T.C.
GAZİANTEP ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
GÜVENLİK STRATEJİLERİ VE YÖNETİMİ ANA BİLİM DALI

TÜRK SİLAHLI KUVVETLERİ PERSONELİNİN BİLİŞİM SUÇLARINA YÖNELİK YAKLAŞIMI (Gaziantep İli Örneği)

YÜKSEK LİSANS TEZİ

ALİ DURDU

GAZİANTEP
OCAK 2015

T.C.
GAZİANTEP ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
GÜVENLİK STRATEJİLERİ VE YÖNETİMİ ANA BİLİM DALI

TÜRK SİLAHLI KUVVETLERİ PERSONELİNİN BİLİŞİM SUÇLARINA YÖNELİK YAKLAŞIMI (Gaziantep İli Örneği)

YÜKSEK LİSANS TEZİ

ALİ DURDU

Tez Danışmanı: Yrd. Doç. Dr. Ömer Faruk VURAL

GAZİANTEP
OCAK 2015

T.C.
GAZİANTEP ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
GÜVENLİK STRATEJİLERİ VE YÖNETİMİ ANA BİLİM DALI

Türk Silahlı Kuvvetleri Personelinin Bilişim Suçlarına Yönelik Yaklaşımı (Gaziantep İli Örneği)

ALİ DURDU

Tez Savunma Tarihi: 30.01.2015

Sosyal Bilimler Enstitüsü Onayı

Prof. Dr. Hilmi BAYRAKTAR
SBE Müdürü

Bu tezin Yüksek Lisans tezi olarak gerekli şartları sağladığını onaylarım.

Prof. Dr. Hilmi BAYRAKTAR
Enstitü ABD Başkanı

Bu tez tarafımca okunmuş, kapsamı ve niteliği açısından bir Yüksek Lisans tezi olarak kabul edilmiştir.

Yrd. Doç. Dr. Ömer Faruk VURAL
Tez Danışmanı

Bu tez tarafımızca okunmuş, kapsam ve niteliği açısından bir Yüksek Lisans tezi olarak kabul edilmiştir.

Jüri Üyeleri:

İmzası

Yrd. Doç. Dr. Ömer Faruk VURAL(Jüri Başkanı) _____

Doç. Dr. Servet DEMİR _____

Yrd. Doç. Dr. Mustafa METE _____

ÖZET

TÜRK SİLAHLI KUVVETLERİ PERSONELİNİN BİLİŞİM SUÇLARINA YÖNELİK YAKLAŞIMI

(Gaziantep İli Örneği)

DURDU, Ali
Yüksek Lisans Tezi, Güvenlik Stratejileri ve Yönetimi ABD
Tez Danışmanı: Yrd. Doç. Dr. Ömer Faruk VURAL
Ocak, 2015, 105 Sayfa

Bu tez çalışmasında, Türk Silahlı Kuvvetlerinde görevli personelin bilgi teknolojileri kavramları çerçevesinde görüşlerini öğrenebilmek, bilişim suçlarına yönelik algıları ve bilgi alt yapısını ölçmek amaçlanmaktadır. Bu çalışma, Gaziantep ilinde halen çalışmakta olan 1 Albay, 1 Yarbay, 3 Yüzbaşı, 1 Üsteğmen, 1 Asteğmen, 4 Başçavuş, 1 Kıdemli Üstçavuş, 3 Uzman Çavuş olmak üzere toplam 15 Türk Silahlı Kuvvetleri personeli üzerinde gerçekleştirilmiştir. Bilgi teknolojileri ve bilişim suçları kavramlarına yönelik görüşlerin elde edilmesi amacıyla, personellere, hazırlanan açık uçlu soruların yer aldığı görüşme formu uygulanmıştır. Katılımcıların vermiş oldukları cevaplar içerik analizi yöntemi doğrultusunda kategorilere ayrılmıştır. Analizler bu kategorilere dayalı olarak yapılmıştır. Analizler sonucunda Türk Silahlı Kuvvetleri personelinin; bilgi teknolojileri ve bilişim suçları konularında farkındalığının artırılması gerekliliği ve konuyla ilgili bilgi düzeyinin yeterli olmadığı ortaya çıkmıştır. Bilişim teknolojilerine yüksek miktarlarda para harcamadan önce karar verici mercilerin eğitim programlarını gözden geçirmeleri gereklidir.

Anahtar Kelimeler: Bilgisayar, İnternet, Bilişim Teknolojileri, Bilişim Suçları, Siber Savaş, Bilgi Güvenliği, Eğitim, Türk Silahlı Kuvvetleri

ABSTRACT

APPROACHES OF THE PERSONAL OF THE TURKISH ARMED FORCES TO THE CRIMES OF INFORMATICS
(A Case Study in Gaziantep)

DURDU, Ali
M.E. Thesis, Department Of Securıty Strategıes And Management
Supervisors: Asst. Prof. Dr. Ömer Faruk VURAL
January, 2015, 105 Pages

In this thesis it is intended to obtain opinions of the staff members of Turkish Armed Forces about information technology, the perceptions towards informatics crimes and to measure members' information backgrounds. This study has been applied to 1 Colonel, 1 Lieutenant Colonel, 3 Captains, 1 First Lieutenant, 1 Third Lieutenant, 4 Master Sergeants, 1 Senior Staff Sergeant and 3 Specialist Sergeants who are currently on duty in Gaziantep. An interview form containing open-ended questions has been applied to staff members in an attempt to obtain opinions towards information technology and informatics crimes. The responses of the participants have been categorized in accordance with the content analysis method. Analysis have been made based on these categories. In consequence of the analysis it has become evident that the awareness of Turkish Armed Forces staff members about the information technology and the informatics crimes ought to be enhanced and the information level concerning the subject is inadequate. Before spending high amount of money for informatics technologies, decision maker authorities ought to review the education programmes.

Key Words: Computer, Internet, Information Technology, Informatics Crimes, Cyber War, Information Security, Education, Turkish Armed Forces

İÇİNDEKİLER

Sayfa No

Sayfa No

Sayfa No

TABLOLAR

Sayfa No

ŞEKİLLER

Sayfa No

EKLER LİSTESİ

Sayfa No

KISALTMALAR

AKT. : Aktaran

ARPANET : Gelişmiş Araştırma Projeleri Ağı

BKZ. : Bakınız

BTK : Bilgi Teknolojileri ve İletişim Kurumu

ÇEV. : Çeviren

DDoS : Dağınık Servis Engelleme

ED. : Editör

GNU : GNU's Not Unix

MİT : Massachusetts Institute of Technology

PLA : Çin Halk Kurtuluş Ordusu

SOME : Siber Olaylara Müdahale Ekibi

TCK : Türk Ceza Kanunu

TCP/IP : Transfer Kontrol Protokolü/İnternet Protokolü

TDK : Türk Dil Kurumu

TİB : Telekomünikasyon İletişim Başkanlığı

TSE : Türk Standartları Enstitüsü

TSK : Türk Silahlı Kuvvetleri

TÜBİTAK : Türkiye Bilimsel ve Teknolojik Araştırmalar Kurumu

USOM : Ulusal Siber Olaylara Müdahale

WWW : Dünya Çapında Ağ

YTCK : Yeni Türk Ceza Kanunu

BİRİNCİ BÖLÜM
GİRİŞ

1.1. Giriş

Küreselleşen dünyada teknolojik gelişmeler sayesinde bütün dünyada mesafeler kalkmış, iletişim kolaylaşmıştır. Örülen internet ağları sayesinde farklı bir dünya oluşmuştur. Oluşan bu dünyada her alana erişim kolaylaşmış; ülkelerin kritik kurumlarına, özel şirketlerin kendi sistemlerine ve stratejik öneme sahip veri tabanlarına yetkisiz girişler görülmeye başlanmıştır. Bu tehditleri bertaraf etmek için siber savunma sistemlerine ihtiyaç duyulmuştur.

Her alanda olduğu gibi savunma alanında da teknoloji sayesinde gelişmeler elde edilmiştir. Hayatın vazgeçilmezi ve çağın gereği olan bilgisayar sistemlerinin savunma alanında yerini almasıyla cephe savaşlarının yerini maliyeti çok daha az olan siber savaşlar almaya başlamıştır. Özellikle son 10 yılda görülen gelişmeler ışığında 21. Yüzyıla siber savaşların damga vuracağı aşikârdır. Savaş kavramının değişmesine sebep olan siber savaşlar ülkelerin farklı önlemler almasında ve yeni stratejiler geliştirmesinde önemli rol oynamaktadır. Bu bağlamda alınan tedbirlerin temelini oluşturacak en önemli faktör personel unsurudur. Aktif, dinamik ve durumun farkında olan çağın ihtiyaçlarına göre hareket edip o yönde kendini geliştirerek teknolojiye ayak uyduran, planlayacağı faaliyetlerde bu hususları göz önünde bulunduran personele kurumların sürekli ihtiyacı olmuştur. Zira bu yönde hareket eden bir insan gücü kurumların geleceğe sağlam adımlarla ilerlemesinde en önemli faktördür. Bunun yanında teknolojik gelişmelerin bireyler ve kurumlar üzerinde faydalarının yanında zararlarının olduğu da aşikârdır. Bilgisayar sistemlerinin toplumun hemen hemen her kesiminde olması iyi niyetli insanların yanında kötü niyetli kişilerin çıkmasına da sebep olmuştur. Bu kötü niyetli kişiler kendilerinin yazdığı korsan program ve yazılımlarla farklı yöntemlerden yararlanıp hedef kitlenin bilgisayar veya işletim sistemli cep telefonlarına ulaşıp bir nevi

kontrolü eline alarak bireye, sisteme, kuruma zarar vermektekiler. Bu açıdan bakıldığı zaman ülkemizin güvenliğinde önemli bir yere sahip Türk Silahlı Kuvvetleri personelinin bilişim suçlarına olan yaklaşımı ve bilgi düzeyi önem arz etmektedir. Sahip olduğu bilgi düzeyi kimi zaman büyük bir stratejik üstünlük olarak ülkemize faydalı olabilir. Bu bilginin olmaması da tam tersi olarak büyük problemler, sonuçlar doğurabilir. Bu açıdan bakıldığı zaman Türk Silahlı Kuvvetleri personeli ve bu personelin kullandığı sistemi iyi bilmesi ve onu dışarıdan gelebilecek her türlü savunmaya karşı da koruması gerektir. Çünkü kullandığı sistemi dışarıdan müdahaleye karşı savunmasız bırakması demek ülke güvenliğini tehlikeye sokması demektir.

Türk Silahlı Kuvvetlerinde görev alan personelin bilişim suçlarına yönelik yaklaşımını ve bilgi düzeyini inceleyen bu çalışma dört bölümden oluşmaktadır. Birinci bölüm giriş bölümüdür. İkinci bölümde tezin kuramsal temelleri anlatılmakta ve konuyla ilgili yapılan araştırmaların verileri ışığında bilişim sistemleri dünyasına ait kavramlar ele alınacaktır. Ayrıca bu kavramlarla birlikte nasıl ve ne şekilde kullanıldığı, kullanan kullanıcıların sınıflandırılması, ne amaçla kullandıkları ve suç işleyen dünyaca ünlü kişiler açıklanacaktır. Dünyada ve Türkiye'de siber alanla alakalı devletlerin aldıkları önlemler, tedbirler, yaptıkları çalışmalar ve kısaca tarihsel gelişimleri açıklanacaktır. Bunun yanı sıra dünyada ve Türkiye'de yaşanmış siber saldırı ve savaşlar ele alınacaktır. Ayrıca dünyada ve Türkiye'de yapılan ortak tatbikatlara yer verilecektir. Üçüncü bölüm altı alt başlıktan oluşmaktadır. Bu alt başlıklar sırasıyla; *araştırmanın yöntemi, araştırmanın deseni, çalışma grubu*, *veri toplama araçları ve teknikleri, veri toplama aracının geçerlik ve güvenirliğinin sağlanması* ve son olarak *verilerin toplanması ve çözümü* şeklinde ele alınmıştır. Dördüncü bölümde; yapılan araştırmayla ilgili bulgular detaylı şekilde ortaya konulacaktır. Dördüncü bölümün sonunda genel bir değerlendirme yapılarak öneriler özetlenecek ve tez çalışması esnasında araştırılması önem arz eden konular belirtilecektir.

1.2. Araştırma Soruları

Araştırmanın amacı doğrultusunda şu sorulara yanıt aranmıştır:

1. Türk Silahlı Kuvvetleri personelinin bilgi teknolojileri ile ilgili bilgi düzeyleri nedir?

2. Türk Silahlı Kuvvetleri personelinin bilişim suçlarına karşı yaklaşımı nedir?

1.3. Araştırmanın Amacı

Bu çalışmada, ülkemizin her türlü iç ve dış savunmasından sorumlu Türk Silahlı Kuvvetlerinde görevli personelin bilgi teknolojileri kavramları çerçevesinde görüşlerini öğrenebilmek, bilişim suçlarına yönelik algıları ve bilgi alt yapısını ölçmek amaçlanmaktadır. Türk Silahlı Kuvvetleri personelinin; bilgi teknolojileri ve bilişim suçları konularında farkındalığını artırmak ve aşina olmalarını sağlamak; bilişim teknolojilerine yüksek miktarlarda paraların harcanmasından ziyade, işin temelini oluşturan görevli personelin bilgi düzeyini ortaya koyup karar verici mercilere eğitim planlamasında yol göstermek hedeflenmektedir.

1.4. Araştırmanın Önemi

Ülkemizin silahlı kuvvetleri, silahlı saldırı karşısında savunmaya ve saldırıya ne kadar hazırsa siber saldırılar karşısında da o kadar hazırlıklı olmalıdır. Gelişen ülkeler her alanda olduğu gibi siber alanda da ordular kurmakta ve siber saldırı manasında yeni siber savunma ya da siber saldırı araçları geliştirmektedir. Ülkemizde yapılan araştırmalara göre Türkiye'nin siber saldırılara açık olduğu ve konunun, kamu kuruluşları tarafından yeterince ciddiye alınmadığı ortaya çıkmıştır (Bıçakçı, 2013). Siber güvenlik alanında donanımın ve yazılımın önemi vurgulanırken bütün bu altyapıyı kullanacak olan personel göz ardı edilmektedir. Tehditlerin ve saldırıların niteliğini derinlemesine anlayan personel ihtiyacı ve mevcut personelin konuya olan yaklaşımı önem arz etmektedir. Zira devir artık top tüfek devri olmaktan çoktan çıkmış durumdadır. Türk ordusu da siber savunma adına gereken hazırlıkları yapıp asrın silahları ile silahlanmasını bilmelidir. Bu manada siber ordular kurup atağa karşı atakla cevap vermeli ve personelin bu konu hakkında eğitilmesini sağlamalıdır. Bu açıdan bakılınca araştırmanın önemi ortaya çıkmaktadır.

1.5. Araştırmanın Varsayımları

Araştırmada, Türk Silahlı Kuvvetleri Personelinin görüşme sorularına tarafsız ve doğru biçimde cevap verdikleri varsayılmıştır.

1.6. Araştırmanın Sınırlılıkları

Araştırma;

Gaziantep ilinde halen çalışmakta olan 1 albay, 1 yarbay, 3 yüzbaşı, 1 üsteğmen, 1 hukukçu asteğmen, 4 başçavuş, 1 kıdemli üstçavuş, 1 kıdemli uzman çavuş, 2 uzman çavuş olmak üzere toplam 15 Türk Silahlı Kuvvetleri personelinden oluşmaktadır. Bu çalışma grubuna ulaşıldığı için araştırma bu çalışma grubu üzerinde yapılmıştır. Gerçekleştirildiği dönem açısından, 2014-2015 eğitim yılının ilk yarısında gerçekleştirilmiştir.

İKİNCİ BÖLÜM
KAYNAK TARAMASI

2.1. Siber Alan İle İlgili Kavramlar

Günümüz bilişim ve teknolojisi baş döndürücü bir hızda gelişmektedir. Bu bağlamda her geçen gün terminolojiye yeni yeni kavramlar girmektedir. Bu çalışmada karşımıza çıkacak olan bu kavramlar, konunun daha iyi kavranıp anlaşılabilmesi için tek tek ele alınıp açıklanacaktır.

2.2. Bilişim Sistemleri

Bu alanda ilk olarak bu alanın temelini oluşturan bilişim sistemleri gelmektedir. Bilişim Sistemleri bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmetin, işlemin ve verinin sunumunda yer alan sistemleri ifade eder. Hayatımızda önemli bir yere sahip olan bilgisayarlar bilgi çağının, iletişim çağının en önemli parçası durumundadır.

İnternetin atası olarak kabul edilen ve ilk defa askeri amaçla kullanılan ABD Savunma Bakanlığı'nın ARPANET (Advanced Research Projects Agency Network) projesi ilk defa 1969 yılında kullanılmıştır ve bu proje günümüzde kullanılan internetin ilk şekillerinden olmuştur (Timisi, 2003). Günümüzde bilgisayar ve internet birbirini büyük bir uyum içerisinde tamamlamaktadır.

1983 yılında TCP/IP (Transmission Control Protocol / Internet Protocol) protokolünün kabul edilmesi ile Türkiye olarak bilişim dünyasına açılımımız da bu süreçten itibaren oluşturulmaya başlamıştır.

Ülkemizde yeni olan bilişim ile alakalı politikalarının oluşturulması, uygulanması, sürekliliğinin sağlanması ve değerlendirilmesi için ilk adım, 4 Ekim 1983 tarihinde Bilim ve Teknoloji Yüksek Kurulu'nun oluşturulmasıdır bu kurul da

77 sayılı Kanun Hükmünde Kararname'nin 18181 sayılı Resmi Gazete 'de yayımlanması ile oluşmuştur. Yüksek Kurul'un oluşumunu düzenleyen 3'üncü madde ile kararların uygulanmasına ilişkin 5'inci madde, 18 Kasım 1989 tarih ve 20336 sayılı Resmi Gazete' de yayımlanan 391 sayılı Kanun Hükmünde Kararname ile değiştirilmiştir (Akdağ, 2009:139). 1992 yılında ise www (World Wide Web - dünya çapında ağ) servisinin oluşturulmuş ve internet bugünkü şeklini almaya başlamıştır. Türkiye'nin, internete 12 Nisan 1993 tarihinden itibaren bağlı olduğu ve ilk bağlantının Ortadoğu Teknik Üniversitesi (ODTÜ) tarafından yapıldığı da bilinmektedir (Özkışlalı, 2008).

Her geçen gün kullanım oranı artan ve insanları bağımlı hale getiren internet ve bilgisayar gibi tüm teknolojik gelişmelerin çağımıza sağladığı faydaların yanında uygun şekilde kullanılmayan ve yasalar ile de denetlenmeyen teknolojinin kullanımı hem bireyde hem de ülkede büyük sorunlara yol açabilir. Çünkü bu teknoloji kullanıcılara sayısız nimetler sunmaktadır ve bunlara erişmek isteyenler bilerek veya farkında olmadan risklere girebilmektedir. Getirdiği sayısız kolaylığın yanında kötü niyetli kişiler tarafından da kullanıldığında bu teknoloji insanlığı tehdit eden büyük bir silaha da dönüşebilir (Özkışlalı, 2008). Bu durum ise uzun vadede toplumsal felaketlere yol açabilir. Dolayısıyla gerçek hayatta karşılaştığımız birçok suç artık internet ortamında da kendine yer bulmuştur hatta daha da büyük boyutlara ulaşmıştır. Devletler de bu suçlarla bireyin, ülkenin ve toplumun devamlılığı için mücadele etmek zorundadır (Özkan, 2006).

2.3. Siber Alan

Siber alan her ne kadar da uluslararası boyutta kabul edilen bir kavram olsa da bilişim teknolojisinin iskeletini oluşturan bu kavram farklı kişi ve kurumlarca çeşitli şekillerde yorumlanmıştır. ABD'nin Savunma Bakanlığı'nca yayınlanan terimler sözlüğünde siber alan; "işlemci ve kontrolörlerin bulunduğu internet, telekomünikasyon ağları ve bilgisayar sistemlerini de içine alan, birbirine bağlı bilgi teknolojileri altyapılarının olduğu küresel bir alan" olarak tanımlanmaktadır (United States of America Department of Defense, 2010:93). Burada bahsedilen alan fiziki ve somut bir alanı temsil etmemektedir. Günümüzde kullandığımız ve w*orld wide web* (www.) olarak ifade ettiğimiz alanı temsil etmektedir. Amerikan Kongre Araştırma Merkezi tarafından yapılan siber alan tanımına göre; "insanların bilgisayarlar ve

telekomünikasyon sistemleri aracılığıyla herhangi bir coğrafi sınırlamaya maruz kalmadan tamamen birbirine bağlı olma durumudur**”** (Hildreth,2001:1).

