.

-Gelen log kaydı gelmişse analiz edilerek IP bilgisi tespit edilen şüpheliler hakkında yakalama çalışmaları yapılmalıdır.

-İlgili harcamalar sonrası ilgili Bankalar ile Savcı talimatı alınarak yazışmalar yapılması gerekmektedir.

SİBER ŞUBE PERSONELİNİN YAPMASI GEREKENLER VE DİKKAT ETMESİ GEREKEN GENEL BİLGİLER:

1. ARAMA KARARI:

-Arama kararında CMK 134. Maddenin belirtilmesi ayrıca arama esnasında karşılaşılan ve elde edilen dijital delillerin incelenmesi gerekmektedir.

-CMK 134. madde uyarınca dijital inceleme MAHKEME KARARI ile olmaktadır. Gecikmesinde sakınca olan durumda dahi Savcılık kararı dâhil değildir.

-Arama kararlarında sıkıntı yaşanmaması için savcıya talep edilirken gerekçelerin net ve açık bir şekilde yazılması gerekmekte ve gereken durumlarda savcıya bilgi verilmesi gerekmektedir.

-Arama kararları alınırken sadece bina numarası değil, hedef adresin açık ve net bir şekilde belirtilmesi gerekmektedir. (Adres tespiti mutlaka yapılmalıdır. Adres giriş-çıkışı ve altyapıları bilinmelidir.)

-Her adres için ayrı arama kararı alınmalıdır.

-Arama adreslerine temini mümkünse çilingirci ile gidilmesi gerekmektedir. Ev sahibinin kapıyı kasıtlı açmaması durumunda çilingirci yardımından faydalanılmalıdır.

- Arama kararı alınırken sadece daire numarası değil "eklentileri" veya "müştemilatı" ifadelerine yer verilmesi gerekmektedir.

-Nöbetçi savcıya ulaşılamadığında bu durumlarda Başsavcı yardımcılarıyla irtibat kurulmalıdır.

-Arama kararının gösterilmesi ikamet sahibine veya şüphelilere olay yerine giden polis memurlarının tasarrufunda olup girerken olabileceği gibi acil işlemlerin bitmesi sonrası da gösterilebilir.

2. ARAMA ESNASINDA:

- Arama esnasında mutlaka refakatçi bulunmalıdır.(Özellikle kamu görevlisi olmasında fayda olmakla birlikte muhtar, azaları veya iki komşu refakat eşliğinde yapılmalıdır.)

- Arama yapılırken başından sonuna kadar fotoğraf ve kamera görüntüleri alınması gerekmektedir.

- Arama yerinde şüpheliye ait eşyalar ve malzemeler kullanılmamalıdır Şüpheliye ait tornavida, pense vs. kullanılmamalıdır.)

-Arama esnasında belirli yerden başlayıp atlamadan düzenli şekilde alanlar sıraya göre arama yapılmalıdır.

-Olay yerinde şüpheliye ait olmasa bile depolama malzemeleri alınmalıdır.

-İncelemek üzere alınan bilgisayar açık olsa dahi olay yerinde inceleme yapılmamalıdır.

-CD-DVD-Flash Bellekler muhafaza altına alınarak taşınmalıdır. (Şüphelinin her daim zarar verebileceği unutulmalıdır.)

-Arama tutanak yapılarak bitirilmelidir. Tutanak ayrıntılı olmalıdır. (Materyalin rengi, cinsi, markası, IMEI numaraları yazılmalıdır.)

-Alınan materyal delil poşetlerine konulmalıdır.

- Personelin delil bütünlüğünü bozacak tutum ve davranışlardan kaçınması gerektiği unutturulmamalıdır.

-Görevli personel gerekli teknik aksam, alet çantası vs. alıp gitmelidir.

3. İNCELEME AŞAMASI:

- Olay yerinden şüphelilerinde getirileceği durumlarda bilgisayarlar alınır.

- Olayda elde edilen deliller gözaltı süresince tamamlanamayacağı ve inceleme raporu bitmeyeceği değerlendirildiği takdirde ön inceleme raporu hazırlanmalıdır.

-İmage alınma işlemi sonrası ön inceleme veya inceleme raporu hazırlanmalıdır.

-İnceleme yapıldıktan sonra ilgili Büro/Şubeye hâkim kişilere değerlendirmek üzere vermelidir.

-Şüpheli ve avukatının alınan dijital materyalden kopya istemesi durumunda CMK 134 uyarınca uygun zamanda mutlaka bir örneğinin verilmesi gerekmektedir.

Alınan materyal özelliklerine göre yapılması gerekenler:

Bilgisayar alınması durumunda:

-Arama sırasında bilgisayara müdahale durumunda şüpheliden yardım alınmamalıdır. (Şüphelinin bilgisayara müdahale etme durumu ortadan kaldırılmalıdır.)

-Bilgisayar açık ise fotoğrafı çekilmelidir.

- Bilgisayar açık ise kullanılmamalı ve kapatılırsa komut olarak yapılmamalı, fişten elektrik bağlantısı kesilmelidir.

-Yazıcı bilgisayara bağlı ise yazıcının belge yazdırma haznesi kontrol edilmesi gerekmektedir. Yazı veya belge yoksa yazıcıda bekleyen bir yazı olabileceği düşünülmeli ve yazıcının hafızası kontrol edilmelidir.

-Tutanakta bilgisayarın durumu (açık veya kapalı olma durumu), markası, modeli, donanımları yazılmalıdır.

Flash bellek alınması durumunda:

-Üst arama sırasında veya herhangi bir yerde flash bellek veya USB girişi olan her şey tutanakta belirtilmesi gerekir. İncelemek üzere el konulur.

-Tutanakta varsa seri numaraları belirtilir. Flash Belleklerin çeşitli biçimlerde bulunabileceği unutulmaması gerekir. Çakmak, kart, saat, kalem vs. şekiller de tutanağa belirtilmesi gerekmektedir.

-MP3 Player, İpod gibi cihazlarda flash bellek kapsamında değerlendirmeli ve veri depolanabileceği unutulmamalıdır.

- Flash bellek şifresinin bulunup bulunmadığı sorulmalı varsa tutanağa geçilmesi gerekmektedir.

Cd/dvd/Videokaset alınması durumunda:

- CD/DVD/Video Kasetler numaralandırılıp el konulması gerekmektedir.

-Alınan CD/DVD/Video Kasetler için şüphelinin parafının alınması yararlı olacaktır.

Hard disk alınması durumunda:

- Arama sırasında bulunan hard diskler korunaklı taşınmalıdır. Hassas ve çabuk kaybolan bilgiler olabileceğinden delillerin bozulmamasına özen gösterilmelidir.

- Arama sırasında bulunan hard diskler bilgisayara bağlı olsun olmasın el konulmalıdır ve tutanakta marka/model/seri numaraları belirtilmesi gerekmektedir.(Bilgisayarın kasa kısmı mutlaka kontrol edilmelidir. Fazladan hard disk çıkma olasılığı unutulmamalıdır.)

Fotoğraf makinesi veya kamera alınması durumunda:

-Günümüzde fotoğraf makinaları ve kameralarda veri depolayabilmektedirler. Veri depolanabilen her materyal delil olabileceğinden el konulması gerekmektedir.

-Hafıza kartı harici dâhili hafıza kartı varsa bu da tutanakta belirtilmelidir.

-Bu makinelerin yanındaki aparatları ile el konulması inceleme aşamasında kolaylık sağlayacaktır. El konulacaksa tutanakta belirtilmelidir. Makinelerin ayırt edici özellikleri tutanakta yazılmalıdır.

- Bu makinelerin el konulmaları yapılırken sesli veya görsel olarak olay yerinde kayıt altına almakta fayda olabilmektedir. (Bazı makinelerin seri numaraları olmayabilir veya silinmiş olabileceği düşülmelidir.)

- Bu makinelerin içerisinden çıkan hafıza kartları ve dâhili kartları tutanakta belirtilmeli, şifreleri var ise temin edilmelidir.

Diğer birimlerin (terör-narkotik-kaçakçılık vb) siber personelinden yardım talebinde bulunurken alması gereken tedbirler:

-İnceleme yapacak siber polisine yararlı olacak her türlü not iletilmelidir.

-Şirket veya kurum gibi yerde arama yapılıyorsa şirket/kurum yetkilisi veya şirket/kurum bilgi işlem personelinden bilgi alınmalı ancak müdahale ettirilmemelidir.

-Adli makamları da inceleme konusunda bilinçlendirmekte fayda vardır.

5. TÜRKİYE'NİN SİBER GÜVENLİK FARKINDALIK DURUMU VE TÜRKİYE'NİN GÜVENLİK POLİTİKALARINA ETKİLERİ

Türkiye'nin resmi siber güvenlik kurumları temelde üç ana amaç çerçevesinde örgütlendirilmiştir. Bu ana amaçların ilk grubunda olanlar siber suçlarla mücadele edip istihbarı çalışmalar yapma amaçlanmaktadır. Bu kurumlar İçişleri Bakanlığına bağlı olan Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı, Jandarma ve Sahil Güvenlik Komutanlığı bünyesindeki birimlerdir. İkinci grupta olanlar ise Türkiye'nin kritik ve önemli altyapılarının siber güvenliğinin sağlayacak olan siber saldırı engelleme ve savunma kapasitelerini oluşturulmasıyla görevlendirilmiş BTK, TSK Siber Savunma Komutanlığı, MİT, TUBİTAK, AFAD gibi kurumlardır. Üçüncü grupta olanlar ise devlet destekli olan özel girişimlerdir. Bunlar ise; Savunma Teknolojileri Mühendislik, ASELSAN ve HAVELSAN bünyesindeki birimlerdir (Darıcılı, 2019:28).

Türkiye'de İçişleri Bakanlığı bünyesinde Emniyet Genel Müdürlüğüne bağlı 2011/2025 sayılı Bakanlar Kurulu Kararıyla kurulmuş olan Siber Suçlarla Mücadele Daire Başkanlığından önce Kaçakçılık ve Organize Suçlarla Mücadele Dairesi bilişim suçlarıyla görevlendirilmişti. Kaçakçılık ve Organize Suçlarla Mücadele Dairesinin bilişim suçları

ile alakalı 2011 verilerine bakıldığında 2007 ve 2011 yılları arasında bilişim suçlarının yükselen bir ivme şeklinde ve arttığı görülecektir (Hekim & Başıbüyük, 2013: 144-146).

İnsan haklarının ihlal olmaması için herkese sorumluluk düşse de asıl olarak devletin büyük sorumluluğu vardır. Devletin kendi sorumluluğundaki topraklarında ve yargı yetkisi olan topraklarında bunu sağlamak yükümlülüğü vardır. Siber saldırılarda özellikle yetkisiz erişim olan hacklemeler, kötücül yazılımlar ile zarar vermeler çoğu zaman devletin sınırları dışından da gelebilmektedir. Bu sebeple insan haklarının korunması için ve gerçek bir siber güvenlik sağlamak için farklı güçlere sahip aktörlerin, devletlerin, devlet dışı kuruluşların ve şirketlerin anlaşmasına ve birlikte hareket etmesine ihtiyaç vardır.

Türkiye de siber güvenlik olaylarına müdahale için ulusal ve uluslararası koordinasyon amacıyla USOM yani "Ulusal Siber Olaylara Müdahale Merkezi" kurulmuştur. Bu birim, Telekomünikasyon İletişim Başkanlığı (TİB) bünyesinde oluşturulmuştur (www.btk.gov.tr).

BTK bünyesinde olan Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT), kendisine ulaşan ihbarları değerlendirerek tehditleri bertaraf etmek için çalışmaktadır. Gerekli gördüğünde Kamu Kurum ve özel kişiler ile ilgili koordinasyon kurar. İhbarların çözüm sürecine kadar takibini yaparak çözüm üretir ve gerekli gördüğünde siber güvenlik tatbikatları yaparak kamu kurumlarının ve kuruluşlarının siber saldırılara karşı farkındalığını geliştirir (www.usom.gov.tr).

Bilgi Teknolojileri ve İletişim Kurumunun sunmuş olduğu "İnternet Bilgi İhbar Merkezi" hizmeti dikkate değerdir. Buna göre 5651 sayılı yasa uyarınca: İntihara yönlendirme, Çocukların cinsel istismarı, Uyuşturucu veya uyarıcı madde kullanımının kolaylaştırılması, Sağlık için tehlikeli madde temini, Müstehcenlik, Fuhuş, Kumar oynanması için yer ve imkân sağlanması, Atatürk aleyhine işlenen suçlar ile ilgili yeterli şüphe oluştuğu takdirde internet uzantılarını yazarak içerikleri, İhbar Web'e giriş yaparak şikâyette veya ihbarda bulunulabilmektedir (www.ihbarweb.org.tr).

İnsanların günümüzde yoğun olarak kullandığı internette suçlar da işlenebilmektedir. Suçla mücadele için ihbarların büyük önemi vardır. Bu sebeple Bilgi

Teknolojileri ve İletişim Kurumunun sağlamış olduğu bu hizmet olumlu olup daha da geliştirilebilir. Örnek vermek gerekirse ihbarların akıbeti hakkında internet sayfalarında yayın yapılabilir veya zararlı uzantıların tespiti ve hangi işlemlerin yapıldığı paylaşılabilir.

USOM siber saldırılara karşılık yerli ve milli imkânlarla anlık olarak 16 milyon IP'yi taramakta olup ülke güvenliği için katkılar sağlamaktadır. Günümüzde hızla artmış olan "oltalama saldırıları"nda kullanılan sahte siteler USOM tarafından belirlenerek engellenmektedir. Resmi ve özel kurumlarda yer alan siber olaylara müdahale ekipleri siber saldırıları engellemeye çalışmaktadır. 150 kişilik uzman ekip 7/24 görev yapmaktadır. BTK ve Aselsan iş birliğiyle geliştirilen Milli Monitör Merkezi ile sivil veya askeri telsizlerde haberleşme kanallarını karıştırabilecek zararlı ve kötücül yayınları ihbar gerekmeksizin tespit edilebilmektedir(www.trthaber.com).

Ulaştırma ve Altyapı Bakan Yardımcısı Ömer Fatih Sayan'ın ifadesine ve belirtmesine göre Türkiye'ye geçen yılda 150 bin siber saldırı gerçekleşmiş olup bu saldırılar bir önceki yılın iki katı olduğu dikkat çekicidir (www.aa.com.tr). İnternette saldırılar ve siber olaylar giderek artmaya devam edecektir. Bunun için hazır olunması gerekmektedir. Sadece yetişmiş insan gücünden değil vatandaşların bilinçlendirilip farkındalık çalışmalarının da artması gerekmektedir. Siber saldırıların önlenmesi için alt yapı çalışmalarının ve güvenlik önlemlerinin alınabilmesi için yeterli kaynak ve bütçelerinde ayrılması gerekmektedir.

Siber güvenlik eğitimleri teşvik edilmeli ve yüksek lisans, doktora seviyesinde siber güvenlik kürsüleri ve bölümleri oluşturulmalıdır. Türkçe kaynak eksiğinin giderilmesi ve alanda geçen kavramların Türkçeye kazandırılması için ilgili kurumların çalışması gerekmektedir. Hackerların ve sistemi kıran, etkisiz kılan kişiler devlete kazandırılarak yeteneklerinden faydalanması için projeler dahi geliştirilmelidir. Türkiye'nin sahip olduğu genç nüfuz potansiyeli bu konular için eğitilip güvenliğin güçlendirilmesine katkı sağlanmalıdır.

Kritik kurumların, özellikle savunma, enerji, gıda, su ile ilgili kurumlara bilişim desteği en üst seviyede verilmesi gerekmektedir. Bunun için tüm devletler önlemler almaktadır. Bu konuya önem verilmesi ülke savunması ve yönetimi için önemlidir. Sadece

saldırıyı engellemeye yönelik değil saldırı gerçekleştiğinde acil durum planları veya kriz yönetimi ile ilgili de çalışma yapılması gerekmektedir.

Türkiye'nin siber güvenliğinin arttırılması için müdahale kabiliyetinin arttırılması gerekmektedir. Her kurum ve birimde teknoloji ile ilgili bir departman harici bir müdahale birimi olması, sızma testleri yapıyor olması ve uzman personelin güncel bilgileriyle görev yapması önem arz etmektedir.

Rusya, Çin ve Amerika Birleşik Devletlerinin siber güvenlik belgelerinde veya siber uzay alanındaki yatırımları ve planlamalarını açıkça belirtmekten kaçınmakta veya sınırlı bilgi vermektedirler. Türkiye'de bu tavra dikkat etmeli ve planlamalarını gerekirse müttefikleriyle dahi paylaşmamalıdır.

Günlük hayatımızın her aşamasına girmiş bulunan teknolojik ürünler hayatımızı kolaylaştırırken bazı olumsuz yan etkiler sebepleriyle bir şeyler alıp götürmektedir. Örnek vermek gerekirse televizyon izleme çok yaygın kullanılan ve haber almada yararlı bir iletişim aracıdır. Tabir olarak "dünyayı evimize getirir" denilir. Ancak çok fazla izlenirse bağımlılık oluşacak ve ruhsal sağlık açısından tehlike oluşturacakken, çok yakından televizyon izlenirse veya uzun süre televizyona bakılırsa göz sağlığını bozacağından fiziksel sağlık açısından tehlike oluşturacaktır.

Televizyon ile sosyalleşerek büyüyen çocuklarda şiddet, cinsellik veya suça özendirici hareketler görülür. Bu televizyon örneğini cep telefonu, bilgisayar, tablet olarak verdiğimizde teknolojik ürünlerin yararı kadar masum olmayacak kadar zararları olduğunu, özellikle bilinçli kullanılmazsa zararlı olduğu görülecektir.

Günümüz Türkiye'sinde teknolojinin kullanımı azımsanmayacak derecede artmıştır. Örneğin anket sorularından 19. Soru "Bilgi güvenliği ihlali olduğunda bu ihlali kime bildirirsiniz?". Bunu sormaktaki amaç aslında internet kullan kişiler aktivitelerinin ve bilgilerinin birileri tarafından izlendiği veya çalındığı endişesi ile karşılaşırsa nasıl davranacaklarını ölçmektir. Gerçekten de telefon veya bilgisayar kullanan hemen hemen herkes izlenip veya dinlendiğinden kuşku duymaktadırlar.

5.1: Araştırmada Kullanılacak kavramlar

Araştırma yaparken kullanılan kelimeler ve anlamları aşağıda verilecektir:

Siber zorbalık: Teknolojik bilgi gerektirerek ve teknolojik bilgi kullanılarak akıllı telefon uygulamaları, e-posta, SMS, sohbet odaları, forumlar, bloglar ve diğer sosyal ağlarda kişilerin mağdur edilmesidir (Sayımer ve Akça, 2017:4).

İhbar web: Bilgi Teknolojileri ve İletişim Kurumunun sağlamış olduğu bir hizmettir. 5651 sayılı yasa uyarınca belirli suçlarla internette paylaşım görülmesi durumunda yeterli şüphe oluşursa internet uzantılarını yazarak içerikleri, İhbar Web'e giriş yaparak ihbar yapılabilir.

Siber güvenlik çalışanı veya bilgi işlem uzmanı: Bilgisayar sistemlerini kuran, yöneten, sistemleri test eden, güvenlik önlemlerini alan personel veya çalışanlardır.

Uzaktan erişim sağlamak (AnyDesk Uzaktan PC erişim, VPN, Bulut sunucu vs.): Uzak masaüstü yazılımı olarak bilinir ve iş bilgisayarına evden bağlanma kolaylığı sağlamaktadır. VPN ise ip değişikliği sağlayarak ip gizlemeye yarayan sunucudur.

5.2: Araştırmanın Sınırlılıkları, Amaçları ve Kullanılan Yöntem

Araştırmada siber güvenlik alanında farkındalık algısı anlamında ölçüm yapmayı amaçlamaktadır. Araştırma belli bir kesim veya kişiler merkez alınarak yapılmamıştır. İnternet ortamında Google Docs- Google Formlar üzerinde anket oluşturulup paylaşım yoluyla kişilere ulaştırılmıştır. Anket cevapları sırasında isim-soy isim alınmamış olup katılımcıların etki altında kalmadan rahat bir şekilde cevaplamaları istenilmiştir.