2.4. Siber Savunma

Diğer kavram ise siber savunma kavramıdır. Bu kavramı da şu şekilde ifade edilmektedir;

Siber Savunma, kurum, kuruluş ve kullanıcıların bilgi varlıklarını korumak amacıyla kullanılan yöntemler, politikalar, kavramlar, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulama deneyimleri ve kullanılan teknolojilerin bütünü olarak tanımlanıyor (ITU-T, 2008:6)**.** Her türlü engelleri aşabilme özelliğe sahip olan siber ve bilişim teknolojileri tabanında çözümler bulmak zorunludur. Siber savunmada etkinliğin arttırılabilmesi için alınabilecek önlemler şu şekilde sıralanabilir:

2.4.1. Bireysel Düzeyde

Kişilerin olası bilişim suçları konusunda eğitilmeleri bireysel düzeyde alınabilecek tedbirlerin başında gelmektedir. Bu kapsamda değerlendirildiğinde çocukların okulda bilgisayar derslerinin yanında ek olarak verilebilecek önleyici tedbirler de önem arz etmektedir (Aydın vd., 2006).

Casus yazılım, virüs, trojan vs. gibi zararlı yazılımlar basit şekilde karşı konulabilir. Bunun da işletim sisteminin ve anti virüs yazılımının güncel tutmakla mümkün olduğu belirtilmektedir. Teknolojinin ilerlemesiyle artık virüsler de anti virüs programlarını kolayca geçebilmektedirler. Bu nedenle her zaman güncelleme özelliği otomatik olarak ayarlanmalı ve virüs programı asla kapatılmamalıdır. Ayrıca bilgisayarda yer alan güvenlik duvarını da sürekli aktif kullanmamız gerekmektedir. Unutulmamalıdır ki internette aktif olarak dolaşan bir milyondan fazla zararlı yazılım var ve bu nedenle bu basit önlemleri ihmal etmemeliyiz (Köksal ve İlbaş, 2013).

2.4.2. Kurumsal Düzeyde:

Kurumsal alanda da güvenlik sağlamanın birinci yolu bireysel düzeyde eğitimden geçmektedir. Kurum ve kuruluşlara yönelik suçların çoğunun onların mal varlıklarına yöneliktir. Bu durumda yüksek bütçelerle oluşturulan kurum ve kuruluşların öncelikle siber tehditlere karşı koyacak bir politikasının da mutlaka

olması gerekmektedir. Bunun için hem kurum içi hem de kurum dışı destek alınabilir. Sisteme kurumdan da kurum dışından da saldırı söz konusu olabilir o nedenle sistem güvenliği konusunda ciddi tedbirlerin alınması gerekmektedir. Öncelikle çalışanların güvenliği için kurallar belirlenmeli ve teknik ve sistematik bir güvenlik için devletle birlikte uluslararası platformlarda belirlenen temel ölçütlere sadık kalmak şartıyla ve onlarla birlikte çalışılmalıdır. Firmalar arası da bilgi paylaşımı güvenli bir bilgi ve iletişim için çok gereklidir (Aydın vd., 2006).

2.4.3. Ulusal Düzeyde:

Siber güvenliğin en önemli noktasını devlet kurumları oluşturmaktadır. Çünkü devlet tarafından hem güvenli bir ağ alt yapısı oluşturulmalı hem de bunun hukuki bir zemini sağlanmalıdır. Bu tarz suçlar konusunda bazı devletlerin olaylara ilgisiz kalmasının altında yatan temel etken de alt yapının yetersiz olması ve hukuki zeminin eksikliğidir. Devletin siber suçlar konusunda gerekli cezaları oluşturması da ve işlenebilecek her türlü suça karşı caydırıcı bir cezanın da olması gerekmektedir. Sadece siber alanda görev alan yetkili birimler oluşturularak personelinin de yetiştirilmesi gerekmektedir. Çıkan yasalar çerçevesinde siber suçlarla ilgilenen hâkim, savcı ve diğer kolluk görevlileri de birlikte hareket ederek hem suçların belgelendirilmesi hem de yakalanıp gerekli cezanın verilmesi açısından önemli bir adım olacaktır.

Kurumların kendi sistemleri içerisinde kullanmış oldukları sisteme "intranet" adı verilmektedir. Burada erişim sadece yerel olarak yapılmaktadır. Bu sistemin sadece yerel ağ şeklinde çalıştığı ve dışarı ile bağlantısının olmamasından dolayı sistem dışarıdan gelebilecek tehditlere karşı da kapalıdır. Fakat tehdidin sistemin içerisinden gelme ihtimali vardır o sebeple de yine risk taşımaktadır. Riski azaltmak için de intranet ağı daha küçük birimler ve parçacıklar halinde muhafaza edilmelidir (Aydın vd., 2006).

2.4.4. Uluslararası Düzeyde:

Birçok ülkenin Ulusal Siber Olaylara Müdahale (USOM) timi vardır. Siber saldırı ve bu saldırılara karşı güvenlik için ülkelerin birbirleriyle iş birliği içerisinde olması gerekmektedir. Bu amaçla Interpol seviyesinde özel bir birim oluşturularak iletişim daha hızlı hale getirilebilir. Siber suçlarla mücadelede hukuki olarak da

devletlerin hayati öneme sahip bu alanda işbirliği içerisinde olması gerekmektedir. Bu anlamda ülke ağı içerisinde oluşturulan log dosyaları, e-postalar ve her türlü elektronik delillerin iyi muhafaza edilmesi de gerekmektedir. Talep eden ülkelere işbirliği ve bilgi paylaşımı çerçevesinde teslim edilmelidir. Siber suç ve suçlulardan bahsedildiği bu teknolojik uzayda geç kalınıp teslim edilemeyen bilgilerin de yine aynı suçlularca değiştirilmesi, tahrip edilmesi veya silinmesi de muhtemeldir (Aydın vd., 2006).

2.5. Siber Terörizm

Siber terör kavramı, terör ve siber kavramlarının günümüz teknolojilerine göre bilişim suçuna yönelik oluşturulmuş bir ifadedir. Terör kelimesinin sözlük anlamı, *"korkutma, yıldırma",* terörizm ise *"yıldırıcılık"* anlamına gelmektedir (TDK, 2014).

Terörizm, her ortamda ülkeleri tehdit eden ve oluşmuş olan güvenlik ortamını tehlikeye sokan bir olgu olarak çok çeşitli makalelerde ve tezlerde, değişik şekillerde ele alınmıştır (Asan, 2007; Aydın D. , 2006; Kedikli, 2006; Yılmaz E. S., 2013). Bir ülke için ifade edilen terörizm diğer bir ülke yararına olabilir o nedenle uluslararası alanda da hala bu konuda ortak bir anlayışa gidilememiştir. Bu durumu da Yayla (2013) *"yabancı işgaline karşı"* ve *"kendi kaderini tayin amaçlı meşru mücadele"* ile terörizm arasındaki ayrımın ortak bir kararla yapılamamasından kaynaklandığını ifade ediyor. Buna iten sebeplerin başında ise her ülkenin terörizm olgusuna farklı yaklaşımı olduğunu belirtiyor.

Hala net olarak ifade edebileceğimiz bir siber terör tanımı olmamasına rağmen bu terimi ilk kez Barry Collin 1980'lerde kullanmıştır (Akdağ, 2009). Krasavin (2012) ise siber terörizmi, "terörist faaliyetlerin siber alan kullanılarak gerçekleştirilmesi olarak ya da terör örgütlerinin siber alanı araç olarak kullanmaları" olarak tanımlar**.**

Siber terörizmle alakalı hem siber hem de terörizmi içeren tanımlar yer almaktadır.

Denning (2001)'e göre siber terörizm "Politik veya sosyal hedeflerin gerçekleştirilmesi için bir devleti veya vatandaşlarını aşağılamak veya korkutmak üzere bilgisayarlara, ağlara veya bilgilerin depolandığı yerlere gerçekleştirilen kanunsuz saldırı veya saldırı tehditlerdir"**.**

Özkan (2006:81) ise siber terörizmi, "belirli bir politik ve sosyal hedefe ulaşabilmek için; bilgisayar veya bilgisayar sistemlerinin, bireylere ve mallara karşı bir hükümeti veya toplumu yıldırma, baskı altında tutma amacıyla kullanılması" olarak tanımlamaktadır.

Stanford Üniversitesi, Uluslararası Güvenlik ve işbirliği Merkezi (CISAC) siber suçlarla alakalı çalışma yapmıştır ve bu çalışmada siber terörizm kavramını tanımlamaya çalışmıştır. Bu oluşan taslak da Stanford Taslağı olarak bilinmekte olup tanımlanan siber terörizm de şu şekilde olmuştur.

"Hukuken yetkili kılınmış görevlilerinin eylemleri dışında, siber sistemlere karşı girişilen ve kişi veya kişilerin ölümü ya da yaralanması, kamu düzeninin bozulması veya önemli ekonomik zararlara veya mallara karşı önemli zararlara neden olması muhtemel olan şiddet, bozma ve engelleme eylemlerinin kasıtlı şekilde yapılması veya yapılacağı tehdididir**"** (Özcan, 2002:309)**.**

Siber terörizmin neden bu kadar farklı yorumlandığını Akdağ (2009) şöyle ifade etmektedir;

Çevrenizdekilere siber terörün ne olduğunu sorsanız %90 ihtimalle çok farklı cevaplar alırsınız. Soru sorduğumuz kişiler eğer bilgisayar konusunda uzman kişiler ise, onlar da bu durumu çok basit bir şekilde ele alacaklardır. Fakat bu soru devlet kademelerinde, devlet güvenliğinden sorumlu personele sorulursa alacağınız cevabın çok ciddi olacağını fark edeceksiniz. Bu durum bizlerin hala siber terör, siber terörizm gibi konularda daha ciddi ve bilimsel yaklaşımımızın olmadığını gösteriyor. Bu farklı algılamalar da bize gösteriyor ki bizim daha bilimsel yaklaşımlara ihtiyacımız vardır ve bu konuda daha ciddi hazırlanmamız gerekmektedir.

2.6. Siber Suç

Teknolojiyi üreten toplumların teknolojiye de isim verdikleri bilinen bir gerçektir. Bu nedenle teknolojik alanlarda, teknoloji ile alakalı birçok kavramda da olduğu gibi siber suç, siber güvenlik, siber alan ile ilişkili dilimizde de yaygın olarak kullanılan ifade yoktur ayrıca bunların da henüz tam olarak ne ifade ettikleri bilinmemektedir. Siber suç kavramı siber ve suç kavramının birleşiminden oluşturulmuş yeni bir kavramdır. Siber, İngilizcede yer alan "cyber" kelimesinden gelmektedir. Bu kelime bilgisayar veya bilgisayar ağlarını ilgilendiren kavram veya

varlıkları tanımlamak için kullanılan bir ifadedir. Siber alan kelimesi ise İngilizcede "cyber space" kelimesinin dilimize çevrilmesinden gelmektedir. Bu kavram da bilgisayarla alakalı, birbiriyle bağlantılı somut ve soyut parçaların ve insanların etkileşimde bulunduğu alanı tarif etmede kullanılan bir kavramdır. (Klimburg, 2012)

Siber suç ifadesi bilişim sistemleriyle alakalı çalışmalarda farklı şekillerde de ifade edilmektedir. Mesela "bilgisayar suçu", "sanal suç", "elektronik suç," "dijital suç" veya "ileri teknoloji suçları" gibi ifadelere de rastlanabilir. İfadede farklılık olsa da asıl anlatılmak istenen yine aynı suç tanımıdır. Bu da bilişim sistemine yönelik veya bilişim sistemleri ile yapılan, işlenen suçlardır (Hekim ve Başıbüyük, 2013).

2.7. Siber Silahlar

Siber silah konusunda farklı tanımlamalar yapılmaktadır. Bakır (2013) siber silah kavramını siber ataklar sırasında karşı tarafı etkisiz bırakmak, zarar vermek ve veri çalmak için kullanılan siber ortam araçlar olarak tanımlamaktadır.

Silah ve siber silah kelimeleri her ne kadar birbirine benzese de birbirinden çok farklı kavramlardır. Silah yok etmeyi amaçlarken siber silah ise kimi zaman yok etme, kimi zaman iz silme, kimi zaman bilgi kaçırma, kimi zaman da bilgiyi değiştirme amacıyla kullanılabilir. Stuxnet, bu güne kadar bilinen en gelişmiş, en güncel siber silaha bir örnektir. Stuxnet, Amerika'nın yardımıyla İsrail tarafından gerçekleştirildiği iddia edilen bir silahtır ve amacı İran'ın Natanz kentindeki nükleer zenginleştirme programını yavaşlatmak ve çökertmektir (Farwell ve Rohozinski, 2011).

Gerçek savaşlarda kullanılan güdümlü füzeler 3 temel unsurun birleşiminden oluşmaktadır. Bunlar, İletim aracı (roket motoru), navigasyon sistemi ve patlayıcı yüktür. Siber silah için de bu bahsedilen 3 temel unsur uygundur. Her türlü siteler ve dosya paylaşım ve iletim araçları siber silahın hedefe ulaşmasını sağlayabilir. Ulaşılmak istenen hedefin sistem açıkları ve zayıf kısımları navigasyon olarak ifade edilebilir. Son olarak da sistemde açığı bulunan ve zayıf kısımlarından girilerek sisteme zarar verebilecek gerçek silah gibi patlayıcı olarak ifade edilebilen sistem gelmektedir buna da patlayıcı yük denilebilir (Bakır, 2013).

Siber Silahlar

1- Virüsler

1- Tarayıcıların ana sayfalarını değiştiren virüs,
2- İstenmeyen sitelere bağlanan virüs,
3- İşletim sistemini yavaşlatan, çökerten virüs

2- Solucanlar

1- USB sürücülere ve fiziksel hard disk sürücülerine kendini kopyalayarak bulaşan solucan,
2- Kendini rar arşivine koyarak karşı tarafa yollayan solucan.

3- Trojan

1- Bilgisayarın kamerası üzerinden gizlice görüntü kaydı yapma,
2- Mikrofon aracılığı ile ortamı dinleme,
3- Bilgisayarın ekran görüntülerini kaydederek takip etme
4- Klavye girişlerini kayıt altına alma,
5- Fare hareketlerini ve tıklamalarını kaydederek ekran klavyesine karşı şifreleri çalma.

4- Zombi ve Botnetler

1- Http Flood attack yapan botnet uygulaması,
2- IP Spoofing ile TCP/IP paketler gönderen zombi uygulaması.

5- Yemleme saldırıları

1- Sahte site ile yapılan yemleme saldırısı,
2- Sahte e-posta yollayarak yemleme saldırısı,
3- Http**s** kullanmadan yapılan yemleme saldırısı.

6- Spam

Spam e-posta atan uygulama

7- Spyware

1- Facebook, twitter kişi listesine yazı yazan casus yazılım
2- Bilgisayara kayıtlı şifreleri çalan casus uygulama

8- Keylogger

Klavye ile girilen tüm kayıtları tutan uygulama

9- Sniffer

MSN Messenger üzerindeki konuşmaları koklayan uygulama (Küçük ve Soğukpınar, 2013).

10- DDos

Koordineli olarak gerçekleşen, Botnet'lerin veya gönüllülük esasıyla oluşturulan ağdaki binlerce sistemin, kurban olarak belirlenen hedefe aynı anda saldırılmasına dağıtık servis dışı bırakma atağı denir.

"Bu gibi siber silahlar, siber ortamda şebekelere yetkisiz erişmekte, bu şebekeleri çalışamaz hale getirmekte ve bunların hizmet sunumunu engellemekte; siber ortamdaki bilgilere yetkisiz erişmekte, bu bilgileri değiştirmekte, yok etmekte, çalmakta ve ifşa etmektedir" (Ünver vd., 2009).

2.8. Siber Savaş

Siber, İngilizcede yer alan "cyber" kelimesinden gelmektedir. Bu kelime bilgisayar veya bilgisayar ağlarını ilgilendiren kavram veya varlıkları tanımlamak için kullanılan bir ifadedir. Savaş kelimesi de İngilizcede "war" kelimesinden gelmektedir. Siber savaş (Cyber war) kelimesinin birleşmesinden oluşan bir ifadedir (Yayla, 2013).

Siber savunma, siber alan, siber terörizm gibi kavramların henüz kabul edilen ortak bir tanımı olmadığı gibi siber savaş kavramının da ortak bir tanımı bulunmamaktadır. Farklı tanımları mevcuttur. ABD Savunma Bakanlığı (2010) siber operasyonları, "saldırıyı düzenleyenlerin temel amaçlarına ulaşmak için sahip oldukları siber kapasitenin siber alanda kullanılması" olarak tanımlamıştır. Buna ek olarak da Hildreth (2001) siber savaşı, "bilgi teknolojilerini korumak için siber alanda savunma yapmak veya saldırmak ya da rakip saldırıları engellemek için yapılan faaliyetlerin tümü" olarak ifade etmektedir (Gürkaynak ve Eren, 2011:268).

Gürkaynak ve Eren (2011) siber terör ve savaş arasındaki farkı şöyle belirtmektedir. Siber terör ve siber savaş her ne kadar kavram olarak birbirine benzese de birbirinden farklıdır. Siber savaş ülkeler arası meydana gelen fiziki savaşa eşlik edebilir veya fiziki savaş olmadan rakip ülkelerin birbirlerine siber alanda saldırmaları olarak da ifade edilebilir. Siber terörizm ise fiziki şartlarda

meydana gelebilecek terör eylemlerinin bilişim veya siber araçlar kullanılarak yapılması olarak ifade edilmektedir (Krasavin, 2012).

Siber savaş kavramı teknolojinin ilerlemesiyle birlikte daha da fazla kendinden söz ettirmeye başlayacaktır şeklinde güvenlik uzmanlarının düşünceleri vardır. Özellikle teknolojiye bağlılık, ekonomik alt yapılara yönelik dostça olmayan girişimlerin de bunun bir göstergesi olacağı belirtilmektedir. Devletler de bu tarz oluşabilecek tehditlere, ülkelerine yönelik gelebilecek saldırılara cevap vermede güvenlik sistemi uzmanlarına ve politikacılarına bu konuların takibini yaptırmaktadır. Büyük devletler, özellikle Amerika siber savaş olarak adlandırdıkları bu içinde bulundukları, gelişmeleri ülkenin ulusal politikası olarak görmektedir. Ülkelere fikir vermesi açısından değerlendirildiğinde geçtiğimiz yıllarda yaşanan Rusya ve Gürcistan kısa süreli savaşı siber savaşa bir örnektir ve gelecek yılarda da bu tarz savaşların olması kuvvetle muhtemeldir (Akdağ, 2009).

Siber Savaş Örnekleri

1. 1982 – Farewell Dosyası
2. 1990 – Körfez Savaşı
3. 1998 – Ay Işığı Labirenti
4. 1999 – NATO Kosova Krizi
5. 2007 – Suriye İsrail Gerginliği
6. 2007 – Estonya Siber Savaşı
7. 2008 – Gürcistan Siber Savaşı
8. 2008 – İsrail'in Gazze İşgali
9. 2009 – Kırgızistan Olayları
10. 2009 – Mavi Marmara Saldırısı (Bircan, 2012)
11. 2012 – Çin - Filipinler (Turla, 2012)
12. 2014 – Rusya – Ukrayna (Jones, 2014)

Siber savaşta olabilecekler

1. Nükleer tesislerde, petrol ve doğalgaz hatlarında sorun çıkıp patlamalara sebep olabilir.

2. Hava kontrol sisteminin kaybedilmesi sonucu uçaklar havada çarpışabilir. Uydu sistemlerinin ele geçirilmesi uyduların düşmesine ya da yörüngeden çıkmasına sebep olur.
3. Elektronik bankacılık durursa bankalardan ve ATM'lerden para çekilemez.
4. Metro, tren hatları ve trafik ışıklarının arızalanması büyük kazalara yol açabilir.
5. Elektrik dağıtım şebekesine yapılan olası bir saldırı durumunda elektrikle çalışan hiçbir alet kullanılamaz.
6. Cep telefonları ile görüşme yapılamaz. Yapılsa da başkaları tarafından konuşmalar dinlenebilir, mesajlar okunabilir. Hatta telefonunuzdan bilginiz olmadan mesajlar gönderilebilir, gelen mesajlar başka telefona aktarılıp banka hesaplarına erişilebilir.
7. Uçaklar, helikopterler teknik arıza verdirilip düşürülebilir. Hava Savunma sistemleri etkisiz hale getirilebilir.
8. Barajlar, acil servisler, ulaşım vs. gibi pek çok şey olası bir siber savaşta etkilenebilecek yerlerdendir (Andress ve Winterfeld, 2014).