Anket uygulanırken yüksek lisans tezi kapsamında araştırmanın yapıldığı belirtilmiştir. Bu da anketin şeffaf yapıldığı ve ne için yapıldığı hakkında kafalarda soru işareti bırakmamak adına belirtilmiştir. Anket sorularının cevapları analiz edilerek yorumlanmaya çalışılmıştır.

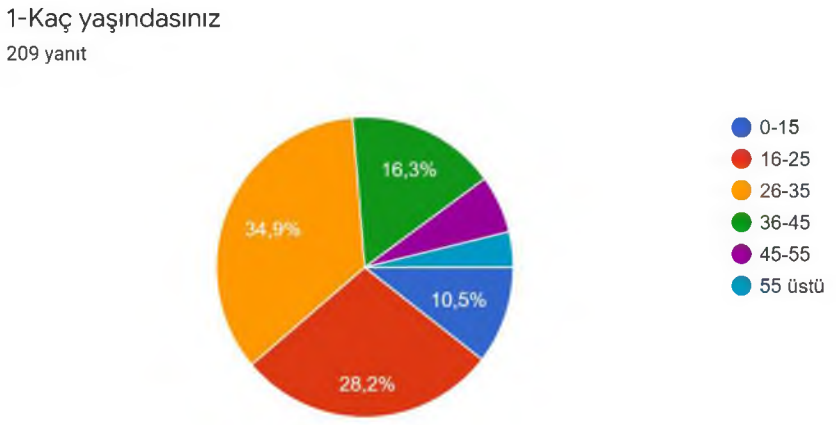
5.3: Araştırmanın Örneklemi ve Soruların Belirlenmesinde Yöntem

Araştırmanın örneklemi çalışmaya katkı sağlayacak gönüllülük esasına dayanarak 210 katılımcıya online olarak gönderilerek internet üzerinden anket yapılmıştır (https://docs.google.com/forms/d/1nQLnSM0iTEgu1eigLpGgdGncESSwWIC83De6xTX5CtM/edit).

Sorular belirlenirken siber güvenlik alanında farkındalıklar ölçülecek düzeyde ve her türlü düzeye hitap edebilecek sorular sorulmaya çalışılmıştır. Anket soruları ve sorular hakkında seçim ve yöntem bilgisi aşağıda sunulmuştur.

5.3.1: Katılımcıların Yaş Aralığına Göre Dağılımı

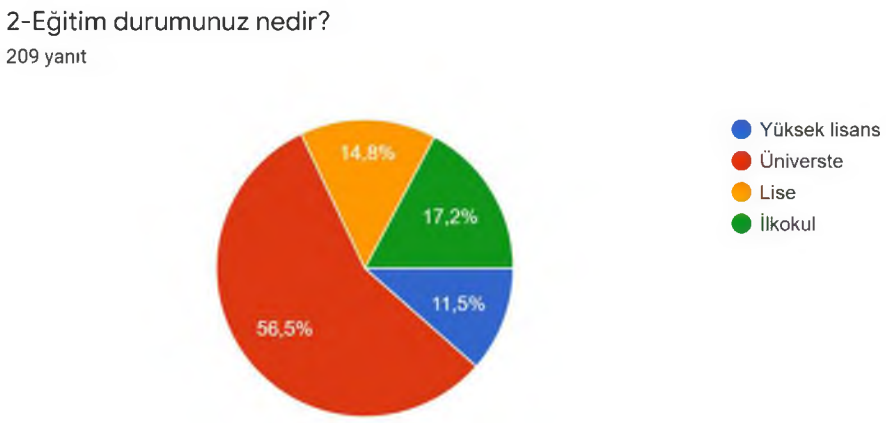
Bu soru seçilirken ankete hangi yaş düzeyinde katılımcı katılmış bu ölçülmek istenilmiştir. Buna göre 16-35 yaş arasındaki katılımcıların ve internet-teknoloji ile ilgilenen kitlenin çoğunlukta olması dikkat çekicidir.



Şekil 5.1. Katılımcıların Yaş Aralığına Göre Dağılımı

5.3.2: Katılımcıların Eğitim Durumuna Göre Dağılımı

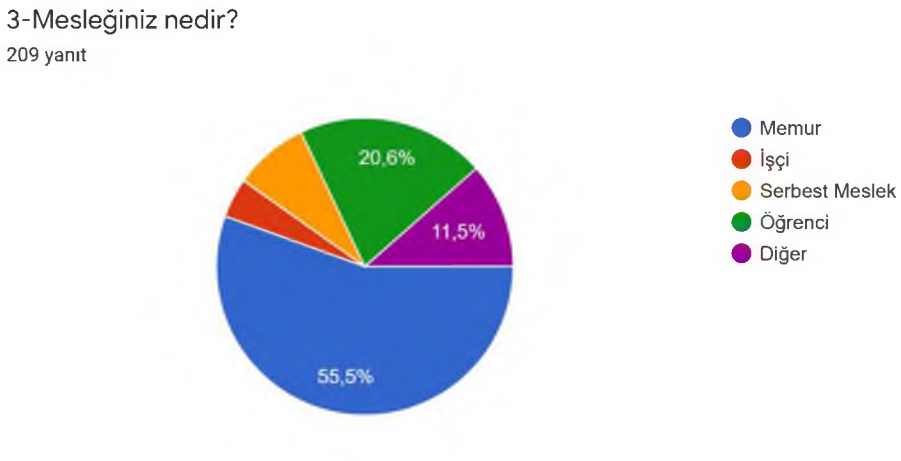
Bu soru seçilirken ankete hangi eğitim düzeyinde katılımcının olduğu ölçülmek istenilmiştir. Burada da özellikle Üniversite mezunu katılımcıların yüksek bir orana sahip olması dikkat çekicidir.



Şekil 5.2. Katılımcıların Eğitim Durumuna Göre Dağılımı

5.3.3: Katılımcıların Meslek Durumuna Göre Dağılımı

Bu soru seçilirken ankete hangi meslekte katılımcının olduğu tespit edilmek istenilmiştir. Burada da özellikle memur katılımcıların yüksek bir orana sahip olması dikkat çekicidir.



Şekil 5.3. Katılımcıların Meslek Durumuna Göre Dağılımı

5.3.4: Katılımcıların Problem Algı Durumu

Bu soru seçilirken ankete katılanların Türkiye'de sorun ve problem algılarının ne olduğu ölçülmek istenilmiştir. Burada da özellikle belli başlı eğitim-iş-sağlık-güvenlik-yabancı düşmanlığı gibi seçenekler sunulmuş olup eğitimi problem olarak gören katılımcıların yüksek bir orana sahip olması dikkat çekicidir. Burada da güvenliği bir problem olarak görme %10,6 ile düşük kalmıştır.

Şekil 5.4. Katılımcıların Problem Algı Durumu

5.3.5: Katılımcıların Olumlu Bakış Açısı (Türkiye'de)

Bu soru seçilirken ankete katılanların Türkiye'de olumlu gördüğü alanların hangisi olduğu ölçülmek istenilmiştir. Burada da özellikle iklim ve çevreyi olumlu olarak gören katılımcıların yüksek bir orana sahip olması dikkat çekicidir.

Şekil 5.5. Katılımcıların Olumlu Bakış Açısı (Türkiye'de)

5.3.6: Katılımcıların İş Yaşamlarında Problem Algı Durumu

Bu soru seçilirken ankete katılanların iş yaşamlarında yaşadıkları problemlerin neler olduğu ve bunda güvenliğin hangi oranda olduğu ölçülmek istenilmiştir. Burada da özellikle iş şartlarının ve düşük ücreti problem olarak gören katılımcıların yüksek bir orana sahip olması dikkat çekicidir.

Şekil 5.6. Katılımcıların İş Yaşamlarında Problem Algı Durumu

5.3.7: Katılımcıların Türkiye'nin Güvenliği İle İlgili Bakış Açıları

Bu soru seçilirken ankete katılanların Türkiye'de güvenliğe bakış açısı ölçülmek istenilmiştir. Burada da özellikle güvenliğin orta olarak gören katılımcıların yüksek bir orana sahip olması dikkat çekicidir.

Şekil 5.7. Katılımcıların İş Yaşamlarında Problem Algı Durumu

5.3.8: Katılımcıların Türkiye'nin Siber Güvenliği İle İlgili Bakış Açısı

Bu soru seçilirken ankete katılanların Siber güvenliğine bakış açısı ölçülmek istenilmiştir. Burada da özellikle siber güvenliğin orta olarak gören katılımcıların yüksek bir orana sahip olması dikkat çekicidir. Bu soru bir önceki soruyla bağlantılı olup güvenlik ile siber güvenlik oranlarının birbirine yakın olması dikkat çekicidir.

Şekil 5.8. Katılımcıların Türkiye'nin Siber Güvenliği İle İlgili Bakış Açısı

5.3.9: Katılımcıların Türkiye'nin Siber Güvenlik Farkındalığı İle İlgili Bakış Açısı

Bu soru seçilirken ankete katılanların Siber güvenlik farkındalığına karşı yapılanların yeterli olup olmaması ve bu bilincin yeterli seviyede yapılıp yapılmadığı ile

ilgili bakış açısı ölçülmek istenilmiştir. Burada da özellikle farkındalığı orta olarak gören katılımcıların yüksek bir orana sahip olması dikkat çekicidir. Bu demek oluyor ki hem eğitim camiası olarak hem de gerekli siber güvenlik birimlerinin farkındalık yönünde daha fazla çaba göstermesi gerektiği görülmektedir.

Şekil 5.9. Katılımcıların Türkiye'nin Siber Güvenlik Farkındalığı İle İlgili Bakış Açısı

5.3.10: Katılımcıların Daha Önce Bir Siber Suça Veya Siber Zorbalığa Maruz Kalma Durumu

Bu soru ile ankete katılanların siber mağduriyet yaşayıp yaşamadıkları öğrenilmek istenilmiştir. Sonuca göre ciddi bir oranda siber suça veya siber zorbalığa maruz kalındığı görülmüştür. Bu hem kamu kesiminin hem de özel kesimin üzerine görev ve sorumlulukların düştüğünü göstermiştir.