2.9. Siber Uzay

"Siber Uzay" kavramını ilk defa 1982 yılında "Burning Chrone" adlı eserde bir bilim kurgu yazarı olan Gibson tarafından kullanılmıştır. Daha sonra aynı yazarın 1984 yılında çıkan "Neuromance" adlı eserinde bu kavramı daha da detaylandırmış ve her ulustan milyarlarca meşru kullanıcı tarafından her gün tecrübe edilen uzlaşılmış bir varsayım ve düşünülemez, tahmin edilemez karmaşa' şeklinde tanımlamıştır (Bıçakçı, 2013).

Günümüzde bilgisayar satışlarında ve kullanımındaki büyük artış insanın hayatında da değişimlere sebep olmuş ve çoğu zaman işlerini de oldukça kolaylaştırmış. Bilgisayar kullanımı ile birlikte artan internet kullanımı ile somut olarak oluşmuş coğrafi sınırlar ortadan kalkmış ve insanlar her türlü bilgiye saniyeler içerisinde erişebilmektedir ve bu şekilde bilgiye hızlı erişimin sağlandığı ve sınırları olmayan yeni bir dünya oluşmuştur. Oluşan bu yenidünya zamanla siber uzay olarak tanımlanmıştır (Gibson ve Schuyler, 2006).

"Siber uzay fiziksel bir yer değildir. Fiziksel boyut ya da uzay zaman süreklilik ölçümlerine karşı koyar. Bilgisayar ağları, bilişim sistemleri ve telekomünikasyon altyapılarının işbirliği birleşiminin yarattığı çevrenin genel olarak

World Wide Web olarak bilindiği bir kısaltmadır" (Wlingfield, 2000:125). "Siber uzay, günümüzde tek bir homojen uzaydan oluşmamaktadır. Çok sayıda, hızla genişleyen, her biri farklı bir sayısal etkileşim ve iletişim yöntemi sağlayan uzayların bir birleşimidir" (Gibson ve Schuyler, 2006:97).

2.10. Hacker

Hacker, İngilizce bir kelimedir. Türkçe karşılığı ise bilgisayar korsanıdır. Hackerlar, bilgisayar programlarına vakıf, yetenekli kişiler olarak tanınmaktadır. Hacker, şahsî bilgisayarlara veya çeşitli kurum ve kuruluşlara ait bilgisayarlara ve ağlara izinsiz olarak giriş yapan kişidir[1].

Basit manada hacker, dijital alemin güvenlik kusurlarını kullanarak bu işten ekonomik gelir elde eden kişilerdir [2] . Bilgisayar ve haberleşme teknolojileri konusunda bilgi sahibi olan, bilgisayar programlama alanında standardın üzerinde beceriye sahip bulunan ve böylece ileri düzeyde yazılımlar geliştiren ve onları kullanabilen kişilerdir.

Hacker'lar, eylemlerini kimin adına yaptıklarına ve eylemlerinin amaçlarına göre kendi aralarında çeşitlilik göstermektedir:

2.10.1. Siyah Şapkalı Hacker

Tehlikeli olan hacker çeşididir. Amaçları, güvenlik açıklarından faydalanmak suretiyle gizli bilgileri ele geçirmek veya sistemi çalışmaz hale getirmektir. Siyah şapkalı hackerlar genellikle ulaşılmasında sakınca bulunan gizli bilgileri elde etmek suretiyle maddi zararlara sebep olmuşlardır. Maddi zararların yanı sıra sistem açıklarından sızarak, kritik bilgiler ele geçirilmiştir. Siyah şapkalı hackerlar, kritik bilgilerin ele geçirilebileceğini, kritik bilgilerden sorumlu kuruluşların yeterli korunamadığını göstermiştir (Karaarslan vd., 2010).

2.10.2. Beyaz Şapkalı Hacker

Beyaz şapkalı hackerlar, donanımlarını, siyah hackerlara karşı alternatif çözümler üreterek kullanmaktadır. Güvenlik kusurlarını bulan bu kişiler, şirketlere

[1] http://tr.wikipedia.org/wiki/Hacker Erişim, 11/05/2014
[2] Beyaz Şapkalı Hackerlar, http://www.imajweb.com/beyaz-sapkali-hackerlar.html Erişim, 11/05/2014

bu tarz durumlardan nasıl kurtulabilecekleri konusunda yardımcı olmaktadır. Beyaz hacker unvanı almış insanlar bilgilerini ve donanımlarını özel şirketlere ve istihbarat örgütlerine yardım etmek biçiminde sarf etmektedir[3].

2.10.3. Gri ve Kırmızı Şapkalı Hackerlar

Gri şapkalı hackerlar, duruma göre iyi veya kötü olabilen hackerlardır. Malumat pazarlayarak hayatını kazanan kimselerdir. Bu nedenle dikkat edilmesi gereken hackerlardır. Menfaatler çerçevesinde değişiklik gösterebilmektedirler. Günümüzde bir de kırmızı şapkalı hacker olduğunu savunanlar vardır. Ne beyaz şapkalı hacker özelliği, ne de siyah şapkalı hacker özelliği göstermediklerinden, belli bir hacker kültürü ve hactivizm inancı olmasından dolayı RedHack kendini kırmızı şapkalı hacker olarak tanımlamaktadır. Bu grup üyeleri inanç olarak komünist bir inanca sahip olduklarını ileri sürerler[4].

2.10.4. Dünyaca Ünlü Hackerler[5]

2.10.4.1. Jonathan James

Hacker suçlaması ile tutuklanan, yargılanan ve hüküm giyen ilk 18 yaş altı bilgisayar kullanıcısı olan James 16 yaşında tutuklandı.

En ünlü aktivitesi: ABD savunma bakanlığındaki bilgisayarlardan birine bir arka kapı (backdoor) programı yerleştirdi, NASA bilgisayarlarından 1,7 milyon dolarlık yazılım çaldı.

10 yıl ceza aldı, 6 aya indirildi ve iyi halden salıverildi. Bilgisayarlara dokunması yasaktır (Chip, 2009).

2.10.4.2. Adrian Lamo

"Evsiz hacker" olarak adını duyuran Lamo'nun en çok ses getiren operasyonu New York Times ve Microsoft'un sistemlerine girmiş olmasıydı. Aynı

---

[3] Beyaz Şapkalı Hackerlar, http://www.imajweb.com/beyaz-sapkali-hackerlar.html Erişim, 11/05/2014

[4] Beyaz Şapkalı Hackerlar, http://www.imajweb.com/beyaz-sapkali-hackerlar.html Erişim, 11/05/2014

[5] Dünyaca Ünlü Hackerler, http://www.chip.com.tr/galeri/tum-zamanlarin-en-unlu-10-hacker-i_716.html Erişim, 11/05/2014

zamanda Yahoo!, Bank of America, Citigroup ve Cingular sistemlerine de girmiş olabileceği tahmin ediliyor.

65,000 dolar ceza aldı, altı ay ev hapsi ve 2 yıl bilgisayara dokunmama hükmü verildi. Cezasını çekti, şu anda dışarıda (Chip, 2009).

2.10.4.3. Kevin Mitnick

Kendi deyimi ile "abartılmış olan ününün kurbanı" olan Mitnick adalet bakanlığı tarafından ABD tarihinde en çok aranan bilgisayar suçlusu olarak tanınıyor. Hakkında iki film yapıldı: Freedom Downtime ve Takedown.

En ünlü aktivitesi: Telefon sistemlerini hack'lemek ve Digital Equipment Corporation'ın bilgisayar ağına girip yazılım çalmak.

Beş yıl hapis, arkasından 8 ay bilgisayara dokunmama cezası aldı. Cezasını çekti, şu an dışarıda (Chip, 2009).

2.10.4.4. Kevin Poulsen

Kod adı Dark Dante olan Poulsen'in en ünlü aktivitesi LA Radio radyoevinin KIIS-FM telefon hatlarına girerek kendisine çekilişle bir Porsche ve başka bir dizi ödül kazandırması oldu. Federal veri tabanına girmek isterken yakalandı.

Beş yıl hapis cezası çekti. Şu anda dışarıda ve gazeteci olarak çalışıyor (Chip, 2009).

2.10.4.5. Robert Tappan Morris

Dünyanın ilk solucan yazılımı olan Morris solucanının yaratıcısı olan Robert Tappan Morris bu programı aslında "internetin ne kadar büyük olduğunu test etmek için" yazdığını iddia etmekte olsa da programın çok büyük sayıda bilgisayara yayılıp ağları çalışmaz hale getirmesi sonucu yakalandı.

Üç yıl ceza aldı. 400 saat amme hizmeti yaptı ve 10.500 USD ceza ödedi (Chip, 2009).

2.10.4.6. Stephen Wozniak

Apple'ın "Woz" lakaplı yöneticisi bir beyaz hacker. Gençlik yıllarında telefon sistemlerini hack'leyen ve bedava uzun mesafe telefon görüşmeleri yapan Wozniak, Steve Jobs ile beraber Apple'ı kurdu ve bilgisayar dünyasında büyük bir devrim başlattı (Chip, 2009).

2.10.4.7. Tim Berners-Lee

World Wide Web yani www konsepti, Berners-Lee'nin bir icadı olarak ortaya çıkmıştır. Yine bir beyaz hacker olarak nitelendirilen Tim, üniversite yıllarında hacker suçlaması ile ceza almış ve bilgisayarları kullanması 3 yıl boyunca yasaklanmıştı. Üniversite yıllarında kendi bilgisayarını kendisi yapmış olan Lee hypertext (http) sisteminin yaratıcısıdır (Chip, 2009).

2.10.4.8. Linus Torvalds

Windows'un en büyük rakibi Linux'u icat eden Torvalds bilgisayar hayatına Commodore VIC-20 ile başladı. Yaptığı en büyük hack ise ünlü ev bilgisayarı Sinclair'in işletim sistemini değiştirip kolaylaştırması oldu. 1991 yılında Linux sistemini ortaya çıkartması ile dünyaca tanınır bir isim oldu (Chip, 2009).

2.10.4.9. Richard Stallman

GNU projesinin babası olan Stallman okul yıllarında MIT'te "kadrolu beyaz hacker" olarak EMACS projesinde çalışıyordu. Her kurulan şifreli koruma sistemini kırıp öğrencilere açık hale getirmesi ile ünlendi (Chip, 2009).

2.10.4.10. Tsutomu Shimomura

Bir beyaz hacker olarak adını Kevin Mitnick'i yakalayan kişi olarak duyurdu. FBI ile işbirliği yaparak kendisini zamanında hack'lemiş olan Mitnick'ten intikam aldı. Her türlü cep telefonunu kolaylıkla modifiye edebilmesi ile biliniyor (Chip, 2009).

2.10.4.11. Tamer Şahin

18 yaşında 1999 yılında Türkiye'nin en büyük internet servis sağlayıcısı Superonline bilgisayar sistemlerine girdiği suçlamasıyla suçlandı. Bu Türkiye'nin resmi olarak ilk yargılanan hack hareketi olarak ifade edildi.

2001 yılında Türkiye'nin ilk ve en eski bankası olan, Osmanlı Bankası'nı hacklediği iddia edildi fakat bilirkişi heyeti kanıt bulamayınca beraat etti.

2002 yılında Microsoft'ta ciddi güvenlik açıkları keşfedip bu açıkları Microsoft'a bildirdi. Microsoft'u hacklediği ifade edildi ve 10 ülkede haber olarak yayınlandı. Fakat Microsoft bu sayede açıklarını kapattı ve herhangi bir yasal yola başvuruda bulunmadı.

22 yaşında etik hacker olarak kendisini ifade ederek Emniyet Müdürlüğü, Jandarma İstihbarat Teşkilatı (JİT) ve Interpol ile ilk projelerini geliştirdi. Bilgi güvenliği konusunda danışmanlık yaptı.

Tamamı yerli bilgi güvenliği yazılımı olan Mindwall IDS'i geliştirdi ve bunu AT&T, Chase Manhattan Bank, Citibank gibi kuruluşlar da kullanmıştır. Microsoft, HP, AOL, Redhat, Novell gibi dünyaca ünlü üreticilerle ortak çalışmalarda bulundu.

Hacker'ın Aklı adlı bir kitabı bulunmaktadır ve burada yaşadıklarını anlatan Tamer Şahin, kurucusu olduğu TerraMedusa Secure adlı bilgi güvenliği sektöründe çalışmalarına devam etmektedir. Türkiye'de bazı üniversitelerde, kurumlarda, firmalarda bilgi güvenliği üzerine konuşmalar yapan Şahin'in, bazı gazete ve dergilerde de teknoloji üzerine yazıları mevcuttur (Şahin, 2006).

2.10.5. Hacktivist Hareketler

Türkiye' de ve dünyada hacktivist hareketleriyle ses getirmiş bazı gruplar aşağıda listelenmiştir.

2.10.5.1. Wikileaks ve Bradley Manning

Amerikan ordusunda bir süre Irak operasyonunda görev yapmış olan Kıdemli Er (Private First Class, (PFC)) Bradley Edward Manning 1966-2010 yılları arasında ABD Dış İşleri Bakanlığı tarafından yapılmış gizli yazışma ve orduya özel kullanılan veri tabanından indirmiş olduğu belge ve görüntüleri, 2010 yılında Wikileaks adlı bir internet sitesine sızdırmıştır. Bu durum ABD yönetimini sıkıntıya düşürmüştür ve bir diplomatik krize sebep olmuştur ve uluslararası arenada bir panik

havası oluşturmuştur. Manning'in yayınladığı belgeler de resmi rakamlarla sivil kayıplar, karşılaşılan ve rapor edilen tüm ayrıntılı bilgiler mevcuttu. Çünkü bu görüntüler içerisinde Cenevre Sözleşmesinin ihlalini içeren görüntüler de yer almaktaydı. Manning, görev yaptığı Kuveyt'te üssünde tutuklanarak hücreye atılmıştır ve 52 yıl hapis istemiyle yargılanmıştır. 14 Ağustos 2013 tarihinde sonuca bağlanan ceza kararıyla birlikte Manning 35 yıl hapis cezasına çarptırıldı (Wikipedia, 2014).

ABD yetkilileri Wikileaks ve kurucusu Julian Assange hakkında sansüre karar vermiş ve bu siteye erişimi engellemiştir. Bu durum üzerine tüm dünyada internetin özgür olması, bilgiye erişimin özgür olması gerektiğini savunan eylemlere sahne olmuştur. Ünlü hacker grubu Anonymous ise tepkisini sokaklarda duyurmaya çalışmıştır (Kara, 2013).

Wikileaks, sınır tanımadan herkesin erişebileceği, kolaylıkla doküman gönderebileceği bir sisteme sahiptir. Bu sayede gönderilen tüm bilgiler büyük bir bilgi havuzunda muhafaza edilir. Dosya ya da belge gönderenlerin kimlikleri gizli tutulur. Bu sayede herkes Wikileaks aracılığıyla sesini duyurup bir şeyleri düzeltme gayreti içerisinde olur. Böylece herkes hem bilgi havuzuna gönderdikleri belgelerle katkıda bulunmuş olur hem de olası haksızlıklara karşı sesini duyurmuş, bilgileri herkese ulaştırmış olur (Kara, 2013).

2.10.5.2. Aaron H. Swartz

Aaron H. Swartz, ABD federal mahkemelerinin veri tabanından 2009 yılında yaklaşık 18 milyon belgeyi indirip, internette ücretsiz yayınlamıştır. Bu belgeler PACER veri tabanından para karşılığı satılan belgelerdir. Daha sonra 2011 yılında JSTOR (Journal Storage) adlı çevrimiçi akademik makale ve dergilerde arşivleme için kullanılan sistemden de 3 milyondan daha fazla belgeyi, makaleyi ve kitabı MIT Üniversitesinin (Massachusetts Institute of Technology) bilgisayarlarını kullanarak bilgisayarına indirmiş ve bunları internet üzerinden herkesin kullanımına açmıştır. Bu durumdan dolayı, hakkında yasadışı dosya indirme ve bilgi korsanlığı suçlarından dava açılmış ve 35 yıl hapis cezasına çarptırılması beklenmekte iken 10 Ocak 2013 tarihinde Swartz intihar etmiştir (Kara, 2013). Bir hacker İsveçli bir yayınevinin sitesinden yüz binlerce bilimsel makale indirmiştir ve onların tamamını

Swartz'ın ölümünün 1. Yıldönümünde Swartz anısına yayınlamıştır (Wikipedia, 2014).

Reddit adlı sosyal haber sitesini kuran kişi Aaron H. Swartz'dır. Ayrıca Demand Prograss adlı bir hareket oluşturmuştur ve bu hareketin öncüsü konumundadır. Bu hareket, telif ve mülkiyet hakkı konulu, internette telif hakkı ihlali durumunda ve telif hakkı ile korunan şeyleri yayınlatmamak için çalışan aksi durumda da hak sahiplerine adı geçen siteler hakkında mahkeme kararı çıkartmayı sağlayan PİPA ve SOPA adlı yasa tasarısına karşı oluşmuş bir harekettir. İnternette bilgi özgürce paylaşılmalıdır ve internet özgürlüğü bu hareketin temel taleplerinin başında gelmektedir (Kara, 2013).

2.10.5.3. Anonymous

2003 yılında internet üzerinden bir araya gelerek oluşmuş bir gruptur. Grubun simgesi gülen adamdır. Grubun da kendisi için seçtiği sloganı "Biz anonimiz. Orduyuz. Affetmeyiz. Unutmayız. Bizi bekleyin" şeklindedir. Bu grubun dünyanın her tarafından üyesi olduğu ifade edilmektedir. Bu nedenle çevrenizde herhangi bir kişi bile bu gruba üye olabilir ve dolayısıyla da sayısı net olarak bilinmemektedir. Hiyerarşik bir düzene karşı olan bu grup liderliğe de karşı olarak ön plana çıkmaktadır. Devletin sitelerine saldırarak siyasi tepkilerini ifade etmektedirler ve ayrıca sabit bir politika da takip etmemektedirler. Şimdiye kadar savundukları bilinen tek durum da internetin özgür olmasıdır. 2010 yılında Wikileaks sitesinden ifşa edilen belge ve dokümanların açıklanması olayının ardından sansür propagandalarını sokaklarda gülen adam maskeleriyle yapmışlardır. Bir hacker grubu olarak seslerini sadece internet üzerinden duyurmadan sokaklarda da propaganda yapmak grubun dikkat çekmesine yardımcı olmaktadır. DDoS saldırı silahı ise grubun internet saldırılarında kullandığı bir yöntemdir.

Grubun dünyanın her tarafından saldırısı olmaktadır ve bu durum da Anonymous'a bağlı olan grupların dört bir yanda olduğunu göstermektedir. Grubun bu kadar geniş çapta olması grubun dağınık bir yapılanma şekline sahip olduğunu göstermektedir. Organize olmak istedikleri zaman ise internet bu kadar dağınık ve birbirinden uzak kişileri tek bir tık kadar yaklaştırmaktadır. Bu dağınıklık ve kısa

sürede organize olabilme hali kimi zaman saldırılmak istenen hedefler konusunda ikiliklere sebebiyet de verebilmektedir.

Grup adını ilk kez Sony'ye yaptığı operasyonla duyurmuştur. Daha sonra da çeşitli saldırılarla ününü artırmıştır. Bunlardan bazıları; ABD ordusuna silah tedarik eden Lockheed Martin şirketine yaptığı saldırı, İrlanda yerel seçimlerinde 2011 yılında bir partinin web sitesine girerek siteye mesaj bırakması, Arap Baharı'na destek veren Tunuslu hackerlarla birlikte devletin bazı sitelerinin çökertilmesi operasyonu. Ayrıca, Wikileaks olayının ardından Visa, MasterCard ve PayPal bu siteyle çalışmak istememiş ve bunu bahane ederek MasterCard ve Visa'nın sitelerini çökertmişlerdir. Burger King adlı firmanın Twitter adresini hackleyip, bu firmaya rakip firma olan McDonalds'ın logosunu ve resimlerini Burger King'in hesabından yayınlamıştır. İsrail'in Gazze'ye saldırması sonucu İsrail'e ait web sitelerini hedef alan saldırılar düzenlemiş ve birçok siteyi çökertmiştir (Kara, 2013). "opTurkey" Operasyon adıyla, 12 Haziran 2013'de grup RTÜK'ün İnternet sitesini erişilmez kıldı.Grubun Türkiye'deki üyelerinin Twitter hesabından yapılan açıklamada, "Tango Down | RTÜK - Doğruları yazan medya kuruluşlarına ceza verdiniz. Simdi de Anonymous sizi cezalandırdı" denildi (Wikipedia, 2012). Ayrıca Suriye Devlet Başkanı Beşar Esad da Anonymous'un hedefi oldu. Anonymous, Başkanlık bürosunun e-mail hesabına girerek yüzlerce yazışmayı internete sızdırdı (Haber, 2012).