Şekil 5.10. Katılımcıların Daha Önce Bir Siber Suça Veya Siber Zorbalığa Maruz Kalma Durumu

5.3.11: Katılımcıların siber zorbalık yaparak birini mağdur etme durumu

Bu soru ile ankete katılanların başka birisine siber mağduriyet yaşatıp yaşatmadıkları öğrenilmek istenilmiştir. Sonuca göre ciddi bir oranda birilerini siber zorbalığa maruz bıraktığı görülmüştür. Tabi isim-soy isim alınmadan anket yapıldığı için katılanların doğruluk ve samimi beyanları alındığı düşünüldüğünden hareketle sadece mağduriyet değil aynı zamanda mağdur edenlerin sayısı ve suça yönelimlerin teknoloji ile arttığı söylenebilmektedir.

Şekil 5.11. Katılımcıların siber zorbalık yaparak birini mağdur etme durumu

5.3.12: Katılımcıların Bilgisayar Ve Cep Telefonu Kullanırken Aldığı Güvenlik Önlemleri

Bu soru ile ankete katılanların teknolojik alet kullanırken gerekli güvenlik önlemlerini alıp almadıkları araştırılmak istenilmiştir. Çok büyük bir oran bir önlem olmadan kullanıyor olması bu alanın istismara açıklığını göz önüne sermektedir.

Şekil 5.12. Katılımcıların Bilgisayar Ve Cep Telefonu Kullanırken Aldığı Güvenlik Önlemleri

5.3.13: Katılımcıların (Çocukları Varsa) Çocuklarına Siber Tehditlere Karşı Farkındalık Eğitimi Verme Durumu

Bu soru ile ankete katılanların özellikle çocukları olan katılımcıların çocuklarına siber tehditlere karşı farkındalık eğitimi verip vermedikleri ve konuyu ne kadar önemsedikleri ölçülmek istenilmiştir. Çok büyük bir oran eğitim verilmemiş olması bu alana verilen önemin eksikliğini gözler önüne sermiştir. Bu sebeple devletin makro politikalar alarak gerekli farkındalık bilinci oluşturması gerekliliği çıkarılmıştır.

Şekil 5.13. Katılımcıların (Çocukları Varsa) Çocuklarına Siber Tehditlere Karşı Farkındalık Eğitimi Verme Durumu

5.3.14: Katılımcıların (Çocukları Varsa) çocuklarının siber tehditlere karşı öğrenim gördüğü okulda farkındalık eğitimi konusundaki görüşleri

Bu soru ile ankete katılanların özellikle çocuklarının siber tehditlere karşı öğrenim gördüğü okulda farkındalık eğitimi verilip verilmedikleri ve konunun ne kadar takipçisi oldukları ölçülmek istenilmiştir. Çok büyük bir oran eğitim verilmemiş olması bu alana verilen önemin eksikliğini gözler önüne sermiştir. Bu sebeple özellikle Milli Eğitim Bakanlığı başta olmak üzere tüm kurumlara görevler düşmektedir. Sadece müfredata konu ekleyerek değil etkili mücadele için denetim ve gözetim mekanizmaları oluşturarak bu alandaki eksiklikleri gidermesi gerekmektedir.

Şekil 5.14. Katılımcıların (Çocukları Varsa) çocuklarının siber tehditlere karşı öğrenim gördüğü okulda farkındalık eğitimi konusundaki görüşleri

5.3.15: Katılımcıların Bilgi Teknolojileri Ve İletişim Kurumunun Sunmuş Olduğu İhbar web İle İlgili Farkındalık Durumu

Bu soru ile ankete katılanların Bilgi Teknolojileri ve İletişim Kurumunun sağlamış olduğu bir hizmetten haberlerinin olup olmadığı tespit edilmeye çalışılmıştır. 5651 sayılı yasa uyarınca belirli suçlarla internette paylaşım görülmesi durumunda yeterli şüphe oluşursa internet uzantılarını yazarak içerikleri, İhbar Web'e giriş yaparak ihbar yapılabilir.

Şekil 5.15. Katılımcıların Bilgi Teknolojileri Ve İletişim Kurumunun Sunmuş Olduğu İhbar web İle İlgili Farkındalık Durumu

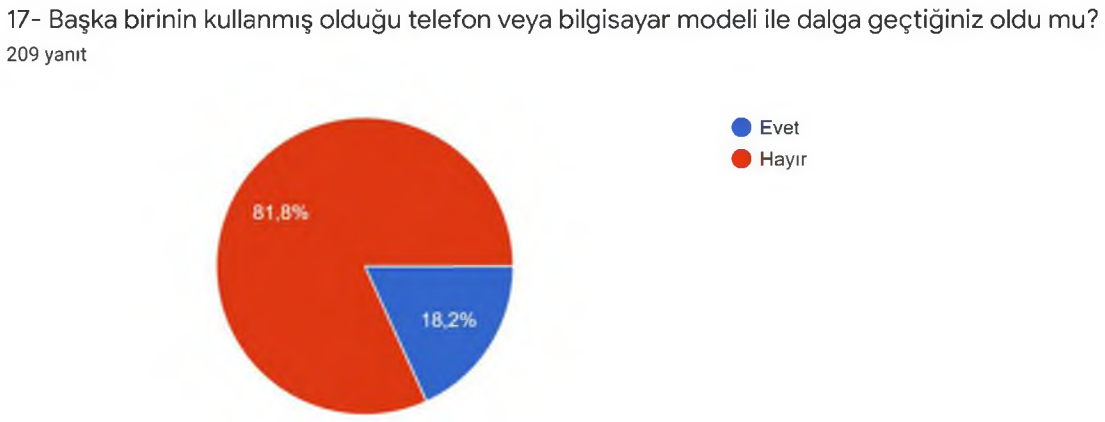
5.3.16: Katılımcıların Bir Siber Suça Maruz Kalma Durumunda Farkındalık Durumu

Bu soru ile ankete katılanların siber suçla karşılaştıklarında yeterli farkındalığa sahip mi ve suça maruz kaldıklarında ne yapacaklarını bilip bilmedikleri sorulmuştur. Ne yapacaklarını bilmeyenlerin oranı yüksek çıkması dikkat çekicidir.

Şekil 5.16. Katılımcıların Bir Siber Suça Maruz Kalma Durumunda Farkındalık Durumu

5.3.17: Katılımcıların Başka Birinin Kullanmış Olduğu Telefon Veya Bilgisayar Modeli İle Dalga Geçme Durumu

Bu soru ile ankete katılanların teknolojiyi takip durumu, yeni ve güncel cihaz kullanıp kullanmadıkları ve eski model cihaz kullanan kişileri dalga konusu yapıp yapmadıkları sorulmuştur.



Şekil 5.17. Katılımcıların Başka Birinin Kullanmış Olduğu Telefon Veya Bilgisayar Modeli İle Dalga Geçme Durumu

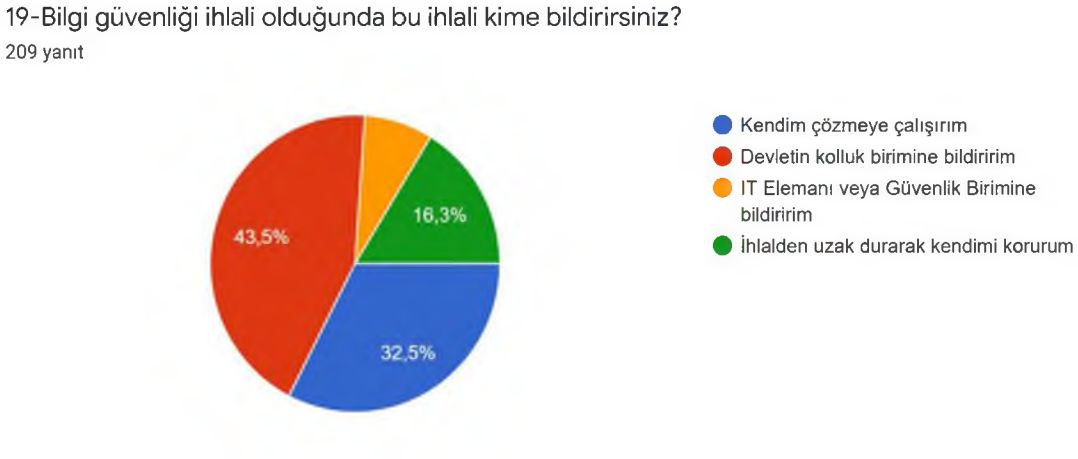
5.3.18: Katılımcıların İş Yerlerinde Düzenli İşleyen Siber Güvenlik Çalışanı Veya Bilgi İşlem Uzmanı İle Çalışma Durumları

Bu soru ile ankete katılanların iş yerlerinde siber güvenlik çalışanının olup olmadığı araştırılmak istenilmiştir. Yüksek ölçüde hayır çıkması veya çalışsa bile haberlerinin olmaması da siber farkındalığın yeterince gelişmediğinin göstergesidir.

Şekil 5.18. Katılımcıların İş Yerlerinde Düzenli İşleyen Siber Güvenlik Çalışanı Veya Bilgi İşlem Uzmanı İle Çalışma Durumları

5.3.19: Katılımcıların Bilgi Güvenliği İhlali Konusundaki Farkındalığı

Bu soru ile ankete katılanların bilgi güvenliği ihlali konusundaki farkındalığı ölçülmeye çalışılmıştır. Burada da devletin kolluk birimin bildiririm yüksek çıkması dikkat çekmiştir.