2.10.5.4. RedHack

1997 yılında kurulan, kendilerini Marksist ve Sosyalist olarak tanımlayan hacker grubu. Şubat 2012'de Ankara Emniyet Müdürlüğü'nün internet sitesini çökerterek adlarını duyuran grup aynı zamanda Türkiye genelinde yaklaşık 350'ye yakın emniyet müdürlüğü sitesini geçici bir süreliğine çalışamaz hale getirdi. Grubun çekirdek kadrosunu oluşturan üye sayısının ise 12 olduğu ifade ediliyor.

Sosyal medyayı kullanarak hem eylemlerini, protestolarını hem de saldırılarını destekçileri ile paylaşmaktadır. Grup çekirdek üyeleri haricinde diğer üyelerle bir tanışıklıkları yoktur. Eylemlerini de halkın ihtiyacına göre düzenlediklerini belirtmektedirler. Türkiye'de yaşan güncel olayları dikkatlice takip edip protestolarını ve tepkilerini hem bilgisayar başında hem de sokaklarda duyurmaktadır. Kendilerini hacker olarak değil de devrimci olarak tanıtan grup dış

istihbarat servisleriyle birlikte çalışmadıklarını, kişisel tekliflere ve şirketlerin tekliflerine cevap bile vermediklerini ifade etmektedirler. Bir tüzük çerçevesinde çalışan grubun, örgütlenmenin bir ürünü olarak RedHack adlı grubun oluştuğunu belirtmektedir. Grup kendisine karşı oluşturulan siber timlere karşı da kendilerini savunacak teknik bilgi ve birikime sahip olduklarını belirtmektedir ayrıca kendilerine güvendiklerini olası saldırı karşısında savunma ve saldırı yeteneklerini de değerlendirebileceklerini belirtmektedirler (RedHack, 2013)

Hala faaliyetlerine devam eden grubun son aylarda güncel olaylarla alakalı tepkilerini ifade ettikleri saldırılar gerçekleştirmektedir. Son günlerde Soma'da yaşanan maden kazası ile ilgili AKP Manisa Milletvekili'nin hazırladığı rapora erişip raporu yayınlama faaliyeti, başbakanın danışmanının e-mail hesapları, facebook ve twitter hesaplarının ele geçirilip konuşmaları ve geçen bilgileri yayınlama faaliyeti (Wikipedia, 2014)

2.10.5.5. LulzSec

ABD büyükelçiliğinin yapmış olduğu gizli anlaşma belgeleri Wikileaks adlı sitede açıklanmış, Wikileaks sitesi bu durumdan dolayı hackerlara tarafından DDoS saldırıları ile saldırıya uğramıştır. Anonymous grubu da MasterCard, Visa ve Paypal ve birçok kuruma saldırı başlatmıştır. Ardından protestolar yapılmıştır. Bu protestoların hemen ardından ortaya kendilerine LulzSec ismi verdikleri hactivist bir grup ortaya çıkmıştır.

LulzSec bazı önemli şirketlerin ve ülkenin önemli kurum sitelerine saldırılar yapmış ve bu saldırılarda da desteğini "Halk ya da tüketiciler aleyhine çalışmalar yaptığı" iddiasından almaktadır. Fakat bu grubun ömrü pek uzun sürmemiştir. 2011 yılında sadece 50 gün faaliyetlerine devam etmişlerdir ve kendilerini feshettiklerini ilan etmişlerdir. Fakat grup 2012 yılına gelindiğinde ise LulzSec reborn olarak yeniden faaliyetlerine devam etmiştir. Grubun en yaygın olarak kullandığı silah türü DDoS siber saldırı silahıdır. Bu saldırı yöntemiyle ABD ve İngiltere'de faaliyet gösteren yüksek özelliğe sahip hükümet ve özel sektör web sitelerini hedeflemiştir.

Grup aslında Anonymous adlı hactivist grubun bir parçası olarak bilinmektedir. Grubun birçok devlet ve özel sektör şirketine saldırısı olmuştur. Bu saldırılar arasında 20th Century Fox, Nintendo, PayPal, MasterCard ve Sony Pictures gibi şirketler de yer almaktadır. Özellikle Sony Playstation ağını hedef alan saldırısı

dünyada geniş yankı oluşturmuştur. Bu saldırı sonucunda veri tabanında yer alan yaklaşık 77 milyon playstation kullanıcısının bilgisine erişmişi ve onları elde ettiğini duyurmuştur. Grup aynı zamanda CIA web sitesine saldırmış ve siteyi erişime kapatmıştır. Bu siteyi kapatma sorumluluğunu kabul eden grup lideri Glen McEwen (24) Avustralya'da Federal polis yetkilileri tarafından yakalanmıştır (24.04.2013) (Kara, 2013).

2.10.5.6. Cyber-Warrior Team (Akıncılar)

Ülkemizin maddi, manevi değer ve inançlarına saldırıda bulunan web sitelerini hacklemesi ile tanınan bir Türk hacktivist grubudur. Mavi Marmara gemisi ile Gazze'ye yardım götürmek isteyen yardımseverlere uluslararası sularda yaptığı saldırı sonrasında tepkisini İsrail'in birçok web sitesini çökertmekle göstermiştir. Herhangi bir kurum, örgüt, parti, siyasal ya da ideolojik görüş ile bağlantısı olmayan gruba ait bir de internet sitesi mevcuttur. Grup üye olmak isteyen herkese açıktır ve uzmanlık ve bilgi düzeylerine göre de organizasyonlarda görev verilmektedir. 2003 yılında Temmuz ayında Irak'ta ülkemiz askerlerinden 11 tanesinin başına çuval geçirilmesi olayını protesto etmek için 1500 adet Amerikan sitesini hacklemiştir (Kara, 2013). Hacklediği sitelere "BİR TÜRK AMERİKA'YA BEDELDİR 11 TÜRK İÇİN DÜNYAYI FETHEDERİZ" ve "Şimdilik 1.500 tane sitenizi topraklarımıza dâhil ediyoruz IP/Cyber Warrior Team Akıncılar Grubu" şeklinde mesaj bırakmıştır (iP/CyberWarrior Team, tarih yok).

Amerika'daki 1500 sitenin çökertilmesinin ardından FBI tarafından aranan Türk korsan grubu, Danimarka'da yaşanan ve Hz. Muhammed (sas) karikatürü krizinden dolayı buna muhalefet etmeyen, sessiz kalarak destek olan ve bu duruma tepkisini göstermeyen 3000 siteyi hackledikleri bilgisini verdi (Günacar, 2011).

> "……. Filistinli 17 yaşındaki Muhammed Hüseyin Ebu Hudayr'ın diri diri yakılarak öldürülmesi sonrasında hızla gelişen olaylara İsrail'in orantısız ve sert saldırıları ve bu saldırılarda hayatını kaybeden çoğu çocuk 600'a yakın Filistinliye karşı dünyanın sessiz kalmasını ve her defasında İsrail'in bu saldırgan davranışlarının cezasız kalmasını protesto eden grup, İsrail'e tepkilerini internet üzerinden yayın yapan web sitelerine yönelik hack saldırıları ile gösterdiklerini açıkladılar.
> Hacklenen bin 500 site içinde en dikkat çekenler, İsrail'in en büyük gazetesi Haaretz, İsrail'in en büyük teknoloji sitelerinden msn ile iş ortağı olan, elem.il.msn.com, İsrail baş hahamın resmi sitesi, Avrupa hahamlar birliği resmi sitesi gibi birçok devlet sitesi ve özel siteler hacklendi. Akıncılar Grubu hackledikleri sitelere Türkçe ve İngilizce olarak; "Kudüs davası Müslümanların onur mücadelesidir. Başbakan Erdoğan: "Bu topraklarda dökülen her gözyaşı bizim gözyaşımızdır" Biz hiçbir zaman vicdanı kurumuş bir millet olmadık. Filistinli başını öne eğmedi, eğmeyecek. Akıncılar olarak

> bütün dünyaya sesleniyoruz: Ya hakkın yanında olacaksınız ya batılın yanında olacaksınız. Biz Hakkında yanında olmak için Filistin davasını seçtik. Biz OSMANLI'yız, Biz TÜRKİYE'yiz, Biz AKINCILAR'ız" şeklinde not bıraktı. Cyber Warrior Akıncılar Gurubu'ndan yapılan açıklamada, "İsrail devleti bizim için yok hükmündedir ve terörist bir devlettir. Filistinlilere on yıllardır yaptıkları zulme ve saldırılara dünyanın sessiz kalması, İsrail'e herhangi bir yaptırım uygulamaması kabul edilebilir değildir. Biz Akıncılar Gurubu olarak dünyanın göz yumduğu bu İsrail zulmüne sessiz kalmayacağız. Filistin halkının yanında yer aldığımızı göstereceğiz. Dünya sussa da biz susmayacağız……." denildi" (İHA, 2014).

2.10.5.7. Ayyıldız Tim

Ayyıldız Tim adlı hacker grubu, Türkiye aleyhine yapılan bir saldırı durumunda bunu engellemeye çalışan ve Türkiye lehine saldırılar düzenleyen bir gruptur. Grubun üstlendiği görev Türkiye'yi siber saldırılardan korumaktır. Türkiye'yi hedef alan bir olası veya olan bir saldırı durumunda bu saldırılara karşı saldırı yapıp cevap vermeyi bir görev olarak edinmiştir. Devlet kurumları, devlet büyükleri, maddi ve manevi değerlerimize yapılan saldırıları ülke bütünlüğüne yapılan saldırılar olarak görmüş ve karşı saldırıya geçmiştir. Grubun farkı kendilerini, grup yöneticilerini açıklamaktan rahatsızlık duymamaktadır. Grubun kendilerine ait bir web siteleri vardır ve burada yaptıkları faaliyetler hakkında bilgi vermektedirler. Ayrıca yaptıkları eylemlerin de yasa dışı olmadığını iddia etmektedirler. Yaptıkları önemli saldırı ve karşı saldırılardan bir tanesi Pentagon'un web sitesine erişimi 8 saat boyunca kapatmıştır diğeri ise ülkemiz Telekomünikasyon İletişim Başkanlığı (TİB)'na Anonymous tarafından gerçekleştirilen saldırıya karşı atak ile cevap vermeleridir (Kara, 2013).

Gazze'ye saldırı düzenleyen İsrail'i protesto etmek için günlerce sosyal medya üzerinden Coca-Cola'yı boykot ettiğini ve takipçilerine çağrıda bulunmuştur. Buna ek olarak bir hamle ile Coca-Cola'nın resmi sitesi coca-cola.com ve coca-cola.com.tr adreslerini hackledi ve hayranlarını sevindirdi. Grup Facebook sayfasından da duyurduğu hackleme işleminin ardından "Gazze için, ölen çocuklar için Coca-Cola erişime kapatılmıştır!" şeklinde açıklama yaparak protestolarını da gerçekleştirmiş oldular (Doğan, 2014; Hürriyet, 2014)

2.10.5.8. 1923 Turk-Grup

Dünyaca ünlü Türk hacker grubu 1923 Turk-Grup adlı hacker grubu Avrupa'da bir çok siteye saldırıda bulundu. İtalyan Zone-H sitesi de bu saldırıları doğruladı.

TRT Haber'de canlı yayında hedeflerini ve amaçlarını belirten grup kendilerini bir Beyaz Şapkalı Hacker olarak tanımlıyor. Hedeflerini de PKK terör örgütünün propagandasını yapan internet siteleri ile birlikte pornografik, kumar, bahis ve çocuk istismarı gibi internet siteleri olarak belirtiyorlar. Ayrıca Avrupa'daki hedeflerinin de sebebini Türkiye'nin aleyhine yayınlar yapıp karalama kampanyasına girişen siteler olarak belirtmektedirler.

Bugüne kadar yaklaşık 150 Bin internet sitesini hackleyen 1923Türk-Grup yöneticileri "Türkiye'nin Siber Savunma Gücü 1923TURK-GRUP olarak İnternet ortamında Milli benliğimize, Ulu Önderimiz Mustafa Kemal Atatürk'e, Bayrağımıza ve Devletimize karşı yapılan her türlü çirkince saldırının karşısındayız" ayrıca "Sözde Ermeni Soykırımına destek veren Fransa olmak üzere diğer Avrupa ülkelerine de saldırılarımız sürecektir" şeklinde ifade ettiler.

Yapılan son saldırılarda grubun hacklediği sitelere verilen zarar yaklaşık 1,5 milyon Euro olduğu tahmin edilmektedir (Bitdunyası, 2012).

2.11. Dünyada Siber Alan

Gelişen teknoloji ve insanların sınır tanımayan istek ve arzuları önüne geçilemeyecek bir hal almıştır. Küreselleşmenin vermiş olduğu bir haz ile dünya artık evimize sığabilecek kadar ufak. Bilinmeyeni bilme arzusu insanların kabiliyetlerinin inkişafına sebep olmuştur. İnsanoğlu atomu parçalarına ayırabildiğinde artık ölümcül bir silah yapmaya hazırdı. Aynı şekilde evde oturduğu yerde sınırsız bilgiye de ulaştığını anladığı anda diğer kişi ve tüzel kişilerin haklarına müdahaleyi kendisine vazife bildi.

Cephe savaşlarının sona ermeye başladığı bu yüzyılda insanoğlu başka bir cephe arayışına girdi ve siber alanı keşfetti. Bundan sonra insanoğlu en ufak bir anlaşmazlıkta hasmına sanal yani siber alanda zarar vermeyi kendine idol saydı. Bu rekabet devletler muvazenesine taşındı ve artık her devlet çatısı altında siber ordular kuruldu ve aynı zamanda gelebilecek tehditlere karşı siber savunma teşkilatları kuruldu. Bu alanda başı çeken dünya devleri kendi siber savunma teşkilatlarını kurmuş ve bununla alakalı yasalar yürürlüğe konulmuştur. Dünya çapındaki BM, NATO ve AB gibi birlikler kendilerine gelebilecek olası saldırılara karşı ortak hareket etme kararları almışlardır. Ne var ki siber suçlarının adını koymak pek de

kolay olamamıştır. Çünkü birine göre suç sayılan bir eylem diğerlerine göre özgürlük olarak nitelendiriliyordu.

İnternetten kaynaklanan ve teknik alt yapısının sebep olduğu sorunlar nedeniyle inanılmaz derecede hızlı gelişen bu teknoloji ile bu gelişmelerin getirmiş olduğu olumsuz durumlar karşısında yapılan hukuki düzenlemeler de bu teknolojinin çok gerisinde kalmıştır. Çünkü işlenen geleneksel suçlarla birlikte bir araç olarak da kullanılmaya başlandı ve başlı başına bir suç aleti ya da suç olarak da ifade edilmeye başlandı. Bu sorunların farkına varan ülkeler hemen kendilerince bir takım çözümler bulmaya, önlemler almaya çalışmışlardır (Keçeci, 2014).

Dünyada siber alanla ilgili hemen hemen her devletin siber alanla alakalı bir takım çalışmaları vardır. Dünya'daki bazı devletlerden örnekler;

2.11.1. Amerika Birleşik Devletleri:

ABD Başkanına bağlı "Commission of Critical Infrastructure Protection" adlı bir komisyon 1996 yılının Temmuz ayında oluşturuldu. Bu komisyon internet alanında çalışma yapan ilk ulusal komisyon olarak belirtilmektedir. Bu komisyonun görevi ise siber suçların takibini yapmak ve olabilecek suçları önlemeye çalışmaktır. Bununla birlikte ABD'de siber suçları önlemek ve onlarla mücadele etmek amacıyla FBI kurumuna bağlı "National Infrastructure Protection Center*"* ve *"*Computer Crime Squad" adlarıyla iki merkez kurulmuştur. Bunların dışında "Information Technology Association of America*"*, *"*Trap and Trace Center Authority*"*, *"*CIA Information Warfare Center*"* gibi birimler ABD'deki siber suçlarla mücadele için oluşturulmuş diğer birimler arasındadır (Atıcı ve Gümüş, 2003).

Londra'da King's College'da bir öğretim görevlisinin "Siber Savaş Olmayacak" adlı kitabında siber saldırıların abartıldığı ifade edilmektedir. Abartılması da normal olarak görülüyor çünkü siber saldırılara temel oluşturabilecek bir sistemin varlığı hala ortada ve bu durum da ABD'yi siber tehdit noktasında kendisini güçlendirmeye itiyor. Pentagon'un 4000 'Siber Savaşçıyı' işe aldığı ve altyapı sistemini güçlendirmek ve saldırılardan korumak için yeni bir başkanlık önergesi imzalandığı da belirtilmektedir (Hürriyet, 2013).

2.11.2. İtalya:

İtalya Emniyet Genel Müdürlüğüne bağlı *"Posta ve İletişim Güvenliği Daire Başkanlığı''* oluşturulmuştur. Bu başkanlık 30 Mart 1998 tarihinde kurulmuş ve amacı ise siber suçlarla mücadele etmektir. 20 farklı ilde ofisi bulunmakta ve personel-lojistik ve teknik alan olmak üzere iki bölümü bünyesinde barındıran kurum başkanlığa bağlı olarak faaliyet göstermektedir ve dijital dünyada işlenen her suç bu başkanlığın görev alanına girmektedir (Atıcı ve Gümüş, 2003).

2.11.3. Fransa:

Her ülkede olduğu gibi Fransa'da da siber saldırıları ve siber suçları önleme maksadıyla bir dizi önlemler alınmaya çalışılmıştır. Başbakana bağlı Milli Savunma Genel Sekreterliği (SGDN) bünyesinde birçok birim kurulmuştur. Bunlardan bazıları; "*Haberleşme Sistemleri Güvenliği Merkez Birimi"* (DCSSI), *"Haberleşme Teknolojisi Kullanılarak Yapılan Dolandırıcılıkların Soruşturulması Birimi"* (SEFTI), ''*Bilgisayar Ortamında İslenen Suçların Bastırılması Birimi''* (BCRCI) ile "*İletişim ve Enformasyon ve Teknolojilerinin Kullanımı Suretiyle İşlenen Suçlarla Mücadele Bürosu* "dur (Atıcı ve Gümüş, 2003:108).

2.11.4. İsviçre:

İsviçre *"Federal Ceza Yasası"* ve *"Haksız Rekabet Yasası"* adı altında iki federal yasayı siber suçlar, siber terörizm ve bilişim suçlarıyla mücadele etmek için çıkarmıştır. Bu yasalardan Federal Ceza Yasası, yasadışı yollarla teknolojiyi kullanarak bilgi edinme, değiştirme, tahrip etme, silme ve çalma gibi suçların cezalandırılması için çıkarılmıştır. Diğer Haksız Rekabet Yasası ise, yine bilişim suçlarının cezalandırılması ve bunlara verilecek cezalar için çıkarılmış bir ceza yasasıdır fakat ticari amaçlı işlenen bilişim suçları bu yasa kapsamında değerlendirilmektedir (Atıcı ve Gümüş, 2003).

2.11.5. Hindistan:

Dünyanın en kalabalık ülkesi olan Çin'den sonra 2. sırada yer alan Hindistan'ın yakın gelecekte büyük nüfusu, bilişim sektöründeki yazılım ve donanımla alakalı yatırımlarıyla ve de son yıllarda siber alana verdiği önemle birlikte

dünyada stratejik ve politik anlamda güç dengelerini önemli oranda etkileyeceği tahmin edilmektedir.

Bilişim sektöründe giderek büyüyen tehditlerle mücadele etmek ve gelecek tehditleri bertaraf edebilmek için Hindistan Devleti Inter Departmental Information Security Task Force (ISTF) isimli kuruluşu oluşturmuş ve Ulusal Güvenlik Konseyi (National Security Council) ile birlikte en üst düzeyde yetkilendirmiştir. Bu şekilde çok kapsamlı bir ulusal siber güvenlik politikasına kapılarını açmıştır. ISTF isimli kuruluşun yaptığı öneriler doğrultusunda devlet düzeyinde çalışmalarla bilişim suçları ile mücadeleye başlamış ve geliştirmiştir.

1. Ulusal bilgi güvenliği tehdit algılamalarının saptanması
2. Kritik altyapıların korunması
3. Bilgi güvenliğinin sağlanması için gerekli yasal düzenlemelerin hazırlanması
4. Siber güvenlik konusunda farkındalık yaratılması ve ilgili personelin eğitimi
5. Siber güvenlik konusunda araştırma ve geliştirmelerin desteklenmesi ve bu çalışmalara özel sektörün ve üniversitelerin de dâhil edilmesi (Durna, et al., 2012:5).

Hindistan'da Bilgi Güvenliği Çerçeve Politikası hazırlanmıştır. Bu politikanın amacı ise Hindistan'a ait olan kritik alt yapıların korunması ve ağların korunmasıdır. Ulusal boyutta ve ülkenin her tarafında Bilgi Güvenliği Farkındalığı ve Eğitimi Kampanyası sürdürülmektedir. Bu Eğitim kampanyasının asıl hedefi ise ülkenin siber alanını güvenli hale getirmektir. Bu kampanya ile de şunlar hedeflenmektedir.