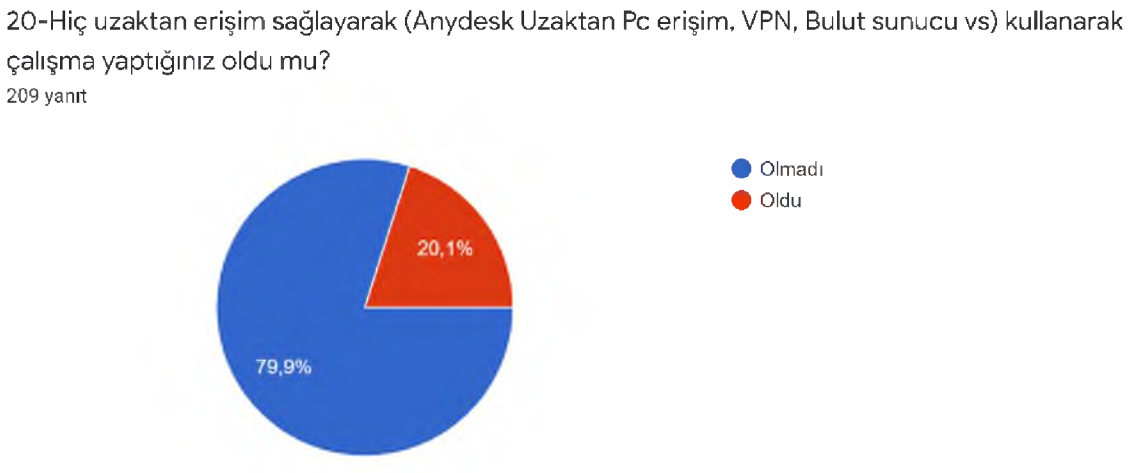


Şekil 5.19: Katılımcıların Bilgi Güvenliği İhlali Konusundaki Farkındalığı

5.3.20: Katılımcıların Uzaktan Erişim Sağlayarak Çalışma Konusundaki Farkındalığı

Bu soru ile ankete katılanların Uzaktan Erişim ile siber bilgi düzeyleri ve teknolojiyi ne düzeyde kullandıkları ölçülmek istenilmiştir. Uzak masaüstü yazılımı

olarak bilinen programlar ile iş bilgisayarına evden bağlanma kolaylığı sağlamakta olup VPN ile de ip değişikliği sağlayarak ip gizlemeye yarayan sunucu hizmetidir.



Şekil 5.20: Katılımcıların Uzaktan Erişim Sağlayarak Çalışma Konusundaki Farkındalığı

5.4: Araştırmanın Bulguları

Araştırmanın bulgularını maddeler halinde sıralayacak olursak:

a) Memur katılımcıların yüksek bir orana sahip olması

b) Siber güvenliğin orta olarak gören katılımcıların yüksek bir orana sahip olması dikkat çekicidir.

c) Siber farkındalığı orta olarak gören katılımcıların yüksek bir orana sahip olması dikkat çekicidir.

d) Ciddi bir oranda siber suça veya siber zorbalığa maruz kalındığı görülmüştür.

e) Çok büyük bir oran cep telefon ve bilgisayarlarında bir önlem olmadan kullanıyor olması bu alanın istismara açıklığını göz önüne sermektedir.

f) Katılımcıların çocuklarına çok büyük bir oran eğitim verilmemiş olması bu alana verilen önemin eksikliğini gözler önüne sermiştir.

g) Katılımcıların siber suçla karşılaştıklarında yeterli farkındalığa sahip mi ve suça maruz kaldıklarında ne yapacaklarını bilip bilmedikleri sorulduğunda ne yapacaklarını bilmeyenlerin oranı yüksek çıkması dikkat çekicidir.

h) katılımcıların bilgi güvenliği ihlali konusundaki farkındalığı ölçülmeye çalışılmış ve bir suç ile karşılaştıklarında devletin kolluk birimine bildiririm diyenlerin yüksek çıkması dikkat çekmiştir.

5.5: Araştırmada Karşılaşılan Zorluklar

Araştırma internet üzerinden yapıldığından fiziki iletişim kurma veya maliyete katlanmak gibi zorluklar olmamıştır. Ancak tek dikkat edici zorluk bazı soruların yanıtlanıp bazılarının yanıtlanmaması olmuştur. Bunda da bazı soruların ankete katılanların kişisel durumlarından kaynaklanmaktadır. Örnek vermek gerekirse bazı sorularda "Çocuklarınız var ise" diye başlamakta olup sadece çocukları olan katılımcıların konu üzerindeki algısı ölçülmüştür.

5.6: Araştırmada Toplanan Verilerin Analizi ve Tartışması

Bu çalışmada birincil ve ikincil kaynaklar kullanılmıştır. Birincil kaynak olarak anket uygulaması yapılmıştır. İkincil kaynak olarak ise literatürde yayınlanmış kitap, makale gibi kaynaklardan yararlanılmıştır.

Araştırmada veri toplamak ve verileri analiz etmek için anket yapılmıştır. Anket sonuçları analiz edilerek tablo oluşturulmuştur. Daha sonra bu tablolardan sonuçlar analiz edilerek varsayımlar yapılmıştır.

Sonuç olarak anket araştırmasında günümüzde ciddi bir oranda siber suça veya siber zorbalığa maruz kalındığı, siber güvenliği ve siber farkındalığın yeterli olmadığı, çok büyük bir oranda cep telefon ve bilgisayarlarında bir önlem olmadan kullanan kişilerin olması ve bu sebeple istismara açıklığını göz önüne sermektedir.

6. SONUÇ

Yeni teknolojiler ve yeni icatlar ile siber uzay günden güne hayatımızdaki önemi artmaktadır. Yeni teknolojilerin cazibesi ve kolaylığı olduğu kadar beraberinde getirdiği riskler ve tehditler de artış göstermektedir. Dijitalleşen ve özellikle internetleşen her şey mutlaka bir güvenlik açığı oluşturmaktadır. Buna rağmen insanlar internetten vazgeçememekte ve artan şekilde ona bağımlı hale gelmiştir.

Siber alanın özellikle küreselleşme ile birlikte ve teknolojinin her alana yayılıp bunun psikolojiden sosyolojiye, ticaretten ekonomiye kadar birçok alanda belirleyici bir unsur haline gelmesiyle sosyal bilimcilerde bu alanda çalışmalara başlamışlardır. Siber güvenliğin ve siber alanın son yıllarda gelişmesine rağmen hala işin başında olduğu da gerçekliktir. Bunun siber uzayın doğası gereği sürekli gelişen teknolojinin olması kadar siber ile ilgili durumların tanımlanmasının ve kavramsallaşmanın güçlüğü de etkilidir. Siber uzay interaktif bir alan olup kullanıcılar ondan yararlanmakla birlikte ona katkı da sağlamaktadır. Bu sebeple siber uzay ile ilgili kavramlar ve literatür sürekli değişmekte ve gelişmektedir. Yeni ifadeler ve kullanılan emojiler ile diller, kültürler ve sosyal olarak insanlık etkilenmektedir ve etkilenmeye devam edecektir.

Büyük devrimler veya önemli olaylar insan haklarını geliştirmiştir. İnsan Hakları Sözleşmeleri insanın kazandığı tarihsel kazanımları ifade etmektedir. Bu sözleşmeleri benimseyip uygulamak insan olmanın ve insanlık tarihi adına değerlidir. İnsan hakları sadece fiziksel olarak insan hakkı ihlal edilmemekte, internet ve sanal ortamda da insan hakları ihlal edilebilmektedir. Bu sebeple insan hakkı ihlallerinin önlenmesi için gerekli düzenlemeler interneti de kapsayacak şekilde yapılması gereklidir.

Bu çalışmanın yapılmasındaki amaç, Türkiye'de siber güvenlik politikaları oluşturulurken güvenlik meselesi olarak algılanmasında yeterli olmayıp vatandaşların siber tehdit algısının oluşmadığını ispatlamaktır. Bunu desteklemek içinde anket yapma yoluna gidilmiştir. Ayrıca Türkiye'nin bu yeni tehdit algısına karşı güvenlik politikalarının yeterli seviyede ve önemde olmadığı düşünülmektedir. Bu sebeple çalışmanın başlığı siber güvenlik bağlamında yeni tehdit algılamalarının Türkiye'nin güvenlik politikalarına etkileri olarak belirlenmiştir.

Türkiye'nin siber güvenlik politikalarının güvenlikleştirme boyutu yeterli düzeyde değildir. Siber güvenlik pek ala güvenlikleştirilip olağan üstü tedbirler ve yasaklamalar getirilerek yapılabilir olsa bile bunun vatandaşlar tarafından bir tehdit olarak algılanması da gerekmektedir. Güvenlik teorilerinin genel olarak tarihine bakıldığında devlet merkezli güvenlik anlayışından bireyi önceleyen güvenlik anlayışına doğru bir yol izlemiştir. Günümüzde sadece devletin siber güvenliği değil; kurumların, kuruluşların ve bireylerin siber güvenliği önem kazanmıştır. Ancak siber güvenliğe verilen önem yeterli düzeylere gelememiştir.

Vatandaşlar siber tehditlerle karşılaşınca ne yapacaklarını bilmemeleri durumu çok sık karşılaşılan durumdur. Siber tehditlerle mücadele ve siber saldırılara karşı güvenliği sağlamak için öncelikle siber saldırının anatomisinin bilinmesi gerekmektedir. Siber saldırıların bilinmesi doğal olarak nasıl tedbirler alınmasını bilmeye yararı olur. Hem teorik hem de pratik olarak siber güvenlik alanında akademik çalışmaların ağırlık kazanması da gerekmektedir. Sadece ortaöğretim düzeyi değil ilkokul düzeyinde bilgisayar ve siber güvenlik teknolojisi anlamında müfredatları hazırlanması gelecek için en önemli yatırımların başında gelecektir.

Gerçek kişiler için özel hayatın gizliliği ve mahremiyet alanın ihlali gibi temel insan haklarını ihlal ederken, devletler için ulusal güvenliklerini tehdit etmektedir. Bu sebeple bireylerden devletlere kadar mikro ve makro ölçekte siber güvenlik tedbirlerinin alınması hayati öneme sahiptir.

Siber savaş, siber saldırı, siber terörizm gibi kavramlar uluslararası hukuk nezdinde kabul görmesi, konu hakkında çalışmalar ve makalelere ihtiyaç duyulmaktadır. Ayrıca Birleşmiş Milletler nezdinde yeni düzenlemelere ve kuralların oluşturulmasına ihtiyaç duyulmaktadır. Kurallar konulurken siber saldırı ve savaş tanımları yapılması haricinde nasıl yaptırımların uygulanacağı da belirtilmelidir. Uluslararası Adalet Divanı, Uluslararası Ceza Mahkemesi, AİHS ve diğer uluslararası yargı divanlarında siber saldırı suçunu işlemiş devletler hakkında ve hatta devlet görevlileri hakkında yargılamalar yapılmalıdır.

Tarih boyunca güvenlik konusu hem hassas hem de önemli konular arasında gelmiştir. Uluslararası sistemde hâkim olan anarşik doğada devletler saldırı yaptığında saldırı yapan belirli olup gerektiği durumlarda yargı organlarında sorumluluk doğurmaktadır. Ancak siber

dünyada saldırının kaynağının kim-hangi devlet tarafından yapıldığının bilinmemesi sebepleriyle devletler siber güvenlik alanına yatırım yapmak zorundadırlar. Saldırganın bulunması insan haklarının önlenmesi açısından da önem taşımaktadır.

Nasıl ki 21. Yüzyıla gelirken soğuk savaş sona erip iki kutuplu sistem son bulmuşsa teknolojinin gelişimi ile birlikte birçok aktör güvenlik için tehdit haline gelmiştir. Devletler de sadece askeri unsurların değil siber saldırıların da tehdit olarak görüldüğü bir döneme girilmiştir. Tam anlamıyla siber saldırıları önlemek mümkün gözükmemekle birlikte devletler alacakları siber güvenlik önlemleri ve tedbirler ile zararları minimize edebilirler.

Ortam sanal olsa bile işlenen suç gerçek olup somut dünyada sonuç ve yaptırım doğurmaktadır. Dünya genelinde siber suçların işlenme oranları arttığı bilinmekte ve bu suçlardan mağdurlar arasında kişilerden özel veya kamu sektörüne kadar her kesim bulunabilmektedir. Özellikle bir hareket ile binlerce kişiyi mağdur edebilmesi özelliği sebebiyle kitle mağduriyeti yaratabilmektedir. En önemli özelliği ise bu suç türlerinde sınır aşma olgusu sık karşılaşılmakta ve bu da suçla mücadeleyi zorlaştırmaktadır.

Türkiye'de yasa koyucular kapsamlı olarak siber suçların yaptırımlarını arttırmak için çalışmalar yapmalı ve suçlarla etkin mücadele yöntemi geliştirilmelidir. Özellikle siber suçlara karşı yeni yöntemler geliştirilmeli ve teknik altyapıların güçlendirilmesi gerekmektedir. Tespit araçları ve mekanizmaları çoğaltılmalı, güvenlik ve hizmet sektörleri başta olmak üzere tüm sektörlerde siber güvenliğe verilen önem arttırılmalıdır.

Kamuoyunda sürekli siyasi, ekonomik ve spor gündemlerine öncelik verilmesi sebepleriyle siber güvenlik alanı hiçbir zaman gereken değeri görmemiştir. Örneğin bir banka sistemlerine siber saldırı ile büyük miktarlarda ve çok sayıda mağdurlu suçlar işlenebilmektedir. Ancak haberlerde fiziki banka soygunu daha fazla ilgi görebilmektedir. Böyle örnekler çoğaltılabilir.

Uluslararası ilişkilerde özellikle siber uzay anlamında devletlerarasında güvensizlik artmaktadır. Büyük devletler başta olmak üzere siber rekabetin arttığı günümüz dünyasında devletler teknoloji yarışına girmişlerdir. Özellikle güvenlik ikilemi yani ne kadar tedbir alınıp ne kadar saldırı yapılacağı dengesi devamlı değişmektedir.

Güvenlik teorilerinin tarihine bakıldığında devlet merkezli güvenlik anlayışından bireyi ve kurumları önceleyen güvenlik anlayışlarına doğru bir yol izlemiştir. Bu siber güvenlik anlamında ayrı bir önemi vardır. Günümüzde sadece devletin siber güvenliği değil; kurumların, kuruluşların ve bireylerin siber güvenliği de önem kazanmıştır.

Türkiye, siber akademik düzey ve pratik uygulamaları açısından ABD, Rusya, Japonya, Kore ve Çin ile karşılaştırıldığında zayıf olduğu görülecektir. Bu sebeple kendisini önce bu ülkelere karşı geliştirmesi ve bu ülkelerden gelebilecek siber tehditlere karşı korumaya alması gerekmektedir. Günümüzde siber güvenlik yatırımları ve çalışmaları hız kazanmıştır ve Türkiye'nin duyarsız kalmaması ve teknolojik yatırımlara hız vermesi gerekmektedir. Terör örgütleri, çıkar grupları ve sınır aşan suç işleyen örgütler siber saldırıları her an kullanabilmektedirler. Bu açıdan Türkiye yurt içi veya yurt dışı kaynaklı siber saldırılara karşı her daim hazır olmak zorundadır. Ayrıca Türkiye sadece kendi resmi kurumlarını değil ekonomik çıkarları gereği ticari şirket ve özel sektör girişimcilerini de korumak zorundadır.

Tüm bu sebeplerle Türkiye siber uzay kapasitesini geliştirmek zorundadır. Türkiye; siber güvenlik stratejisi, siber güvenlik eylem planları, siber güvenlik durum raporları ve eksiklileri belirleyerek gereksinim duyulacak her türlü önlemlerin alınması bir ihtiyaç değil artık zorunluluktur.

7. KAYNAKLAR

Acar,H. & Pekcandanoğlu, M.(2020). Analysis of Cyber Security and Cyber Espionage Policies, Türkiye Rusya Araştırmaları Dergisi 3(Yaz 2020).Et: 18.09.2020 (https://www.dergipark.org.tr/tr/pub/trad/issue/55699/745123).

Akarslan, H. (2015). Bilişim Suçları (2. Baskı), Seçkin Yayıncılık, Ankara.

Akca, E. B. &Sayımer, İ. & Salı, J.B. & Başak, B. E. (2014). Okulda Siber Zorbalığın Nedenleri, Türleri ve Medya Okuryazarlığı Eğitiminin Önleyici Çalışmalardaki Yeri, Elektronik Mesleki Gelişim ve Araştırma Dergisi (EJOIR), Cilt:2, Özel Sayı, S:17-30.

Aksaray,S. (2011). Siber Zorbalık, Ç.Ü. Sosyal Bilimler Enstitüsü Dergisi, Cilt 20(Sayı 2):Sayfa:405-432.

Akman, E. (2019). Akıllı Telefonsuz Kalma Korkusunun (Nomofobi) Akademik Başarıya Etkisi: Süleyman Demirel Üniversitesi Siyaset Bilimi ve Kamu Yönetimi Öğrencileri Üzerinden Bir Değerlendirme, AVRASYA Uluslararası Araştırmalar Dergisi, Cilt: 7 Sayı: 16 Sayfa: 256 – 275.

Akyeşilmen, N. (2018). Disiplinler arası Bir Yaklaşımla Siber Politika ve Siber Güvenlik, Orion Kitabevi, Ankara.

Arıboğan, Ü.& Ayman, G.& Dedeoğlu, B. (2005). Uluslararası İlişkiler Sözlüğü, der. Faruk Sönmezoğlu, Der Yayınları, İstanbul.

Arı, T. (2011). Uluslararası İlişkiler Teorileri Çatışma, Hegemonya, İşbirliği, MKM Yayıncılık, Bursa.

Arısoy, Ö. (2009). İnternet Bağımlılığı ve Tedavisi, Psikiyatride Güncel Yaklaşımlar -Current Approaches In Psychiatry, 1:55-67.

Ayhan, B.& Köseliören, M. (2019). İnternet, Online Oyun ve Bağımlılık. Online Journal of Technology Addiction & Cyberbullying, 2019, 6(1), 1-30.

Bahtiyar, Z. (2003). Virüsler Ve Güvenlik, Pusula Yayıncılık, İstanbul.

Baysal, B. & Lüleci, Ç. (2015). Kopenhag Okulu ve Güvenlikleştirme Teorisi, Güvenlik Stratejileri Dergisi, 11 (22) , 61-96. Et: 22.05.2020 (https://www.academia.edu/17191181/Kopenhag_Okulu_ve_G%C3%BCvenlikle%C5%9Ftirme_Teorisi).

Bayer, H. & Aksoğan, M. & Çoban, T. & Çelik, E. (2017). Anlamsal Sosyal Mühendislik Çerçevesinde Saldırı Teknikleri ve Önlemler, 23-24 Eylül 2017, International Balkan and Near Eastern Social Sciences Congress Series, 361-367, Kırklareli. Et: 06.05.2020 (https://www.researchgate.net/publication/330278996_Anlamsal_Sosyal_Muhendislik_Cercevesinde_Saldiri_Teknikleri_ve_Onlemler).

Batu, M. & İplikçi, H. G. (2019). Yeni Medya Rahatsızlıkları: Yeni Nesil Medyaya Farklı Bir Bakış. Et: 24.11.2020 Erişim Adresi: (https://www.researchgate.net/publication/330441059_YENI_MEDYA_RAHATSIZLIKLARI_YENI_NESIL_MEDYAYA_FARKLI_BIR_BAKIS).

BBC News Türkçe.9 Nisan 2015. Fransız yayın kuruluşu TV5 Monde'a siber 'IŞİD saldırısı'. E.t: 16.11.2020 (www.bbc.com/turkce/haberler/2015/04/150409_fransa_siber_saldiri).

Bendiek, A. (2012). European Cyber Security Policy, Stiftung Wissenschaft und Politik German Institute for International anf Security Affairs, Berlin.

Benedek, W. (2006). İnsan Hakları Kavramı ve İnsan Haklarının Niteliği, İnsan Haklarını Anlamak içinde, İnsan Haklarını Anlamak İnsan Hakları Eğitimi El Kitabı, Avrupa İnsan Hakları ve Demokrasi İçin Eğitim ve Araştırma Merkezi (ETC), Graz.

Benedek, W.& Kettemann, M. (2013). İfade Özgürlüğü ve İnternet, Avrupa Konseyi, Türk Yargısının İfade Özgürlüğü Konusunda Kapasitesinin Güçlendirilmesi AB-AK Ortak Projesi, Baskı: Matbam Ajans, (https://rm.coe.int/16807005e4 e.t:12.02.2020).

Bendovschi, A. (2015). Cyber-Attacks- Trends, Patterns and Security Countermeasures, ScienceDirect Procedia Economics and Finance 28, 24-31. Et: 29.09.2020 (https://www.sciencedirect.com).

Bıçakcı, S. (2014). "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", Uluslararası İlişkiler Akademik Dergisi, Cilt 10, Sayı 40 s. 101-130. Et: 07.05.2020 (https://www.uidergisi.com.tr/wp-content/uploads/2015/04/Bicakci-NATOnun-Gelisen-Tehdit-Algisi.pdf)

Bilgi Teknolojileri ve İletişim Kurumu. (2017). USOM ve Kurumsal Siber Olaylara Müdahale Ekibi. E.t:18.03.2020 (https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi).