1. Ülkenin kritik bilişim sistemleri ve altyapılarına yönelik saldırıların önlenmesi,
2. Siber saldırılar karşısındaki zafiyetin azaltılması,
3. Siber saldırılardan doğan zararların en aza indirilmesi ve müdahale/düzeltmelerin en hızlı şekilde yapılabilmesi. (Durna, et al., 2012:6)

Güvenli bir siber uzay oluşturabilmek için yapılması planlananlar:

1. Olası saldırı esnasında analizin durmaksızın yapılması ve buna temel olabilecek bir bilişim sistemi geliştirilmesi ve cezai sorumlulukların belirtilmesi
2. Kritik ağ, altyapı ve bilişim sistemlerinin özenle korunması ve bu yönde tedbirler alınması

3. Olası saldırıyı önceden tespit etme ve buna yönelik ikaz sistemi geliştirilip saldırıdan haberdar olunmasını sağlamak
4. Ekonomiyi korumak için olası organize saldırılar karşısında tam bir muhafaza sağlanabilmesi
5. Önemli firmaların bilişim sistemlerinin güvenliklerini en üst düzeyde sağlayabilmeleri için onlara AR-GE desteğinin verilmesi, kritik düzeyde olan sistem ve firmalara da bu destekle yardımcı olunması (Durna, et al., 2012:6)

2.11.6. Çin

Çin halk Cumhuriyeti siber alana çok büyük bir önem vermiştir ve bu amaca hizmet etmek için Çin Halk Kurtuluş Ordusu'nun (People's Liberation Army – PLA) üzerine büyük bir destek vermiştir. Çin askeri stratejisine göre, klasik savaşla birlikte ilerleyen, onunla fırsatları değerlendirebilecek bir siber güvenlik hayati öneme sahiptir. Çünkü siber güvenlik savaşta hayati sonuçlar ortaya çıkarabilmektedir. Bu nedenle siber güvenlikten birinci dereceden sorumlu olarak orduyu tutmuştur. Çin Halk Kurtuluş Ordusu'nun (PLA) Genel Kurmay Bölümünde (General Staff Department – GSD) iki ayrı bölümü ülkenin bilişim alt yapısından ve korunmasından sorumlu olarak belirtmiştir. "Bu birimler hava, kara, deniz kuvvetleri ve milis kuvvetlerin ilgili siber güvenlik birimleriyle birlikte Çin sınırları içerisindeki tüm iletişim trafiğini izlemektedirler" (Durna, ve diğerleri, 2012). Bu alanda aralıksız AR-GE çalışmaları düzenlenmektedir ve her birimin altında en az 12 adet operasyonel büro bulunmaktadır. Bu bürolardaki çalışanlarla birlikte resmi olmayan bir rapora göre sadece 1 bölüm bünyesinde 120000'den fazla çalışan olduğu belirtilmektedir (Durna, ve diğerleri, 2012).

PLA'da dünyanın en hızlı bilgisayarları ve bilgisayar sistemleri mevcuttur. Jiangnan Bilgisayar Teknolojileri Araştırma Enstitüsü (Jiangnan Computer Technology Research Institute) ise Çin'deki en eski ve büyük AR-GE merkezidir. Bu AR-GE merkezi Çin'de yer alan bilgisayar merkezlerine süper bilgisayarlarla ve süper bilgisayar yatırımlarıyla destek vermektedir. Süper bilgisayarlarla PLA bünyesinde organizasyonlar düzenleyip, diğer ülkelerin kullandıkları karmaşık kodları ve şifreleri kırma çalışmaları ise gittikçe artmıştır.

Çin, bilişim savaşları ve bilgi teknolojileri alanında bu alanda öncü olmak istemektedir ve bu durumu da açıkça beyan etmiş ve yaklaşık 20 yıldan beri bu

alanla alakalı teoriler, doktrinler ve politikalar geliştirmiştir. Çin'in bazı ordu merkezlerinde de siber savaş eğitimleri de vermektedir. Bu da 90'lardan itibaren modernleşme ve bilgileştirme adı altında geliştirilen bir durum olup bilişim teknolojileri ve siber uzay alanlarında etkin güç haline gelme amaçları için ne kadar çalıştıklarını göstermektedir.

2.11.7. Estonya:

Rusya'nın 2007 yılında Estonya'ya yönelik saldırıları sorunu ülkede birçok kurum bu durumdan zarar görmüştür. Bu olay ülkede siber alan, siber uzay kavramlarını daha sık telaffuz edilir olmasına vesile olmuştur. Bu durum ülkenin siber politikasını da kendi içerisinde ciddi şekilde sorgulamasına sebep olmuştur. Ülkenin siber savunma amacıyla yeteneklerini ortaya koyabilmesi ve siber faaliyetlerin gerçekleştirilmesi için Savunma Bakanlığı üzerinde önemli çalışmalara başlamışlardır. Bu çalışmaların başında Defense League (Savunma Ligi) adını verdikleri bir çalışma da bulunmaktadır. Yapılan çalışma ile bu organizasyon Estonya halkının elektronik yaşamları için eğitim sunmak, onları koruma altına almak, bilişim uzmanları yetiştirmek gibi görev üstlenmiştir.

Ülkede Siber Güvenlik Konseyi oluşturulmuştur ve bu konseyi ile de ülkenin zayıf olduğu alanlarda güçlenmek, gelebilecek siber saldırılara cevap verebilmek, kritik öneme sahip altyapılarını da en kısa sürede çözüme kavuşturabilmek amacıyla ülkede siber atılımları gerçekleştirecek çok önemli adımlar atılmıştır ve uluslararası işbirliğini de güçlendirmeye başlamıştır.

NATO üyesi olan Estonya, bu çatı altında bulunan Bilişim Güvenliği alanında diğer üye ülkelerle de işbirliğini artırarak bu alanda giderek daha da aktif bir rol oynamaya başlamıştır. NATO bünyesinde oluşturulan Siber Savunma Mükemmeliyet Merkezi ile de üye ülkelerle bilgi paylaşımından, AR-GE çalışmalarına kadar birçok alanda araştırma ve geliştirme faaliyetlerine devam etmektedir. Ayrıca bu merkezin en önemli bilgi sağlayıcılarından biri olarak da bilişim alanına ne kadar önem verdiğini de göstermektedir.

Ülkede, Kritik Altyapıları Koruma Şubesi kurulmuş ve bu şube de geliştirilen projeleri destekleyerek hayata geçirmekle ve olası, acil saldırılara karşı da bir değerlendirme raporu da hazırlamaktadır (Durna, ve diğerleri, 2012).

2.11.8. Birleşik Krallık:

İngiltere'de hükümet 2010 yılında bir rapor hazırlayıp parlamentoya sunmuş. Bu rapor Ulusal Güvenlik Stratejisi olarak ifade edilmektedir ve yayınlamıştır. Organize şebekeler, siber saldırılar karşısında verilecek cevap, siber teröristler de raporda yer almıştır. Rapor, İngiltere'de ülkenin karşılaşabileceği olası riskleri gruplara ayırmış ve siber saldırı ise en yüksek risk grubunda olarak ifade edilmiştir. Ayrıca diğer ülkelerden de İngiltere'ye siber saldırıların olduğu ifade edilerek bu yıl ve bu yılı izleyen on beş yıl boyunca en yüksek dereceli olarak ulusal güvenlik risklerinden biri olması gerektiğine vurgu yapılmıştır.

İngiltere'de kurulan kuruluşlar, "Office of Cyber Security and Information Assurance" siber güvenlik alanında çok büyük değişiklik yapılmıştır. Ulusal Güvenlik Stratejisi programı ile birlikte askeri alanda da yeni siber güvenlik birimleri kurulmuştur. Savunma Bakanlığı'na bağlı (Global Operations and Security Control Centre) Küresel Operasyonlar ve Güvenlik Kontrol Merkezi ile birlikte (Defence Cyber Operations Group) Siber Operasyonları Savunma Grubu ayrıca Joint Cyber Unit adlı bir birim de kurulmuştur. Karşılaşılan siber suçların organize suçu olması halinde ise bu suçlarla ilgilenecek olan National Crime Agency (Ulusal Suç Birimi) adlı bir de kurum oluşturulmuş.

İletişim alt yapısının büyük bir kısmının özel sektörün elinde olduğu için Ulusal Altyapının Korunması Merkezi (Center for the Protection of National Infrastructure) sayesinde bu kuruluşlarla devamlı iletişim halinde olup onlarla bilgi alışverişi içerisindedir.

Ülkede Siber Güvenlik uzmanlarının yetiştirilmesi için yeni programlar açılmış ve bu programlara katılımı teşvik etmiş. Üniversitelerin ilgili bölümlerinde ise yüksek lisans, doktora programları açarak araştırma merkezleri kurmayı planlamıştır. Bu araştırma merkezine ise 2 milyon poundluk bir bütçe ayırmıştır (Durna, ve diğerleri, 2012).

2.11.9. Almanya:

Almanya hükümeti ülkede yaşayan halka büyük bir sosyal ve ekonomik refah sağlamak amacıyla siber alana yönelik büyük katkılar sağlamaya çalışmaktadır. Almanya'da da birçok ülke de olduğu gibi genel güvenlik stratejisi Alman Ordusu tarafından sağlanmaktadır. Fakat siber alanın sınır tanımaz yanından dolayı ülkede siber alan üzerine yürütülen politikalarda uluslararası işbirliği ve koordinasyon

olmazsa olmazlardandır. Bu işbirliğine Almanya'nın dâhil olduğu G8, NATO, AB vs. gibi grupların haricinde birçok örgüt ve grup ta dâhildir.

Ülkede siber güvenlikle alakalı alınan tedbirlerden bazıları şunlardır:

Kritik bilgi alt yapılarının korunması alınacak tedbirlerin en başında gelmektedir. Buna ek olarak kamu ve özel sektör kurum ve kuruluşları ile birlikte daha koordineli ve bilgi paylaşımının sağlandığı bir bileşen oluşturmak da önem arz etmektedir.

Information Technology Systems (Bilgi Teknolojileri Sistemleri)'ni geliştirip daha güvenli alt yapılar oluşturmak. Oluşturulan bu alt yapıların kullanıcılarından da geri dönütler alınarak ortak bir çerçevede sistemi geliştirmek

Güvenli bir Federal ağ oluşturarak elektronik ses ve veri iletiminde hizmet etmelerini sağlamak

Bilgisayar Acil Durum Müdahale Ekipleri ile olası acil durumlarda hazırlıklı olmak ve bu alanda her zaman bir saldırı bekleyerek her zaman hazırlıklı olmak

Ulusal Siber Müdahale Merkezi oluşturularak diğer devletler iş birliği halinde olmak, oluşturulan bu merkez Bilgi Güvenliği Federal Dairesi, Anayasayı Koruma ve Sivil Koruma Federal Dairesi ve Afet Yardımı Federal Dairesi ile direk olarak birlikte çalışma halinde olacak. Ayrıca Devlet Bakanı başkanlığında oluşturulan bir kriz yönetim kadrosu bulunmaktadır. Olası bir sorun veya saldırının kritik seviyelere çıkması halinde kriz yönetim kadrosunu derhal bilgilendirecektir.

Devletin siber saldırılara karşı her an hazırlıklı olması isteniyorsa bu durumda devletin yetkili makam ve mercileriyle sürekli bir işbirliği halinde olması gerekmektedir (Durna, ve diğerleri, 2012).

2.11.10. İsrail:

İnternette bir virüs programının destek verdiği bir araştırmaya sonucu ortaya çıkan rapora göre siber saldırılara en hazırlıklı olan ülkelerden birisi olan İsrail'in gelişmiş siber saldırı yetenekleri mevcuttu. İsrail'in gizli istihbarat şirketi içerisinde oluşturduğu ve geneli emekli ajan ve askerlerden oluşan "Birim 8200" adlı bir ünite oluşturmuş ve saldırıya yönelik bir strateji benimsemişlerdir.

Siber savunma ve saldırı faaliyetlerini icra ederken kullandıkları ifade C4ISR adlı bir koddur. Bu kod Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance: Komuta, Kontrol, Muhabere, Bilgisayar, İstihbarat, Gözetleme, Keşif anlamlarına gelmektedir (Durna, ve diğerleri, 2012).

Ayrıca bu kodun yanı sıra istihbarat uydusu ve askeri haberleşme sistemleri de mevcuttur.

İsrail yönetimine göre siber saldırı veya bilişim kaynaklı gelebilecek her hangi bir saldırı füzelerle yapılmış bir saldırı kadar belki de daha tehlikeli olarak düşünülmektedir. Bu nedenle oluşturulan birimlere yeni ve yetişmiş elemanlar temin etmek için personelin eğitimine de özen göstermektedir. Eğitilen personel de ordu içerisinde kurulan siber birimlere yönlendirilmektedir.

İsrail politikası, ülkeyi siber saldırılara karşı koruyacak tüm tedbirlerin alındığını ve ülke her an siber tehditlere karşı hazır durumda olduğu şeklinde ifade etmektedir. Negev çölünde tüm dünyadaki internet ve bilgi trafiğini kontrol eden sistemleri mevcuttur. İsrail askeri birlik, istihbarat ve siber mücadeleyi bir arada tutarak ulusal güvenlik politikasını da bu yönde belirlemiştir.

Günümüzde birçok ülkenin kritik, hassas ve gizli bilgi taşıyan sistemleri internet tabanlı sistemler üzerinde muhafaza edilmektedir. Bu durum da ülkelerin siber saldırılara karşı daha savunmasız olduğunu gösterir. Fakat İsrail bu tür durumlara maruz kalmamak için kritik sistemlerini internet olmadan çalışabilen intranet sistemleri üzerinde muhafaza etmiştir. Bu durumda ise olası siber saldırılar karşısında gelebilecek tehditleri önleme ve veri kaybı, tahrifatı gibi durumlarla karşılaşmamak için başvurduğu tedbirlerden en önemlilerindendir. Çünkü dışarıdan gelebilecek tehditler için internete ihtiyaç vardır ve intranet ağı ise sadece yerel olarak çalıştığından böyle bir tehlikeyi tamamen uzaklaştırmış olmaktadır (Durna, ve diğerleri, 2012).

2.11.11. Kuzey Kore:

Kuzey Kore ilk defa 1998 yılında siber alana yönelmiştir ve o günden bu yana kendisini sürekli yenilemiştir. Birçok siber silah ve teknik kapasitesini de gittikçe artıran teknik alt yapısını da oluşturma çalışmalarına devam etmektedir. 2007 yılında geliştirmiş olduğu ilk yazılım bombasını test etmiş ve bu hareketiyle BM Güvenlik Konseyi'nin tepkisini almıştır. Bu olaydan sonra BM Güvenlik Konsey, Kuzey Kore'ye her türlü bilgisayar ve dizüstü bilgisayarı satışını yasaklamıştır. Bu karara rağmen Kuzey Kore ordusu siber silahlar geliştirme çalışmalarına hızla devam etmektedir ve şimdiye kadar sürekli geliştirdiği 121 adet birim kurmuş ve birçok siber silah üretmiştir (Türkay, 2013).

2.12. Türkiye'de Siber Alan

Türkiye de teknolojinin gelişmesiyle beraber siber suçlarla mücadele etmek için ilk defa 1997 yılında Emniyet Genel Müdürlüğü (EGM) bünyesinde "Bilişim Suçları Bürosu" kurulmuştur. 1998 yılında ise *"Bilgisayar Suçları ve Bilgi Güvenliği Kurulu"* adında bir kurul oluşturulmuştur. Bilişim konusu suçlarda bilgi güvenliği konusunda araştırma yapmak ve bu konuda yasada boşluk olup olmadığının tespiti ve tespit edilen problemlerin tez zamanda giderilmesi amacıyla oluşturulmuş bir gruptur. Oluşturulan bu büronun içeriği de genişletilerek yeni bir müdürlük oluşturuldu. Bu müdürlük "*İnternet* ve *Bilişim Suçları Şube Müdürlüğü"* adını aldı. EGM'de yer alan başkanlık ve müdürlük bünyesindeki bölümlerin görevi siber alanla alakalı gelişmelerin takibini yapmak, ülkemize gelecek olası saldırlar, sistemlere izinsiz erişim yapanlar konusunda tedbir almak, bu görevde yer alacak yeni personelleri eğitmek ve bu konuda çalışmalarını sürdüren kurum ve kuruluşlarla iletişime geçerek bilgi paylaşımında bulunmak.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ve siber güvenlikten sorumlu tüm kurum ve kuruluşun üst düzey yetkililerinin de bulunacağı Siber Güvenli Kurulu 11 Kasım 2013 tarihli resmi gazetede yayımlandı. Haziran ayı içerisinde oluşturulan çatı kuruluş niteliğinde olan Ulusal Siber Olaylara Müdahale (USOM) ve bakanlık ve kritik sektörlerde oluşturulacak Siber Olaylara Müdahale Ekibi (SOME)'de bu ulusal merkeze bağlı olarak görev yapacaktır.

Oluşturulan Siber Güvenlik Kurulunda Ulaştırma, Denizcilik ve Haberleşme Bakanı başkanlığında Dışişleri, İçişleri, Milli Savunma, Ulaştırma, Denizcilik ve Haberleşme bakanlıkları müsteşarları, Kamu Düzeni ve Güvenliği Müsteşarı, Milli İstihbarat Teşkilatı Müsteşarı, Genel Kurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Mali Suçlar Araştırma Kurulu Başkanı, Türkiye İletişim Başkanı ile Ulaştırma, Denizcilik ve Haberleşme Bakanlık ve kamu kurumlarının üst düzey yöneticilerden oluşacak. (Hürriyet, 2013).

Bilim, Sanayi ve Teknoloji Bakanı, kamu ve özel sektörde dijital verilerin güvenliğini sağlamak için "beyaz şapkalı hackerlar" yetiştireceklerini açıkladı. Türk Standartları Enstitüsü'nde (TSE) yetişecek uzmanların, eğitimlerinden sonra da sertifika alacalar ve Türkiye için çalışmalarını sürdüreceklerdir. Eğitim için TSE Yazılım Belgelendirme Müdürlüğü tarafından "Sızma Testi, Eğitim ve Danışmanlık

Hizmeti" konulu program oluşturuldu. Programda 4 farklı uzmanlık alanı belirlendi. Bunlar; stajyer, kayıtlı, sertifikalı ve kıdemlidir. Bu beyaz şapkalı hacker'ların görevi, sistem açıklarını tespit etmek ve bunları sistem yöneticisine bildirmektir. Sızma testini yapan firma ve kişiler, ülkemizde ilk kez bir kamu kurumu olarak TSE'de eğitilecek. Bu da göstermektedir ki ülkenin kamu ve özel sektörde dijital verilerinin korunmasında yetişmiş beyaz şapkalı hacker'lar yer alacaktır (Milliyet, 2013).

Bilişim suçu ilk kez 1991 yılında Türk Ceza Kanunu'nun (TCK) Bilişim Alanında Suçlar başlığı altında yer aldı. 2005 yılında yenilenen 5237 sayılı Türk Ceza Kanunu'nda (TCK) da şu başlıklar altında yer almaktadır:

"Kişilere karşı suçlar" kısmının dokuzuncu bölümünde "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlığı yer almaktadır. Hukuka aykırı olarak kişisel verileri kaydedilmesi suçu (m.135), Kişisel verileri, hukuka aykırı olarak bir başkasına verme, yayma veya ele geçirme suçu (m.136), Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmeme suçu (m.138).

"Topluma karşı suçlar" kısmının onuncu bölümünde "Bilişim Alanında Suçlar" başlığı yer almaktadır. Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girme ve sistemde kalma suçu ve bu fiil nedeniyle veriler yok etme veya değiştirme suçu (m.243/1,3), Bir bilişim sisteminin işleyişini engelleme, bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verinin transfer edilmesi suçu (m.244/1-2), kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlaması suçu (m.244/4), Banka veya kredi kartlarının kötüye kullanılması suçu (m.245). 5237 sayılı TCK'da bilişim alanında suçlar bölümünde suç tipleri ekler kısmında (Ek A.) belirtilmiştir.

2.13. Dünyada Siber Saldırılar

Siber terörü henüz çok genç olmasına rağmen dünya çapında hiçte azımsanmayacak kadar saldırı gerçekleştirmiştir. Bu saldırılara maruz kalan ülkeler ve sebep olan önemli birkaç taneden söz edilecektir:

2.13.1. İsrail-Filistin:

Lev, yaşanan gerilimi İsrail ve Filistin arasında yaşanan gerilim ve savaş ortamı sadece bombalarla silahlarla devam etmemektedir seklinde ifade etmektedir. Bunun yanı sıra siber âlemde de savaşlar devam etmektedir. 2000 yılında 3 İsrail askerinin Hizbullah tarafından kaçırılmasının ardından İsrail tarafından Hamas ve Hizbullah gruplarının internet siteleri büyük bir saldırıya uğradı ve bu saldırılarda DDoS yöntemi kullanıldı. Bu duruma cevaben Filistin'e yakınlık duyan gruplar da İsrail hükümetinin Dışişleri Bakanlığı'nın, borsanın ve Merkez Bankasının siteleri çökertmişlerdir. Bu durum da savaşın siber uzayda da devam ettiğini göstermektedir (Gürkaynak ve Eren, 2011).