Bilgi Teknolojileri ve İletişim Kurumu. (2018). İnternet Bilgi İhbar Merkezi. E.t:18.03.2020 (https://www.ihbarweb.org.tr/).

Burlu, K. (2013). Bilişimin Karanlık Yüzü (4. Baskı), Nirvana Yayınları, Ankara.

Büyükçapar, O. (2018). Bilişim Teknolojileri ve Yazılım, Kodlab Yayın Dağıtım, İstanbul.

Cavelty, M.D. (2015). Cyber-Security, Comtemporary Security Studies, Thomson Digital, Zürih Et: 22.09.2020 (https://www.researchgate.net/publication/281631032).

Chilk, W. (2007). Harassment through the Digital Medium A Cross-Jurisdictional Comparative Analysis on the Law on Cyberstalking (ed: Sylvia Mercado Kierkegaard), Cyberlaw, Security & Privacy, 2. Baskı, Ankara Barosu Başkanlığı.

Cihangir, M. (2020). Sosyal Medya Devriminin Neo-Politik Boyutları: Panoramik Bir İnceleme, Akademik Araştırmalar ve Çalışmalar Dergisi 12 (22): 186-196.

Çakmak, H. & Altunok, T. (2009). Suç, Terör ve Savaş Üçgeninde Siber Dünya, Barış Platin Kitabevi, Ankara.

Çalışkan, M. (2019). Toplum ve Suç Araştırmalarında Sınırları Aşan Bir Suç: "Çevrimiçi Çocuk İstismarı" Ve Bu Suça Karşı Alınabilecek Önlemler, Dumlupınar Üniversitesi Sosyal Bilimler Dergisi, 61, 122-131 Et: 26.09.2020 (http://dergipark.gov.tr/dpusbe).

Çetin, B. (2018). "Geleceğin Teknolojileri ve Gazetecilik Mesleği Üzerine Etkileri: Büyük Veri, Veri Gazeteciliği, Yeni Yaklaşımlar" (Ed. Olcay Uçak), Dijital Medya ve Gazetecilik, ss.31-61, Eğitim Yayınevi, Konya.

Çifci, H. (2017). Her Yönüyle Siber Savaş (2. Basım), TÜBİTAK Popüler Bilim Yayınları, Ankara.

Çoban, B. &Ataman, B. (2016). Gözetim Toplumu [Panoptikon], TMMOB Elektrik Mühendisleri Odası İstanbul Şubesi, Ege Basım, İstanbul.

Darıcılı,A.B. (2018). "Askerileştirilen ve Silahlandırılan Siber Uzay", (Ed. Ali ACARAVCI), Sosyal ve Beşeri Bilimlere Dair Araştırma Örnekleri, ss.311-338, Nobel Yayınları, Ankara.

Darıcılı, A.B. (2019). Türkiye'nin Siber Güvenlik Politikalarının Analizi; Türkiye'nin Potansiyel Siber Güvenlik Stratejisi, TESAM Akademi Dergisi, 6 (2), 11-33. Et: 20.05.2020 (https://dergipark.org.tr/tr/pub/tesamakademi/issue/48432/613517).

Defending the networks, The NATO Policy on Cyber Defence 2011, Et: 22.09.2020 (https://www.nato.int).

Eren, M. (2017). Avrupa Birliği'nin Siber Güvenlik Politikası, (1. Baskı). Beta Basım Yayım Dağıtım, İstanbul.

Eren, V. & Aydın, A. (2014). Sosyal Medyanın Kamuoyu Oluşturmadaki Rolü ve Muhtemel Riskler, KMÜ Sosyal ve Ekonomik Araştırmalar Dergisi 16 (Özel Sayı I): 197-205. Et: 08.05.2020 (http://dergi.kmu.edu.tr/userfiles/file/Mayis20141/28m.pdf).

Efthymiopoulos, M.P. (2019). A cyber-security framework for development, defense and innovation at NATO, Journal of Innovation and Entrepreneurship, 8:12, Cyprus.

ERDEM, H. & Türen, U. & Kalkın, G. (2017), "Mobil Telefon Yoksunluğu Korkusu (Nomofobi) Yayılımı: Türkiye'den Üniversite Öğrencileri ve Kamu Çalışanları Örneklemi", Bilişim Teknolojileri Dergisi, Cilt: 10, Sayı: 1, s. 1-12.

Ergur, A. (2016). Finans Kapitalizminin İçselleştirilmiş Mantığı Olarak Gözeti, (der Çoban, B. &Ataman, B.), Gözetim Toplumu [Panoptikon], TMMOB Elektrik Mühendisleri Odası İstanbul Şubesi, Ege Basım, İstanbul.

FIRAT, M. (2015). Hukuk Devleti Açısından İnternette İnsan Hakkı ve Kişilik Haklarına Saldırı Sorunu. Hacettepe Hukuk Fakültesi Dergisi, 5 (2), 101-116. Retrieved from (https://dergipark.org.tr/tr/pub/hacettepehdf/issue/44831/557617).

Gilpin,R. (2011). Uluslararası İlişkilerin Ekonomi Politiği, Kripto Basım Yayım Dağıtım, Ankara.

Goyushov, S. (2019). Uluslararası İlişkilerde Güvenlik Çalışmalarına İlişkin Teorik Tartışmalar, Akademik Sosyal Araştırmalar Dergisi, Yıl: 7, Sayı: 88. Et: 22.05.2020 (http://www.asosjournal.com/DergiTamDetay.aspx?ID=14702).

Göçer, M. (2002). Uluslararası Hukuk ve İnsan Haklarının Uluslararası Korunması, Seçkin Yayıncılık, Ankara.

Gökçearslan, Ş. & Günbatar, M. S. (2012). Ortaöğrenim Öğrencilerinde İnternet Bağımlılığı, Eğitim Teknolojisi Kuram ve Uygulama Dergisi Cilt:2 Sayı:2, s:10-24.

Griffiths, M.&, Roach, S. C. &Solomon, M. S. (2011). Uluslararası İlişkilerde Temel Düşünürler ve Teoriler. Çev. CESRAN, Nobel Akademik Yayıncılık, Ankara.

Güntay, V. (2015). Uluslararası İlişkiler Bağlamında Güvenlik Algısı Ve Siber Güvenlik; Akdeniz, Karadeniz Ve Avrupa Bölgeleri Üzerine Bir Değerlendirme, The Journal of Academic Social Science Studies, Sayı: 37. Et: 07.05.2020 (http://www.jasstudies.com/DergiTamDetay.aspx?ID=2957).

Güven,M. (2004). İnternet'te Güvenlik ce Hacker Cracker Meselesi, Grafiker Yayıncılık, Ankara.

Hekim, H. & Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları, Uluslararası Güvenlik ve Terörizm Dergisi(UGT), 4(2).

Kapani, M. (2008). *Politika Bilimine Giriş*, Bilgi Yayınevi, Ankara

Kaplan, K. & Ertürk, E. (2012). Dijital Çağ ve Bireyin İdeolojik Aygıtları. The Turkish Online Journal of Design Art and Communication, 2 (4), 7-12. (https://dergipark.org.tr/tr/pub/tojdac/issue/13011/156770 e.t: 12.02.2020)

Karabulut, B. (2015). Güvenlik-"Küreselleşme Sürecinde Güvenliği Yeniden Düşünmek", Barış Kitabevi, Ankara.

Kilkelly, U. (2001). Özel hayata ve aile hayatına saygı gösterilmesi hakkı-Avrupa İnsan Hakları Sözleşmesi'nin 8. Maddesi'nin uygulanmasına ilişkin kılavuz, Avrupa Konseyi, İnsan Hakları Genel Müdürlüğü,Almanya,e.t:12.02.2020 (http://www.inhak.adalet.gov.tr/Resimler/Dokuman/10122019113948ozel_hayat.pdf).

Knutsen, T. L.(2006). Uluslararası İlişkiler Teorisi Tarihi, çev. Mehmet Özay, Açılım Kitap, İstanbul.

Korkmaz, A. (2014). İnsan Hakları Bağlamında Özel Hayatın Gizliliği ve Korunması, Karamanoğlu Mehmet Bey Üniversitesi Sosyal ve Ekonomik Araştırmalar Dergisi 16 (Özel Sayı I): 99-103.

Korkmaz, A. (2016). Siber Zorbalık: Fizikselden Sanala Yeni Şiddet, Anadolu Üniversitesi İletişim Bilimleri Fakültesi Uluslararası Hakemli Dergisi Cilt:24 Sayı:2, s:74-85.

Kuzu, A. (Eylül 2019). MIT-MOSSAD-CIA-GLADIO Dünyanın En Büyük İstihbarat Servisleri, Kariyer Yayıncılık, İstanbul.

Kuzu, A. (Ağustos 2019). Dünyanın En Acımasız Örgütü MOSSAD, Kariyer Yayıncılık, İstanbul.

Meharanjunisa, S. (2020). "Global Perspective:Cyberlaw, Regulations and Compliance", International Journal of Trend in Scientific and Development (IJTSRD), Volume 4 Issue 5. Et: 05.10.2020 (https://www.researchgate.net/publication/342898826).

Murse, T.(2019). How Social Media Has Changed Politics 10 Ways Twitter and Facebook Have Altered Campaign, Et: 23.09.2020 (https://www.thoughtco.com/how-social-media-has-changed-politics-3367534) .

Nandhini, S. & Seemma, P.S. & Sowmiya,M. (2018). Overview of Cyber Security, International Journal of Advanced Research in Computer and Communication Engineering, Vol:7 İssue: 11 Et: 18.09.2020 (https://www.researchgate.net/publication/329678338).

Ögel, K. (2012). İnternet bağımlılığı internetin psikolojisini anlamak ve bağımlılıkla başa çıkmak, (1. Baskı). Türkiye İş Bankası Kültür Yayınları, İstanbul.

Özmen, Ş. Y. (2018). Dijital Şiddet, Siber Zorbalık ve Yeni Medya Okuryazarlığı Üzerine Bir Değerlendirme, Uluslararası Sosyal Araştırmalar Dergisi, Cilt: 11, Sayı: 61, S: 958-966).