2.13.2. İsrail-Anonymous

Küresel saldırgan grubu Anonymous, İsrail hükümetine ait Genel Ağ sitelerini hedef alan çok kapsamlı bir saldırı düzenledi.

Ulusal Siber Büro tarafından yapılan açıklamada, saldırganların önemli sitelerin çoğunu kapatmayı başaramadığını belirtti. İsrailli yetkililerce yapılan açıklamada, 'Şu ana kadar beklenen oldu, hasar yok gibi. Anonymous'un ülkemizin hayati altyapısına zarar verecek becerisi yok. Zaten niyetleri bu olsaydı saldırıyı düzenleyeceklerini günler öncesinden duyurmazlardı. Tek istedikleri medyanın yakından takip ettikleri konularda gürültü yaratmak' denildi. Anonymous'a yakın grupların Genel Ağ sitelerinde günler öncesinden Nisan 2013'te OpIsrael isimli bir saldırı operasyonu başlatacağı duyurulmuştu. İsrail İstatistik Bürosu'nun Genel Ağ sitesinde sabah saatlerinde ulaşılamıyordu. Ancak bunun saldırganlar tarafından olup olmadığı anlaşılamadı. Yerel medya ayrıca Savunma ve Eğitim Bakanlıklarının ve bazı bankaların da saldırıya uğradığı ancak saldırıların püskürtüldüğünü bildirdi. Ayrıca dün gece İsrail borasının ve Maliye Bakanlığı'nın Genel Ağ sitelerine de saldırılar düzenlediği yönünde haberler geldi. Ancak iki kurum da haberleri reddetti. Bazı küçük işyerlerinin de siteleri saldırıya uğradı ve ana sayfalarına İsrail karşıtı mesajlar bırakıldı. Bunun karşılığında İsrailli saldırganlar da radikal İslamcı grupların sitelerine saldırarak İsrail yanlısı mesajlar bıraktı. Geçtiğimiz yıl Ocak ayında Suudi Arabistan merkezli olduğu iddia edilen bir grup tarafından, İsrail borsası ile bir resmi havayolu firmasının Genel Ağ siteleri saldırıya uğramış ve binlerce kişinin kredi kartları bilgilerini yayınlamıştı (Hürriyet, 2013).

2.13.3. Çin-ABD:

Çin ile ABD arasındaki siber gerilime sebep olan olay Çin ve ABD savaş uçaklarının çarpışmasıdır. Bu olayın ardından bazı Çinli gruplar Amerika'ya karşı uzun sureli saldırılarda bulunmuşlardır. Saldırının Çin'den yapıldığı tespit edilmiş fakat Çin hükümeti bu saldırıyı gerçekleştirenleri cezalandırmamış. Bu saldırıları gerçekleştirenler ise Amerika'da Beyaz Saray, Enerji Bakanlığı gibi sitelerin de içerisinde bulunduğu yaklaşık 1200 siteye saldırıda bulunmuştur (Gürkaynak ve Eren, 2011).

2013 yılında ise ABD'li yetkililer aralarında ülkenin füze savunma, askeri uçak ve savaş gemilerinin de bulunduğu birçok taslağın Çinli saldırganlar tarafından çalındığını ifade etti.

Pentagon tarafından açıklanan bir belgede saldırı 'Esnek askeri sisteme gelişmiş siber tehdit' olarak ifade edildi. Çalınan tasarımlar arasında gelişmiş Patriot füze sistemleri, F/A 18 savaş uçağı, V-22 OSprey savaş uçağı ve F35 savaş jeti tasarımları yer almakta. Ulusal Güvenlik Danışmanı ise bu olayın iki ülke arasında gerginliklere neden olabileceğine dikkat çekerek ABD Başkanı'nın bu konuda oldukça endişeli olduğunu dile getirdi. Diğer yandan Avustralya da Çin'i casusluk yapmakla suçluyor. Avustralyalı yetkililer Avustralya istihbarat servisi binasının güvenlik sistemi planlarının Çinli Genel Ağ saldırganları tarafından çalındığını belirtmişti (Milliyet Gazetesi, 2013).

2.13.4. Estonya-Rusya:

Rusya tarafından 2007 yılında Estonya'ya yapılan siber saldırı önemli güncel saldırılardan bir tanesi olarak ifade edilmektedir. Rusya bu saldırılarda Estonya hükümetine yönelik saldırıları çok yoğun bir şekilde gerçekleştirmiştir ve ulusal medyaya ait siteler, hükümete ait siteler, bankalara ait siteler gibi çok önemli kurum ve kuruluşlara ait siteler siber tehdit altına girmiştir. Bu saldırıların çoğu da DDoS türünden saldırılar olmakla beraber bu saldırılar sonucunda çoğu site kullanılamaz hale gelmiş. Siber saldırıların ne kadar kolay bir şekilde ülkeleri etkileyebildiği, teknoloji ile bu kadar kolay şekilde saldırılar düzenlenebildiği ve internet sistemi ile ülkelerin saldırılara ne kadar açık oldukları da ifade edilmektedir (Gürkaynak ve Eren, 2011).

2.13.5. Rusya-Gürcistan:

2008 yılında Güney Osetya yüzünden Rusya ile Gürcistan arasında çıkan çatışma siber güvenlik konusunu yeniden gündeme getirmiştir. Ortaya çıkan sıcak çatışmalarla birlikte Rusya Gürcistan'a yoğun şekilde siber saldırıya geçti. 2007 yılında Estonya ile Rusya arasında gerçekleşen siber saldırılarla benzerlik gösteren bu saldırı da yine aynı sonuçlar ortaya çıkmıştır. Fakat Gürcistan'ın internet alt yapısı Estonya kadar gelişmiş olmadığı için beklenen etki tam anlamıyla gerçekleştirilemedi (Bıçakçı, 2013). Bu saldırılar fiziki saldırılarla birlikte siber saldırıların da gerçekleşebileceği ve asıl zararın da buradan verdirilebileceğini göstermiştir. Gürcistan'a yapılan saldırıların ülkeye en önemli etkisi kritik bir savaş zamanında iletişim ve bağlantının kesilmesidir. Bu durumda Dışişleri Bakanlığı, oluşan bu zayıflığı gidermek için Google'dan izin alarak Blogger sitesinde bir blog açmış ve haberleşmeyi buradan sağlamaya başlamıştır. Ülkenin milli bankası on gün süreyle kendisini toparlayamadı ve bu nedenle müşterilerine hizmet veremez oldu (Çalışkan, 2012).

2.13.6. Kırgızistan-Rusya:

2009 yılında Kırgızistan'da meydana gelen saldırıda ülkenin iki ana internet sağlayıcısı hedef alınmış ve yine Estonya ve Gürcistan örneklerinde olduğu gibi DDoS yöntemiyle saldırılar gerçekleştirilmiş. Bu saldırıların arkasında Rusya olduğu ifade edilse de herhangi bir kanıt, delil bulunamamış. Yapılan saldırı sonucunda iki servis sağlayıcının web siteleri çökmüş ve elektronik posta servisleri kullanılamaz hale gelmiş (Gürkaynak ve Eren, 2011).

2.13.7. Pakistan-Hindistan:

İki ülke arasında Keşmir sorunu nedeniyle ortaya çıkan sorun sadece politika şeklinde gerçek dünyada kalmamakla beraber ülke sempatizanlarının da araya girmesiyle daha da büyük bir boyut kazanmıştır. Pakistan taraftarı bazı hacker'lar özellikle olayı tüm dünyaya duyurmak için Hindistan için önemli olan bazı sitelere saldırmıştır. Bunların arasında Hindistan Parlamentosu web sitesi, Atom Araştırma Merkezi ve Hindistan Bilim Enstitüsü de yer almaktadır. Hindistan sempatizanı hacker'lar da kendilerinin haklı olduğunu göstermek için kendilerince

bir saldırı taktikleri geliştirip Pakistan'a siber saldırıda bulunmuşlardır. Bu saldırılar mevcut olan sorunun kat kat artmasına sebep olmuştur (Gürkaynak ve Eren, 2011).

2.13.8. Güney Kıbrıs Rum Yönetimi:

Başkanlık seçimlerinin yapıldığı Güney Kıbrıs Rum Yönetimi'nde, seçim kurulu başkanı, uluslar arası hacker grubu Anonymous tarafından İçişleri Bakanlığı'nın elektronik sistemine 2013 yılında şubat ayı içerisinde hafta sonu siber saldırı düzenlendiğini açıkladı. Yetkili, saldırının herhangi ciddi bir sorun yaratmadan bakanlığın güvenlik sistemleri tarafından önlendiğini söyledi.

Güney Kıbrıs Rum Yönetimi'nde yapılan başkanlık seçimiyle ilgili haberlerin ve sonuçlarının yayımlandığı akşam saatlerinde Rum İçişleri Bakanlığı'nın genel ağ sistemine erişim bir süre kesilmişti.

Rum medyasında çıkan haberde, daha önce hacker grubu Anonymous'un, Rum İçişleri Bakanlığı'nın bilgisayar sistemine saldıracağı tehdidinde bulunduğu belirtildi (Hürriyet, 2013).

2.13.9. Katar- Suriye:

Esad yanlısı Genel Ağ korsanları El Cezire'nin örün sayfasına saldırdı.

Katar merkezli televizyon kanalı El Cezire'nin örün sayfası, Esad yanlısı El Reşidun tarafından hack'lendi. Akşam saatlerinde başlatılan siber saldırıda kanalın hem Arapça hem de İngilizce yayın yapan siteleri saldırıya uğradı. Sitede bir süre El Reşidun tarafından hazırlanan görsel yer aldı. Siteye bırakılan mesajda, 'saldırının El Cezirenin Suriye halkına ve hükümetine karşı tutumu ve muhaliflere verdiği destek nedeniyle yapıldığı belirtildi.' Saldırı sonrasında El Cezire'den yapılan açıklamada ise kanalın dış hizmetlerinin zarar gördüğü ve sorunun kısa sürede çözüldüğü duyuruldu. El Reşidun, daha önce de bazı hükümet sayfaları, haber ajansları, militan gruplara ait sitelere saldırıda bulunmuştu (Habertürk, 2012).

Suriye'nin Elektronik ordusu olarak tanıtan hacker grup önce web sayfasını hack'lediği El Cezire'nin SMS servisini de hack'lendi ve SMS'lerde Katar Başbakanı'nın suikasta uğradığını yazdılar. El Cezire televizyonunda yaptığın son açıklamada SMS servisinin hacker'ların saldırısına uğradığını doğruladı (Hürriyet, 2012).

2.13.10. ABD-İran:

Uluslararası haber ajansı Reutars'ın haberine göre, ABD'nin nükleer programından dolayı kendilerine ekonomik yaptırım uygulamasına öfkelenen İranlı hacker'lar, aylardır ABD merkezli Bank of America, Citigroup ve JP Morgan Chase'e siber saldırı gerçekleştirildi. Haberde söz konusu saldırılardan ABD bankalarının ne kadar etkilendiği, zarar görüp görmediğinin ise henüz belirlenemediği belirtildi. İranlı hacker'ların söz konusu bankaların hesaplarını çalıp çalmadıklarının da henüz belirlenemediği vurgulandı. İranlı hacker'ların saldırılarının bankaların hizmet vermesini engellemek şeklinde gerçekleştirildiği belirtilen haberde bu yöntemle Bank of America, Citigroup ve JP Morgan Chase'ın örün sayfalarının kullanılamaz hale getirilmeye çalışıldığı ileri sürüldü. Reuters'ın haberinde, ABD bankalarına saldırı emrini İran recmi tarafından verildiği yoksa yurt sever İranlı hacker'lar kendi başlarına mı hareket ettiğini ise netlik kazanmadığı belirtildi (Ntvmsnbc, 2012).

2.13.11. ABD:

Bilgisayar korsanlarının son hedefi dünyanın en gözde ve kar şirketi olan Apple oldu. Bilgisayar korsanları Apple'a saldırdı. Apple tarafından korsan saldırısı doğrulanırken bu kişilerin yalnızca bazı 'Macintosh' bilgisayarlara zarar verdiği ancak şirketin herhangi bir veri tabanı bilgisini alamadıkları ifade edildi (Milliyet, 2013).

Twitter, Siber saldırıya uğradığını ve 250 bin kullanıcının bilgisinin saldırganlar tarafından ele geçirilmiş olabileceğini bildirdi. Twitter yöneticileri, site hesabından 250 bin kişinin kullanıcı isimlerini, şifrelerini ve e posta adreslerini çalınmış olma ihtimali üzerine, şifreler, iptal edilen bu kullanıcılarını durumdan haberdar edildiğini kaydetti. Sosyal paylaşım sitesi bilgi teknolojileri güvenliğinden sorumlu kişi, saldırının amatör işi olmadığını ifade etti (Cnnturk, 2013).

Microsoft'un Windows 8'de büyük önem verdiği işletim sistemleri için daha esnek bir ortam sağlayan UEFI (Unified extensible firmware Interface), hacker'ların kurbanı oldu ve UEFI'nin sağladığı güvenlik, İtalyan hacker'lar tarafından kırıldı.

ITSEC'in geliştirdiği yeni bootkit, UEFI firmware'ine müdahale ediyor ve temel güvenlik önlemlerini aşıyor. Bu hack, zararlı geliştirenlerin bilgisayara girebilmek için 'fark edilmeyen zararlılar geliştirebileceği ve böylelikle kullanıcının verilerini uzaktan çalabileceği anlamına geliyor. ITSEC, yaptığı testlerde Windows 8

‘in sürücü imzalama işlevini ve işletim sistemini çekirdeğindeki Yama Koruması işlevini nasıl devre dışı bıraktığını gösterdi. Hacker’lar UEFI için bootkit kodu geliştirmenin çok daha kolay olduğunu söylüyorlar. Zira önceden bootkit yazmak için iyi derecede Assembly dili bilmek ve BIOS un nasıl çalıştığını bilmek gerekiyordu. Şimdi ise yeni platform, hacker’lara göre herşeyi makineden soyutluyor ve UEFI bootkitlerini geliştirmesi çok daha kolay hale getiriyor. Yeni UEFI bootkitlerini Windows 8 dışındaki sistemlerle rahatlıkla hedef alabileceğini söylüyor. Hacker’lar UEFI’ın PC kullanıcıları için tek başına tam bir güvenlik sunmayacağını ve yeni alt yapıyı kırmanın kolay olduğu sonucuna varıyorlar (Chip, 2012).

2.13.12. İran:

İran’ın güneyindeki sanayi tesislerini bilgisayarlarının bir internet virüsüyle saldırı düzenlediği bildirildi. Bu olay 2010 yılından beri İran‘ı hedef alan siber savaşını son hamlesi olarak değerlendirildi.

Siber saldırılarla mücadeleden sorumlu Pasif Savunma Kurumundan yapılan açıklamada, geçtiğimiz aylarda bir virüsün Hürmüzgan eyaletinde bazı sanayi kuruluşlarını bilgisayar sistemlerine bulaşmak ancak etkisiz hale getirildiği belirtildi. Kurum tarafından, İSNA haber ajansına yaptığı açıklamada, düşmanlar kargaşa çıkarmak için internet ağları üzerinden sürekli İran’ın sanayi birimlerine saldırdığı, bu virüsün Hurmüzgan’dan ki bazı imalat sanayi tesislerini etkilediği ancak zamanında alınan önlemler ve yetenekli hacker’larını iş birliğiyle ilerlemesinin durdurulduğu ifade edildi.

İran, uranyum zenginleştirme tesislerinin 2010 yılında Stuxnet bilgisayar virüsünün hedefi olmasının ardından internet güvenliğini sıkılaştırmıştı. Tahran yönetimi daha önceki açıklamalarda Stuxnet’in ABD ve İsrail’in işi olduğunu öne sürmüş bağımsız internet güvenliği şirketlerinde bu açıklamaları teyit eden sonuçlara varmıştır. İsrailli yetkililer batının İran’ın petrol ve bankacılık sektörüne uyguladığı yaptırımları Tahran’ın nükleer programını durdurmaya ikna etme konusunda başarısız olması durumunda ülkedeki nükleer tesislere askeri operasyon düzenleme tehdidinde bulunmuştur (Hürriyet, 2012).

2.13.13. İsveç:

İsveç hükümetinin internet sitelerine korsan saldırı düzenlendi ve düzenlenen bu saldırıdan etkilenen kurumların başında Silahlı Kuvvetler ve İsveç

Enstitüsü gelmektedir. Hükümetten konuya ilişkin yapılan açıklamada olayın gerçekleştiği fakat sorunun ne zaman düzeleceği konusunda bilgi veremediklerini ve kim tarafından da yapıldığını henüz tespit edemediklerini belirtti. Saldırıların DDoS türünden olduğunu da ifade etti. Wikileaks'in kurucu ve cinsel taciz iddiasıyla suçlanan ve yargılanmak üzere İsveç'e götürülmek istenen Julian Assange ile alakalı bir durumdan dolayı da olabileceği ifade edilmektedir. Saldırıdan sonra hacker grubu Anonymous'un İsveç kolu da Twitter'da mesaj yayınlayarak hackleme olayının doğruluğunu teyit edemediklerini ifade etti. Anonymous'un siteyi hacklemediğini belirten internet uzmanı Marcin de Kaminski, bunu yapan Anonymous olsaydı bu eylemlerini ses getirecek şekilde yapardı şeklinde belirtti. Çünkü Anonymous grubu korsanları daha önce de Yunanistan ve Polonya resmi sitelerini de hacklemiş ve bunu da duyurmuştu (Hürriyet, 2011).

2.13.14. Güney Kore:

Güney Kore'de birçok site siber saldırıya uğradı. Bu saldırıların da Güney Kore-Kuzey Kore savaşının başlangıç tarihine gelmesinin de manidar olduğu ifade ediliyor.

Yapılan saldırılarda başta başkanlık sarayı Mavi Köşk, başbakanlık gibi önemli devlet o yanı sıra, tirajı çok yüksek gazetelerden olan Chosun İlbo ve yerel dilde yayın yapan gazeteler de nasibini aldı. Devletin iktidarında yer alan partinin de 8 şehirdeki parti teşkilatına ait web sitelerine erişimin sağlanamadığı belirtildi. Saldırıda bulunulan sitelere özellikle ana sayfalarına "Birleştirici Başkan Kim Jong-un çok yaşa!" ifadesi bir süre yazılı olarak kaldı. Ana sayfanın alt kısmında ise "Biz Anonymous'uz. Biz lejyonuz. Biz affetmeyiz. Biz unutmayız. Bizi bekleyin!" şeklinde yazı yer aldı.

Uluslar arası hacker gruplarından Anonymous'un Güney Koreli üyeleri de Kuzey Kore'ye yönelik saldırılarda bulunacaklarını açıkladı. Bu durum karşısında hazırlıklarına devam eden Kuzey Koreli yetkililer de bu durumu bir karşılık olarak değerlendirdiklerini belirterek devletin önemli sitelerindeki tedbirlerini artırırken, Güney Kore'nin Mavi Köşk ve başbakanlığına yapılan saldırısından kalan yazılar siteden kaldırıldığı ifade edildi (Alpago, 2013).

2.13.15. Türkiye-İsrail:

Mavi Marmara Saldırısı 2010

İsrail'in ülkeye hiçbir yardımda bulunulmasını istemediği ve ağır bombardımana tuttuğu Gazze'ye yardım götürmek isteyen farklı din ve milletten gönüllüler, insani yardım taşıyan Mavi Marmara adlı gemi ile Gazze'ye doğru ilerlerken uluslararası sularda 31 Mayıs 2010 tarihinde İsrail askerlerinin baskınına uğramışlardır. Silahlı saldırı olayına kadar gemideki personelle iletişim kurulabiliyor olmasına rağmen saldırı öncesinde gemideki personelin iletişimi sağlayan ve dünya medyasına yayın yapan uydu frekansı ve uydu telefonlarının iletişimi kesilmiştir. Saldırı sonucunda 9 gönüllü yardımsever İsrail askerlerinin silahlı saldırısı sonucunda hayatını kaybetmiştir. Bu olay hem Türkiye'de hem de dünyada geniş yankı bulmuştur. Bu durum karşısında tepkisini göstermek isteyen bazı hacktivist gruplar çok sayıda devlet, özel şirket ve bankanın sitelerine saldırıda bulunmuş ve birçok siteyi çökertmiştir. İsrail uluslararası sularda gerçekleşen bu durumdan dolayı özür dilememekte ısrar ettikçe tepkiler yine İsrail'e ait kamu kurum ve kuruluşlarının sitelerine saldırı olarak defalarca yansımıştır (Kara, 2013).