Peker, A. & Eroğlu, Y. (2015). Ergenlerde Algılanan Sosyal Destek ve Siber Zorbalığa Eğilim Arasındaki İlişkiler: Arkadaştan ve Öğretmenden Algılanan Sosyal Desteğin Aracı Rolü, Turkish Studies International Periodical For The Languages, Literature and History of Turkish or Turkic Volume 10/3, p. 759-778.

Polat, O. (2017). Şiddet. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi Cilt:22 Sayı:1 Erişim tarihi: 30.04.2020 (http://dergipark.gov.tr/maruhad/issue/27591/290653).

Polat, R. (2017). Dijital Hastalık Olarak Nomofobi, e-Journal of New Media / Yeni Medya Elektronik Dergi - eJNM May 2017 Volume 1 Issue 2, p: 164-172.

Sabah Gazetesi. 2019. "Siber saldırı NATO'nun 5. maddesini tetikleyebilir". E.t: 10.10.2020 (https://www.sabah.com.tr/dunya/2019/08/28/siber-saldiri-natonun-5-maddesini-tetikleyebilir).

Sayımer, İ. & Akça, E. B. (2017). Siber Zorbalık Kavramı, Türleri ve İlişkili Olduğu Faktörler: Mevcut Araştırmalar Üzerinden Bir Değerlendirme, Cilt/Vol: 8-Sayı/Num: 30, AJIT-e: Online Academic Journal of Information Technology.

Sargın, S. & Temurçin,K. (2011). Türkiye'nin Suç Coğrafyası. Polis Akademisi Yayınları, Ankara.

Sağıroğlu, Ş. (2018). Siber Güvenlik Ve Savunma: Önem, Tanımlar, Unsurlar Ve Önlemler, (der: Sağıroğlu, Ş. & Alkan, M.), Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık, Grafiker Yayınları, Ankara.

Şafak,E.(2020). "Uluslararası Hukukta Değişen Güvenlik Algısı ve Saldırı Suçu Bağlamında Siber Saldırılar", Selçuk Üniversitesi Hukuk Fakültesi Dergisi(SÜHFD), C. 28, S. 1, s. 127-160.

Tamer,N. & Vatanartıran, S. (2014). Ergenlerin Teknolojik Zorbalık Algıları. Online Journal Of Technology Addiction & Cyberbullying 1 (2) Erişim tarihi: 30.04.2020 (http://dergipark.gov.tr/ojtac/issue/28472/303449).

TASAM(Türk Asya Stratejik Araştırmalar Merkezi). (2004). Siber Terörizm Raporu, Et:05.05.2020 (https://tasam.org/Files/Icerik/File/siber_terorizm_raporu_84be5753-d219-418f-9a68-e6c719b645b1.pdf).

Taş, İ. & Eker, H. & Anlı, G. (2014). Orta Öğretim Öğrencilerinin İnternet ve Oyun Bağımlılık Düzeylerinin İncelenmesi, Online Journal Of Technology Addiction & Cyberbullying, 2014, 1(2), 37-57.

Thinktech STM Teknolojik Düşünme Merkezi Siber Tehdit Durum Raporu Ocak-Mart 2020. Et:05.05.2020(https://thinktech.stm.com.tr/uploads/raporlar/pdf/1042020115521806_stm_siber_tehdit_durum_raporu_ocak_mart_2020.pdf)

Türkiye Cumhuriyeti Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğü, (2018). Açılış yılına göre 2018 Yılında Karara Bağlanan Davalardaki Suç Sayıları, Et:28.04.2020 (http://www.adlisicil.adalet.gov.tr/Resimler/SayfaDokuman/2082019153842istatistik2018.pdf).

Türkiye Cumhuriyeti İç İşleri Bakanlığı Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı. Et:24.04.2020 (https://www.egm.gov.tr/siber/sibersucnedir).

Türkiye Cumhuriyeti İç İşleri Bakanlığı Kamu Düzeni ve Güvenliği Müsteşarlığı. (2017). Güvenlik Terimleri Sözlüğü. Kamu Düzeni ve Güvenliği Müsteşarlığı Yayınları, Ankara.

Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı Bilgi Teknolojileri ve İletişim Kurumu TÜİK Verileri, Et:28.04.2020 (http://www.tuik.gov.tr/UstMenu.do?metod=temelist).

Türkiye Bankalar Birliği, Bankacılıkta Dolandırıcılık Eylemleri Tespit Ve Önleme Yöntemleri. (2015). Et: 06.05.2020 (https://www.tbb.org.tr/gec/KTPV14.pdf).

'Türkiye'nin Siber Kalesi' Siber Saldırılara Karşı 7/24 Nöbette, Trthaber:16 Şubat 2020. E.t:19.03.2020 (https://www.trthaber.com/haber/bilim-teknoloji/turkiyenin-siber-kalesi-siber-saldirilara-karsi-724-nobette-461145.html).

Ulusal Siber Olaylara Müdahale Merkezi (USOM) Siber Güvenliğe İlişkin Temel Bilgiler. (2014). Et:05.05.2020 (https://www.usom.gov.tr/dosya/1418807122-USOM-SGFF-001-Siber%20Guvenlige%20Giris%20ve%20Temel%20Kavramlar.pdf).

Ulusal Siber Olaylara Müdahale Merkezi. E.t:18.03.2020 (https://www.usom.gov.tr/hakkimizda.html).

Ünal, A.Y. Türkiye'nin siber saldırıları önleme merkezi kapılarını AA'ya açtı, Anadolu Ajansı: 08.02.2020. E.t:19.03.2020 (https://www.aa.com.tr/tr/turkiye/turkiyenin-siber-saldirilari-onleme-merkezi-kapilarini-aaya-acti/1727981).

Yalçın, Ö. & Karaçetin, G. (2016). İnternet Bağımlılığı ve Diğer Teknolojik Bağımlılıklar, Çocuk ve Ergen Ruh Sağlığı ve Hastalıkları, Edition: Hardcover, Chapter: 34, Publisher: Türkiye Çocuk ve Genç Psikiyatrisi Derneği, Editors: Aynur Pekcanlar Akay, Eyüp Sabri Ercan, pp.471-527.

Yaman, E. & Eroğlu,Y. & Peker,A. (2011). Okul Zorbalığı ve Siber Zorbalık, Kaknüs Yayınları, İstanbul.

Yılmaz, D. (2005). HACKING Bilişim Korsanlığı ve Korunma Yöntemleri (3. Baskı), Hayat Yayıncılık, İstanbul.

Yüksel, M. (2003). Mahremiyet Hakkı ve Sosyo-Tarihsel Gelişimi. Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi, 58(1): 181-213.

Zedner, L. (2015). Güvenlik, çev. Defne Orhun, Optimist Yayın Grubu, İstanbul.

www.mevzuat.gov.tr, e.t:05.10.2020, (https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2709.pdf).

EKLER:

EK 1: ANKET FORMU

ANKET SORULARI:

1-Kaç yaşındasınız?

0-15 \ 16-25 \ 26-35 \ 36-45 \ 45- 55 \ 55 üstü

2-Eğitim durumunuz nedir?

Yüksek Lisans / Üniversite / Lise / İlkokul

3- Mesleğiniz?

Memur/ İşçi/ Serbest Meslek/ Öğrenci/ Diğer

4-Türkiye'de ki en büyük problem sizce nedir?

Eğitim /İş / Sağlık /Güvenlik / Yabancı Düşmanlığı

5-Türkiye'de gördüğünüz en olumlu şey nedir?

İklim ve Çevre / Kültür / Yaşam Standartları / Yönetim(hükümet)

6-İş yaşamınızda karşılaştığınız problemler nelerdir?

İş şartları / Çalışma saatleri / Düşük ücret /Güvenlik

7- Türkiye'nin güvenliğini nasıl buluyorsunuz?

İyi/ Orta/ Kötü

8- Türkiye'nin siber güvenliğini nasıl buluyorsunuz?

İyi/ Orta/ Kötü

9- Türkiye'de vatandaşların siber güvenlik farkındalığını nasıl buluyorsunuz?

İyi/ Orta/ Kötü

10- Daha önce bir siber suça veya siber zorbalığa maruz kaldınız mı?

Evet/Hayır

11- Daha önce bir siber zorbalık yaparak birini mağdur ettiniz mi?

Evet/Hayır

12- Bilgisayar veya Cep telefonu kullanırken aldığınız güvenlik önlemleri nelerdir?

Virüs programı var/ Bir önlem yok/ Diğerse önleminiz nedir:

13- Çocuklarınız var ise çocuklarınıza siber tehditlere karşı farkındalık eğitimi verdiğiniz oldu mu?

Evet/Hayır

14- Çocuklarınız var ise çocuklarınıza siber tehditlere karşı öğrenim gördüğü okulda yeterince farkındalık eğitimi verildiğini düşünüyor musunuz?

Evet/Hayır

15- Bilgi Teknolojileri ve İletişim Kurumunun sunmuş olduğu ihbar web ile ilgili bilgi sahibi misiniz?

Evet/Hayır

16- Bir siber suça maruz kalırsanız ne yapacağınızı biliyor musunuz?

Evet/Hayır

17- Başka birinin kullanmış olduğu telefon veya bilgisayar modeliyle dalga geçtiğiniz oldu mu?

Evet/Hayır

18- Çalıştığınız iş yerinde düzenli işleyen siber güvenlik çalışanı veya bilgi işlem uzmanı var mı?

Evet/Hayır

19- Bilgi Güvenliği ihlali olduğunda bu ihlali kime bildirirsiniz?

A-Kendim çözmeye çalışırım

B- Devletin kolluk birimine bildiririm

C-Çalıştığım firmanın IT elemanı veya Güvenlik birimine bildiririm

D-İhlalden uzak durarak kendimi korurum.

20- Hiç uzaktan erişim sağlayarak (AnyDesk Uzaktan PC erişim, VPN, Bulut sunucu vs.) kullanarak çalışma yaptığınız oldu?

A-olmadı

B-oldu

ARAŞTIRMA ALANLARI:

Uluslararası İlişkiler

Uluslararası İlişkiler Teorileri

Uluslararası Güvenlik

Güvenlik Stratejileri

Siber Güvenlik

Siber Politikalar

Uluslararası Hukuk ve Siber Suçlar

Siber Hukuk

Sosyal Medya Uzmanlığı

Yeni Medya Okuryazarlığı

Dış Politika

Enerji Güvenliği

Avrupa Birliği

Genel Ekonomi

İşletme