2.14. Türkiye'de Siber Saldırılar

İnternetin sadece iyi niyetli kişilerce kullanılmadığı da bilinen bir gerçektir. Ülkemiz aleyhinde de kötü niyetli kişilerin oluşturmuş olduğu 8000 civarında olduğu düşünülen zararlı internet siteleri mevcuttur. Bunların birçoğu da com, org ya da net uzantılı sitelerdir. Zararlı bu siteler genelde Avrupa ve Amerika üzerinden yayınlarını sürdürmektedir. Bu sitelerin bazıları www.pkk.org, www.ibda-c.org, www.ozgurpolitika.org, www.kurd.gr, www.partizan.org, www.atilim.org, www.evrensel.net, www.hilafet.org, www.tkp-ml.org, www.mlkp.net, www.kurtulus.com, www.hizb-ut-tahrir.org. Bu siteleri her gün yüzlerce kişi ziyaret etmektedir. Siteler genelde yoğun propaganda ve eğitim faaliyetleri için kullanılmaktadır. Bu sitelerin haricinde dünyada da terör adına faaliyet gösteren ve internet ortamını bu amaçla kullanan çok sayıda site mevuttur. Bu siteler uluslararası alanda da faaliyet göstermektedir (Atıcı ve Gümüş, 2003).

2.14.1. Örnek Olay 1:

"…….Bir kamu kurumunda lojmanlarda oturmakta olan bölge müdürü M. özellikle çocuğu tarafından kullanılmakta olan bilgisayar için evine bağlattığı kablosuz modem aracılığıyla internete bağlanır.

Bölge müdürü M., gerek bilgi eksikliği, gerekse de lojmanda oturması ve kendisine ait lojman ile diğer lojmanlar arasında mesafe bulunması, kablosuz modemin sinyal gücünün kendi lojmanında bile birçok yerden sinyal gücünün zayıf olmasından dolayı bağlantı kurulamaması, gibi nedenlerle kablosuz modemi şifrelemez.

Aynı lojmanlarda çalışan diğer bir personel P. ise eşi ile olan sorunların da etkisi ile internette anlık mesajlaşma uygulamaları ve chat odalarında çokça vakit geçirir. Genel olarak kendisine ait internet üzerinden kendi lojmanında gece geç saatlere kadar sohbet eder.

Personel P. bir gün gece lojmanlar içerisindeki idari büroda görevlidir. İdari büro, müdür M.'nin lojmanı ile aynı binadadır. Görev yerine kendisine ait dizüstü bilgisayarı götürür. Personel P. o gece, kendisine ait bilgisayar ile birçok gece evinde olduğu gibi anlık mesajlaşma uygulamaları ile ve chat odalarında vakit geçirir.

Bir kaç gecedir, yarım yamalak İngilizcesi ile konuşmaya çalıştığı İngiltere'deki K. ile o gece de ısrarla sohbet etmek ister. Çünkü K.'nin anlık mesajlaşma uygulamasındaki takma adı "bana dokunmadan edemezsin ki..." şeklindedir. Aslında bir şarkının sözü olan bu sözleri Personel P. iyi olmayan İngilizcesi ile daha çok erkeklere yöneltilmiş bir davet şeklinde algılar. Israrcı davranır. Hatta Personel P. karşısında yazıştığı K.'ye yarı çıplak kadın fotoğrafları gönderir. İlk resmi alan ve fotoğrafı gören K. 18 yaşından küçük olduğu ve internetten gelen bu şekildeki tacizler konusunda nasıl davranması konusunda ailesi ve/veya okulu tarafından bilinçlendirilmiş olduğundan derhal annesine A.'ya haber verir. Annesi A. İngiltere'deki küçük K.'nın yerine bilgisayarın başına geçer, İngiliz emniyetini arar, onların yönlendirmesi ile Personel P. ile sohbet etmeye başlar. İngiliz emniyeti anlık mesajlaşma uygulamasının servis sağlayıcı M. Firması ile irtibata geçer ve hem o anki hem de önceki tüm görüşmelere ait IP kayıtları ve içeriği alır.

Yapılan tespitler sonucunda Türkiye'den IP'lerle karşılaştırılması üzerine Interpol aracılığı ile "acil ve çocuk pornografisi" içerikli mesaj Türk emniyetine Interpol aracılığıyla gelir. Derhal Türkiye'de tespitler yapılır. IP numaraları, tarih ve saat bilgileri üzerinden İngiltere'deki küçük K. ile mesajlaşan kişilerin bulunduğu il tespit edilir ve ilgili il emniyet müdürlüğüne yazı yazılarak, "acil ve çocuk pornografisi" uyarısı ile soruşturmanın hızla tamamlanması ve ilgililer hakkında işlem yapılması istenir. İlgili il emniyet müdürlüğü, derhal mesajı işleme koyar. Kişileri tespit eder.

Sonuç şaşırtıcıdır. Gelen bilgiler bir kamu kurumu lojmanındaki iki ayrı aboneyi işaret etmektedir. İşin daha da ilginç yanı, bir abone kamu kurumunun bölge müdürüdür. İlde sayılan ve sevilen bir insandır. Durum derhal savcılığa aktarılır. Gerekli soruşturma yapılır, ilgililerin ifadesi alınır. İlgili kamu kurumuna haber verilir. Bölge müdürü, gelen evrakı alır almaz hem böyle bir olayda adının geçmesinin üzüntüsü hem de olay ile kendisi veya ailesi arasında bağlantı kuramaması nedeniyle ciddi şekilde şok geçirir.

İşinin ciddiyeti ve her zamanki dürüstlüğü ile derhal evrakı Ankara'ya gönderir. Ankara'dan genel müdürlükten müfettişler gelir. Soruşturma başlar. Müfettişler Personel P.'nin ve Müdür M.'nin ifadelerini alır. Hatta aile bireylerinin dahi ifadeleri alınır. Müdürün evindeki çocuğunun kullandığı bilgisayar da dâhil olmak üzere tüm bilgisayarlara ve diğer depolama birimlerine el konulur. Ankara'ya incelenmek üzere götürülür. Personel P. Suçunu itiraf eder. Kendisinin İngiltere'deki Küçük K. ile görüştüğünü, söz konusu yarı çıplak kadın fotoğraflarını kendisinin gönderdiğini, bağlantıları ve görüşmeleri kural olarak kendi evinde yaptığını, ancak lojmanlardaki idari büroda görevli olduğu bir gece müdürün kablosuz modeminden bağlantı yaptığını, her şeyi tüm ayrıntıları ile anlatır.

> Müfettişler düzenledikleri raporda, fiili işleyen kişinin Personel P. olduğunun anlaşıldığı, ifadeler, teknik inceleme raporu ve diğer deliller ile ortaya koyar, başka nedenlerle Müdür M.'ye disiplin cezası verilmesini ve dosyanın ilgili ilin Cumhuriyet Başsavcılığı'na gönderilmesini önerirler.
>
> Tüm bunlar başına gelen Müdür M. önce müdürlükten alınır. Bunun üzerine başka bir kamu kurumuna geçer ve tayinini de başka ile ister. Artık müdür M. uzman olarak başka bir kurumda çalışmaktadır.
>
> Yapılan yargılama sonucunda uzun uğraşlar vererek müdür M. suçsuz olduğunu anlatır. Sonunda beraat eder, ancak çalıştığı kurumdan, sevdiği ve görev yaptığı ilden, ayrılmak zorunda kalmak ve bir ceza davasında iki yıla yakın süre ile sanık olarak yargılanmak gibi bir olayı kablosuz modemini şifrelemediği için yaşar……." (Köksal ve İlbaş, 2013:13-15).

2.14.2. Örnek Olay 2:

1998 yılında bir grup terörist DHKP/C örgütüne yönelik operasyon sonucunda yakalanmıştır. Yakalanan teröristler ifadelerinde, eğitimlerini komşu bir ülkede aldıklarını, örgüt evinde kaldıklarını, kamp eğitimi aldıklarını ve buradaki eğitimlerinin hem askeri hem de siyasi olduğunu, görüşmelerinde uydu telefonunu kullandıklarını ve şifreli konuşma, görüşme konusunda da eğitim aldıklarını, üst düzey yöneticilerle aralarında mesaj alışverişini internet aracılığıyla yaptıklarını ve kullandıkları teçhizatın şarj işlemlerini de solar (güneş ışığından enerji üreten) sistemle yaptıklarını ifade etmişlerdir (Atıcı ve Gümüş, 2003).

2.14.3. Örnek Olay 3:

> "…….Takma isim kullanan bir kişi bir diğer şahısla sanal ortamda sohbet kurar. Bu sohbet esnasında Serkan rumuzlu kişi, diğer kişiye kredi kartı borçları olduğunu ve kendisine Tatvan'dan bir akrabasının 30.000 TL parayı A hesabına havale edeceğini, bu havaleyi kendi adına çıkarması halinde bankaların borçlarına istinaden paraya el koyabileceklerini söyler. Serkan bu sebeple para transferi için diğer kişiye ait olan banka hesabını kullanmak istediğini söyler. Davalı kişi bu talebi kabul eder. Olayda banka müşterisinin şifresi profesyonel bir dolandırıcılık çetesi tarafından ele geçirilip kişinin hesabı boşaltılır. Dava sonucunda, güvenlik tedbirlerindeki eksikliklerinden dolayı bankanın objektif özen yükümlülüğünü yerine getirmeyip kusurlu olduğu, müşterinin bilgisi ve onayı dışında havale yoluyla aktarılan ve hesaba geri döndürülemeyen 30.001 TL'nin faiziyle birlikte davalı banka tarafından davacı müşteriye iade edilmesi gerektiği kanaatine varılmıştır……." (Köksal ve İlbaş, 2013:23).

2.14.4. Örnek Olay 4:

Aynı şehirden iki kız öğrenci İzmir'de iki farklı üniversiteyi kazanırlar. Buna rağmen aynı evde kalmaya başlarlar. Merve'nin bilgisayarı vardır ve Nuran'ın da bilgisayarı yoktur. Bir süre sonra anlaşamaz ve evlerini de ayırırlar.

Bir gün polis Merve'nin kapısını çalar ve onu alıp karakola ifadesini almak için götürür. Sebep ise Nuran'ın babasına Nuran'ın MSN hesabından özel hayat bilgilerini içeren mailin gönderilmesidir. Fakat Merve buna bir anlam veremez. Önce aynı evde kalırken aynı bilgisayarı kullandıkları doğrudur hatta Nuran'ın MSN hesabı da bilgisayarda otomatik olarak açılmaktadır ve Merve bunu hemen kapatır ayrıca ne babasına ne de başka kimseye Nuran hakkında bir mail göndermediğini ifade eder.

Emniyet bu konuda araştırmalarını sürdürürken Merve'nin bilgisayarına el koyar ve incelemelere başlar. İncelemeler sonrasında Nuran'ın MSN hesabına Merve'nin bilgisayarından defalarca girildiğini tespit eder fakat gönderilen mailin ise bir internet kafeden gönderildiğini tespit eder. Bundan dolayı Merve çok rahatlar çünkü kendisi de böyle bir şey yapmadığını bilmektedir.

Lakin olaylar bundan sonra farklı bir hal alır çünkü Merve ve Nuran'ın birlikte aynı evde kaldıkları dönemlerden Mart 2008 'dir. Suçun işlendiği tarih ise Mart 2009'dur. Bu yıl farkı bir şekilde gözden kaçar ve Merve sanki aynı evde yaşadıkları dönem Nuran'ın hesabına girmiş gibi bir rapor düzenlenir. Bu durum üzerine Merve aleyhine savcılık YTCK 243. Maddeden dolayı dava açar. Merve'ye tebligat gönderilir. Fakat Merve'nin adresi değiştiği için tebligat eline ulaşmaz dolayısıyla da mahkemeye çıkmaz. Bu durum hakkında gıyabi tutuklama kararı çıkartılmasına sebep olur. Merve yaz tatilini geçirmek için ailesiyle gittiği otelde gözaltına alınır. İfadesi alınıp serbest bırakılır.

Hukuk fakültesinde okuyan Merve bu duruma hiçbir anlam veremez ve muhtemelen hiçbir alakasının olmadığı bir olayda sanık sıfatıyla yargılanmak çok ağrına gider. Hâlbuki kendisi de okulunu bitirip hâkim olmak istiyordu. Ortada anlaşılmayan bir durum var o da olayın çok basit olmasıdır. Tek sorun kendi şahsi bilgisayarını ve internetini bir başkasıyla paylaşmıştır. Bu nedenden dolayı bu duruma düşmüştür (Köksal ve İlbaş, 2013).

2.14.5. Örnek Olay 5:

> ".....Mersin Asayiş Şube Müdürlüğü Dolandırıcılık ve Yan Kesicilik Büro Amirliği tarafından 2008 yılında tamamlanan operasyonda, suç şebekesi içinde teknik bilgi sahibi bilgisayar uzmanlarının ve TEDAŞ görevlilerinin de olduğu bir grup suçüstü yakalanmıştır. Bu operasyonda dikkati çeken nokta davanın devam etmesinden kaynaklı burada ismi zikredilmeyecek olan büyük iş merkezlerinin elektrik sayaçlarını bu şebeke vasıtası ile sıfırlaması veya olması gerekenden daha aşağıya çektirmesidir.

> Dolandırıcılık bürosu tarafından ele geçirilen dizüstü bilgisayarda, şebeke elemanları tarafından oluşturulmuş bilgisayar yazılımı ile elektronik sayaçların sayısal veri ve değerlerinin değiştirildiği anlaşılmıştır. Sıradan vatandaşların da bu suç şebekesinin faaliyetlerinden faydalandığını belirtmekte yarar vardır. Şebeke yaptığı bu işlemler sayesinde yüklü miktarda para kazanmıştır ve bu hırsızlığın devlete olan maliyeti net olarak hesaplanabilmiş değildir……." (Akdağ, 2009:61).

2.14.6. Örnek Olay 6:

Bir özel sektör firmasında daha önce çalışmış bir kişi tarafından firmanın internet sitesine e-mail aracılığıyla virüs göndermiştir. Bu şekilde firmanın internet sitesine ve bilgisayar sistemine zarar vermiştir.

Gerçekleşen bu olayın ardından virüs bulaşmış bilgisayar incelenmiş ve bu inceleme sonucunda e-mail'in geldiği bilgisayarın IP adresi, mail'i gönderen sunucu server'in IP numarası, mail'i gönderen ve mail'i alan adresler tespit edilmiştir. Bu şekilde virüs ve gelen mail aracılığıyla başlattığı çalışma sayesinde mesajı gönderen kişiye ulaşılmıştır. Ayrıca bu kişi hakkında yasal süreçler başlatılmıştır (Köksal ve İlbaş, 2013).

2.14.7. Örnek Olay 7:

Sinop'ta yapılması planlanan nükleer santral ile alınacak karar dolayısıyla Sinop halkının da talebi ile dünyaca ünlü hacker grubu RedHack Sinop Valiliğinin sitesine saldırı düzenledi.

Saldırı sonrası site ele geçirildi ve bir süre sitede RedHack'in marşı ile birlikte bir de RedHack'in açıklaması yer aldı. Birkaç saat sonra sitenin saldırılan sayfası yayından kaldırıldı. Bu saldırıları Twitter üzerinden de ilan etmiştir. Daha önce de içlerinde Türk Hava Yollarının da bulunduğu birçok kamu kurum ve kuruluşuna saldırıda bulunmuş siteleri engellemiş, erişime kapatmış ve tüm dikkatleri kendi üzerine çekmiştir (Hürriyet, 2012).

2.14.8. Örnek Olay 8:

> "…….İzmir merkezli 11 ilde düzenlenen operasyonda, gönderdikleri virüslü mail ve mesajlarla kişisel bilgilerini elde ettikleri kişilerin bankalardaki hesaplarından para çeken şebeke çökertildi. 6 ayda 2 milyon TL'lik çaldıkları belirlenen çetenin 18 üyesi gözaltına alındı. Bankalardaki hesaplarından bilgileri olmadan para çekildiğini söyleyen kişilerin şikâyeti üzerine İzmir Emniyet Müdürlüğü Siber Suçlarla Mücadele Şube

> Müdürlüğü ekipleri çalışma başlattı. Ekiplerin araştırmalarında, para çekilen banka şubelerinin güvenlik kamerası kayıtlarından şebeke elemanlarının kimlikleri belirlendi. Bu kişilere yönelik 11 ilde yapılan eş zamanlı baskınlarda, aralarında şebeke liderinin de bulunduğu 18 kişi gözaltına alındı. Operasyon kapsamında 38 kişi hakkında da ayrıca yasal işlem yapıldığı açıklandı.
>
> Polisin araştırmalarından ve gözaltındakilerin verdiği bilgilerden şebekenin faaliyetleri de deşifre edildi. Şüphelilerin ilk olarak Rusya'da bulunan İzmirli saldırgan aracılığı ile işadamlarının arasından seçtikleri mağdurlara virüslü mail ve mesaj gönderdikleri belirlendi. Virüslü mailler sayesinde interaktif bilgileri elde eden şebekenin, mesajla da cep telefonundan bankaların güvenlik amaçlı gönderdiği şifrenin istedikleri telefona gelmesini sağladıkları tespit edildi. Saldırganlardan gelen bu bilgileri alan şebekenin daha sonra belli bir işi bulunmayan kişiler adına bankalarda hesap açtıkları ve mağdurların hesaplarındaki paraları da bu kişilerin hesaplarına aktardıkları saptandı. Şüphelilerin hesaplarını kullandıkları kişilere yüzde 20, kendilerine yüzde 40, Rusya'daki saldırganlara ise yine yüzde 40 pay verdikleri ortaya çıktı.
>
> Şüphelilere yönelik teknik takip sırasında aynı yöntemle, bir inşaat şirketi hesabından 276 bin 856 TL'nin aktarılmasının son anda polis tarafından engellendiği öğrenildi. Şüphelilere yönelik takip sırasında geçmiş tarihlerde ise 6 şebeke elemanının, banka şubelerinden para çektikleri sırada yakalandığı ve bu kişilerden de dördünün tutuklandığı öğrenildi. Saldırganın yakalanması için de Interpol aracılığı ile çalışma yapan polis, hiçbir bankanın maille müşterilerinin kişisel bilgilerini istemediğini, bu nedenle de vatandaşların kendilerinden istenen bu bilgileri vermemeleri gerektiğini dile getirdi. Gözaltındakilerin sorgularının devam ettiği bildirildi……." (Milliyet, 2013).

2.14.9. Örnek Olay 9:

Sanık, bir şahsa virüs içeren bir e-posta gönderdi ve bu sayede tüm şifrelerini ele geçirdi. Ele geçirdiği bu şifreleri kullanarak banka hesabındaki parayı oluşturulan bir hesaba aktardı ve sahte kimlikle bu parayı çekmiştir.

Davacı, sisteme virüs bulaştırarak şifrelerini ele geçirdiği ve banka hesabını boşalttığı sanık hakkında davacı oldu. Sanık hem sahte kimlikle para çekmiştir hem de bilgisayar sistemini bozarak haksız bir çıkar sağlamıştır. Sanık, YTCK'da yer alan "Bir bilişim sisteminin işleyişini engelleme, bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verinin transfer edilmesi (m.244/1-2), kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlaması (m.244/4)" gibi suçlardan dolayı yargılanır.

Sonuçlanan davaya göre, sanık bilgisayar sistemlerini aracı etmek şartıyla dolandırıcılık suçundan dolayı yargılanmış ve cezalandırılmıştır (Köksal ve İlbaş, 2013).

2.14.10. Örnek Olay 10:

Davanın konusu, YTCK'da yer alan "Bir bilişim sisteminin işleyişini engelleme, bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri

yerleştirme, var olan verinin transfer edilmesi (m.244/1-2), kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlaması (m.244/4)" suçları ayrıca da "Bir resmî belgeyi sahte olarak düzenleme, gerçek bir resmî belgeyi başkalarını aldatacak şekilde değiştirme veya sahte resmî belgeyi kullanma (m.204) suçları kapsamına girmektedir.

Olay: Üniversitede görev yapan bir kişi yine aynı üniversitede okuyan biyoloji bölümünde 2. Sınıf öğrencisi olan bir kişinin de bilgisi dâhilinde belki bir çıkar amaçlı, başarısız olduğu notların değiştirilmesi ve bu sayede o derslerden başarılı olmasını sağlamıştır.

İnternet üzerinden bilişim sitemine girilip resmi bir belgede sahtecilik suçu işlenmiştir ve bu şekilde oluşturulan bir kamu davası sonrasında, davalı sanık hakkında Türk Ceza Kanununun 204. Maddesi gereğince evrakta sahtecilik suçundan dolayı yasal işlem başlatılmıştır ve sanık bu çerçevede cezalandırılmıştır (Köksal ve İlbaş, 2013).

2.14.11. Örnek Olay 11:

> ".…….Ulaştırma Bakanı Binali Yıldırım'ın açıkladığı son 2-3 hafta içinde Türkiye'ye yönelik yoğun siber saldırıların en önemli hedeflerinden birinin de Çankaya Köşkü olduğu ortaya çıktı.
>
> Cumhurbaşkanlığı, 3-5 Haziran tarihlerinde 72 saat süren aralıksız siber saldırıya uğradı. TÜBİTAK, Telekom ve ODTÜ'lü uzmanlardan da yardım alarak saldırı önlendi. İncelemeler sonucunda saldırıların yüzde 70'inin yurtdışından olduğunu saptandı.
>
> Köşk kaynaklarından alınan bilgiye göre, Cumhurbaşkanlığı, 3-5 Haziran tarihlerinde 72 saat süren aralıksız siber saldırıya uğradı. Saldırılar üzerine alarma geçen Köşk'ün Bilişim Teknolojileri Başkanlığı, oluşturduğu özel bir ekiple, TÜBİTAK, Telekom ve ODTÜ'lü uzmanlardan da yardım alarak Cumhurbaşkanlığı'nın resmi internet sitesini çökertmeyi hedefleyen saldırıya karşı koydu.
>
> Interpol De Devrede
>
> Saldırıların arkasında ünlü "hacker" grupları Anonymous ve Rechack'ın olduğu saptanırken, geliştirilen özel bir program aracılığıyla "hacker" saldırıları yanıltılıp farklı nokta ve adreslere yönlendirildi. Köşk'ün bu savunmasını aşamayan "hacker" grupları da bir süre sonra saldırılarına son verdi. Hürriyet'in haberine göre, Köşk'ün bilişim uzmanları, incelemeleri sonucunda saldırıların yüzde 70'inin yurtdışından olduğunu saptadı. Yurtdışından yapılan saldırılara ilişkin saptanan bilgisayarların IP numaraları Interpol'e bildirilirken, Türkiye'den yapılan saldırılar için de savcılıklara suç duyurusunda bulunuldu.
>
> Aynı Anda 10 Milyon Tık
>
> Köşk kaynakları, Cumhurbaşkanlığı'nın resmi internet sitesinin günde ortalama 500 bin-1 milyon arasında tıklandığı, ancak bu son saldırılar sırasında siteyi tıklayanların

> sayısının bir anda 10 milyonu aştığı bilgisini verdi. Hackerların bu yolla siteyi yavaşlatıp işlevsiz hale getirmeyi amaçladığı belirtilirken, yapılan incelemede, korsanlarının kullandıkları çeşitli yazılımlarla başka bilgisayarları kontrol altına alıp saldırılarını da bu bilgisayarlar üzerinden gerçekleştirdiği saptandı. Uzmanlar, "Bilgisayar oyunları ve mesajlar gibi çeşitli yöntemlerle sızılan bilgisayarlar daha sonra bu amaçla kullanılıyor. Bilgisayarı kullanılanların ise bundan haberi bile olmuyor" bilgisini verdiler……." (Yılmaz T. , 2013).

2.15. Dünya'da Yapılan Ortak Tatbikatlar

NATO Cyber Coalition 2011 Tatbikatı:

NATO Siber Savunma Yönetim Kurulunun SHAPE karargâhından yürütülen CC2011 tatbikatına aralarında Türkiye'nin de olduğu 21 ülke oyuncu olarak katılmıştır. 7 ülke de gözlemci sıfatıyla katılmıştır. Tatbikat 13-15 Aralık 2011 tarihlerinde Brüksel'in Mons şehrinde düzenlenmiştir (NATO CC11 Exercise Handbook'dan aktaran Akyazı, 2012).

> "…….Tatbikat, bilgisayar olaylarına müdahale konusunda karar verme süreçlerinin denenmesi, senaryoya dayalı olarak verilen ara durumlar aracılığıyla katılımcı ülkelerin siber savunma teknik ve idari yeteneklerinin test edilmesi, NATO ve üye ülkeler arasında siber savunma alanında işbirliği imkânlarının geliştirilmesi amacıyla, 2008 yılından beri her yıl gerçekleştirilmektedir……." (NATO CC11 Exercise Handbook'dan aktaran Akyazı, 2012).

Gerçekleştirilen en son tatbikatı Almanya'da kendi planlamış oldukları ulusal tatbikatla birlikte eş zamanlı olarak yerine getirmiştir. Tatbikatta gerçek bir saldırı gerçekleşmemiş sadece bilgisayar ortamında oluşturulan fake format üzerinde senaryo oluşturularak gerçekleştirilmiştir (NATO CC11 Exercise Handbook'dan aktaran Akyazı, 2012).

Gerçekleştirilen sanal saldırılardan denenen ara durumlar;

a) Kurumun resmi web sitesinin içeriğinin yetkisiz kişilerce değiştirilmesi,
b) Kuruma ait bir IP adresinden başka bir kurum/kuruluşa DDoS saldırısı yapıldığının tespit edilmesi,
c) Kuruma ait bir IP adresinden başka bir kurum/kuruluşa spam mesajlar gönderildiğinin tespit edilmesi,
d) Kuruma başka kaynaktan DDoS saldırısı yapılması
e) Kurumdan ayrılan kötü niyetli bir personelin ayrılmadan önce veri tabanına zarar vermesi,
f) Kuruma ait sistemlere internet üzerinden yayılan bir solucan bulaşması,
g) Telefon yoluyla kurumda çalışan personelden bilgi çalma,
h) Elektronik posta yoluyla kurumda çalışan personelden bilgi çalma,
i) Kurum çalışanlarından biri tarafından 5651 sayılı kanun kapsamında erişimi engellenen bir siteye giriş yapıldığının tesit edilmesi,
j) Kuruma aitmiş gibi görünen sahte bir web sitesinden "spam" mesajlar gönderildiğinin tespit edilmesi,
k) İzinsiz yapılan bir kazı neticesinde kurumun internet bağlantısını sağlayan fiber hattın koparılması,
l) Sistem odasında bulunan soğutma sisteminin mesai saati dışında bir saatte arızalanması,

m) Kurumun bulunduğu bölgede elektrik kesintisi yaşanmasına rağmen jeneratör sisteminin devreye girmemesi,
n) Kurum içinde ismi kolaylıkla tahmin edilerek bağlanabilen bir kablosuz ağ erişim noktasının tespit edilmesi (Akyazı, 2012:62-64).

Dünya'da Gerçekleşmiş Uluslararası Etkinlikler

- Dünya Bilgi Toplumu Zirvesi 2011 (16-20 Mayıs 2011)
- NATO Sivil Olağanüstü Hal Planlama Komitesi'nin Genel Kurul Toplantısı (1-3 Ekim 2012)
- Avrupa ve Bağımsız Devletler Topluluğu için Siber Güvenlik Konulu Bölgesel Forum (23-25 Ekim 2012)
- 7. İnternet Yönetişim Forumu (6-9 Kasım 2012)
- Dünya Telekomünikasyon Standardizasyon Genel Kurulu 2012 (20-29 Kasım 2012) (Olcay, 2013)
- NATO Siber Savunma Tatbikatı 2013 (25-29 Kasım 2013, Estonya) (BTK, 2013)
- Kilitli Kalkan (Locked Shield) Tatbikatı – 2014 (20-23 Mayıs 2014)

2.16. Türkiye'de Yapılan Tatbikatlar

Türkiye'de siber saldırılara karşı zaman zaman tatbikatlar yapılmaktadır. Yapılan tatbikatlar sırasıyla; I. Ulusal Siber Güvenlik Tatbikatı, Siber Kalkan Tatbikatı, II. Ulusal Siber Güvenlik Tatbikatı, Uluslararası Siber Kalkan Tatbikatı 2014, Kilitli Kalkan (Locked Shield) Tatbikatı' dır.

2.16.1. I. Ulusal Siber Güvenlik Tatbikatı

Ülkemizde 25-28 Ocak 2011 tarihlerinde *I. Ulusal Siber Güvenlik Tatbikatı* gerçekleştirilmiştir. Bu tatbikata finans, bilgi teknolojileri ve iletişim, eğitim, savunma, sağlık sektörlerinin; adli birimlerin, kolluk kuvvetlerinin ve çeşitli bakanlıkların ilgili birimlerinin temsilcilerinden oluşan 41 kamu kurumunun, özel sektör kuruluşunun ve sivil toplum kuruluşundan personeller katılmıştır (TÜBİTAK, 2013).

2.16.2. Siber Kalkan Tatbikatı

Elektronik haberleşme sektöründe faaliyet gösteren 12 işletmecinin katılımı ile 23-28 Mayıs 2012 tarihinde "*Siber Kalkan Tatbikatı 2012*" gerçekleştirilmiştir (TÜBİTAK, 2013).

2.16.3. II. Ulusal Siber Güvenlik Tatbikatı

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı koordine ettiği, TÜBİTAK ve BTK tarafından yürütülen 2. Ulusal Siber Güvenlik Tatbikatı, 61 kurum ve kuruluşun katılımıyla gerçekleştirildi.

Siber saldırılara karşı önlem alınması, kurumların bilgi ve iletişim sistemlerinin güçlendirilmesi, kurumlar arası koordinasyonun artırılması amacıyla düzenlenen Ulusal Siber Güvenlik Tatbikatı ikinci kez yapıldı. 61 kurum ve kuruluşun katılımıyla 25 Aralık'ta başlayan tatbikat, 8 aşamadan oluştu. İlk 6 aşamada kurum ve kuruluşlara gerçek siber saldırılar düzenlendi. Her kurum kendi sistemini savunurken, olası açıklar tespit edilmeye çalışıldı. Tatbikatın son 2 aşaması ise, tüm kurum ve kuruluşların katılımıyla Ankara'da yapıldı. Bu aşamada gerçek saldırılarla denenme imkânı olmayan saldırılar yazılı senaryolarla test edildi.

Tatbikatın son aşaması için TOBB ETÜ Konferans Salonu'nda düzenlenen etkinliğe Ulaştırma, Denizcilik ve Haberleşme Bakanı Binali Yıldırım, Bilim, Sanayi ve Teknoloji Bakanı Nihat Ergün, TÜBİTAK Başkanı Prof. Dr. Yücel Altunbaşak, BTK Başkanı Dr. Tayfun Acarer, ITU-IMPACT Başkanı Mohd Noor Amin, davetliler, tatbikatta yer alan 61 kurum ve kuruluştan bilgi güvenliği uzmanı, hukukçu ve iletişim uzmanlarından oluşan temsilciler katıldı (TÜBİTAK, 2013).

Ulaştırma, Denizcilik ve Haberleşme Eski Bakanı Binali Yıldırım Ulusal Siber Güvenlik Tatbikatının son aşaması için TOBB ETÜ Konferans Salonu'nda düzenlenen etkinlikte siber saldırı ve siber tehlikenin her ülkede farklı algılandığını ve bu ülkeler arasında da çok büyük bir farklılık olduğunu ifade etti. Kimi ülkelerin henüz iletişim noktasında sağlam alt yapılarının olmadığını belirtirken, diğer yandan da bazı ülkelerin siber tehdit konusunda ciddi bir şekilde çalıştıklarını özellikle vurguladı. Fakat siber güvenliğin her ülkenin vazgeçilmezi olduğunu da sözlerine ekleyen Yıldırım, siber güvenlik sisteminde sadece bir ülkenin tedbir alması ile veya bu anlamda sistemi bir noktaya eriştirmesi ile sorunların çözülmeyeceğini ifade etti. Küresel ağın da son derece güvenilir olması gerektiğini belirtti ve ağa bağlı tüm

sistemlerin her türlü tehditle karşı karşıya kaldığını bunun da küresel bir tehdit oluşturacağını kaydetti.

Artık yapılan savaşlarda top tüfek yerine siber teknolojinin kullanıldığı ve ülkemizi askeri alanda NATO içerisinde siber tehdit riskini gören ülkeler arasında ilklerden olduğunu da belirti. Çünkü siber saldırı sadece askeri yönden değil sivil saldırganlar tarafından da yapılmaktadır. Siber güvenlik konusunun ülkenin güvenliği için çok önemli bir adım olduğunu belirtti. Ayrıca siber saldırı için çok az bir maliyet gerekirken, yapılan saldırılara karşı savunmak için harcanan paraların çok olduğunu söyledi. Siber tehditlere karşı gelmenin onlarla mücadele etmenin terörle mücadeleden da bir farkının olmadığını ifade etti.

2. Ulusal Siber Güvenlik Tatbikatına katılımın I. Ulusal Siber Güvenlik Tatbikatına katılımdan daha fazla olduğunu ve bu artan rakamları da bu durumdan sıkıntı yaşayan kurum ve kuruluşların olmasına bağlıyor.

Bilim, Sanayi ve Teknoloji Bakanı Nihat Ergün ise ülkemizin siber altyapı kurum çalışmalarını hızla sürdürdüğünü belirtti. Tekrarlanacak olan tatbikat programlarına herkesin katılması gerektiğini vurgulayan Ergün, her an siber bir saldırıya maruz kalabileceğimizi belirtti. Türkiye'nin güçlenmesini istemeyen ve Türkiye'nin zarar görmesini isteyen çok sayıda düşmanı olduğunu ve bunun da kişisel ve grupça yapılan saldırılardan da anlayabildiklerini belirtti. Saldırıların ülkemize her an olduğunu ve bu tatbikatların olası saldırılarda nasıl tedbirler alacağımızı görmesi açısından son derece önemlidir şeklinde ifade etti. Tatbikatlarda eksikliklerimizi görüp daha hızlı yol da alınabileceğini belirtti. Tatbikatlara katılımın artırılmasını ve herkesin bu tatbikatlara katılması gerektiğini söylerken de 'Bir musibet, bin nasihatten evladır' atasözü de eklemeyi unutmadı.

Ülkemizin genç bir nüfusa sahip olmasını bir avantaj olarak gören Engin, gençlerimizin çeşitli kurumlarda güvenlik görevlisi olarak görev yapmak istediklerini belirtip onlara siber güvenlikçi olmayı tavsiye ettiğini ifade etti. Ülkemizin özel güvenlikten ziyade siber güvenlikçiye ihtiyacı olduğunu da sözlerine ekledi. Siber güvenlik konusunda çok iyi derecede eğitim almış gençlere ülkemizde çok ihtiyaç olduğunu da söyledi. Bunun için de sadece gençlerin değil üniversitelerimizin de bu anlamda bölümlerini, müfredatlarını gözden geçirmelerinin daha iyi olacağını ve bu konuda yeni bölümler açılıp yeni açılımlara yol alınması gerektiğini belirtti.

TÜBİTAK Başkanı Prof. Dr. Yücel Altunbaşak konuşmasında, siber güvenlik konusunun 10 yıl öncesine kadar nerdeyse hiç bilinmediğini ve bilinenlerin de sadece filmlerden romanlardan karşılaştığımız kadar olduğunu söylerken şu an geldiğimiz nokta da bu duruma ne kadar büyük çalışmalar yaptığımızı göstermektedir. İran ve Estonya'nın enerji sistemlerine yapılan saldırıların benzeri gibi bizim ülkemize de yapılmayacağının garantisini kimsenin veremeyeceğini belirtti ve siber güvenlik adına daha çok çalışmamız gerektiğini ifade etti.

Ergün, ülkelerin kritik teknolojik ürünleri, kritik teknoloji alanında yatırımları arttıkça sanayi casusluğu adını verdiği yeni bir siber saldırı türü ortaya çıkacağını belirtti. Bundan dolayı siber güvenliğin bizde çok önemli bir yeri olduğunu ve bu alanda çalışan personelimizi daha iyi eğitmeye çalıştıklarını da ifade etti.

Bilgi Teknolojileri ve İletişim Kurumu (BTK) Başkanı Tayfun Acarer da, yapılan tatbikatlarla var olan sistemi test etme fırsatını bulduklarını ifade ederek, bu tarz Siber Güvenlik Tatbikatlarına tüm kurum ve kuruluşlarımızın katılmalarını ve bu konuya hassasiyetle katılmalarını belirtti (TÜBİTAK, 2013).

2.16.4. Uluslararası Siber Kalkan Tatbikatı 2014

Ulaştırma, Denizcilik ve Haberleşme Bakanlığının siber güvenlik politikaları doğrultusunda, Uluslararası Telekomünikasyon Birliği (ITU), Bilgi Teknolojileri ve İletişim Kurumu (BTK) ile ITU-IMPACT işbirliğiyle düzenlenen "Uluslararası Siber Kalkan Tatbikatı 2014", 15-16 Mayıs 2014 tarihlerinde İstanbul'da gerçekleştirildi. **S**iber güvenlik konusunda farkındalığın arttırılması, siber saldırılara karşı koyma yeteneklerinin geliştirilmesi ve uluslararası koordinasyonun sağlanması amacıyla düzenlenen tatbikata ülkelerin ulusal siber olaylara müdahale ekipleri katıldı. Tatbikata BTK Başkanı Dr. Tayfun Acarer, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Haberleşme Genel Müdürü Atilla Çelik ve ITU Telekomünikasyon Geliştirme Bürosu (BDT) Temsilcisi Rosheen Awotar-Mauree birer açılış konuşması yaparak katıldılar (BTK, 2014).

Bilgi Teknolojileri ve İletişim Kurumu Başkanı Dr. Tayfun Acarer bilişim teknolojilerinin kullanıcısı, kullanıcıların kullanım süresi, kullanan kesimin giderek yaygınlaşması ve bu artan bilgi ve iletişim teknolojileri beraberinde siber güvenlik

sorunlarını da getirmektedir. Gerek kişisel gerek kurumsal olsun siber güvenlik ülke güvenliğidir ve bu güvenlik tedbirleri de giderek daha fazla önem kazanmıştır. Ne kadar tedbir alsak da bu konuda tüm kurumların dikkatli olması gerektiğini belirtti. Ayrıca internet bir ağdır ve bu ağı oluşturan tüm kurumlarımız ve kullanıcılarımız bu ağın bir halkası hükmündedir ve en zayıf halka bizim ne kadar dayanıklı olabileceğimizi de gösterir. O nedenle o zinciri oluşturan tüm halkaları güçlendirmek de hepimize düşmektedir. Siber güvenlik alanında ülkemizde birçok çalışma yapıldığını ve yapılan bu çalışmalarla ve tatbikatlarla ülkemizde siber güvenlik konusunda daha duyarlı bir nesil ortaya çıktığını da belirtti.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Haberleşme Genel Müdürü Atilla Çelik de konuşmasında internetin günlük yaşantımızı kolaylaştırdığını belirtirken bunun yanında bir takım sorunlara da sebep olduğunu belirtti. Ulaştırma, Denizcilik ve Haberleşme Bakanlığının koordine ettiği BTK, ITU ve ITU-IMPACT ile işbirliği içinde organize edilen Uluslararası Siber Kalkan Tatbikatına birçok ülkenin siber olaylara müdahale ekipleri (CERT) katılmaktadır.

Çelik, “Uluslararası Siber Kalkan Tatbikatını gerçekleştirmekteki amacımız, uluslararası işbirliğini geliştirmek, siber güvenlik alanındaki kapasiteyi arttırmak, siber saldırılara karşı tepki kabiliyetlerini geliştirmek, kurum içi, kurumlar arası ve uluslararası koordinasyonu geliştirmek ve bu konudaki farkındalık seviyesini arttırmaktır.” (aktaran BTK, 2014) şeklinde açıklama yapmıştır.

ITU Telekomünikasyon Geliştirme Bürosu (BDT) Temsilcisi Rosheen Awotar-Mauree ülkelerin siber olaylara müdahale ekipleri (CERT) kurulmuş olan atak simülasyonları ile yeteneklerini test edip bu esnada neler yapılması gerektiğini de süreçle birlikte takip etmektedirler. Gelecekte nelerin yapılacağı da bu sayede planlanabilmektedir. Ne kadar uzaklaşmaya çalışsak da artık bilişim teknolojilerine çok bağlı olduğumuz da bilinen bir gerçektir ve hayatımızın vazgeçilmez bir parçası haline gelmiştir. Sağlıktan ekonomiye, enerji sektöründen ulaşım sektörüne kadar birçok önemli sektörde internetin sürekli kullanılmasının önemini vurguladı.

Panel ve Çalıştaylar

Uluslararası Siber Kalkan Tatbikatının ilk gününde panel ve çalıştaylar gerçekleştirildi.

ITU-IMPACT Uluslararası İşbirliği ve Politika Direktörü Philip Victor, siber saldırıda bölgesel ve uluslararası işbirliğinin önemine vurgu yaptı.

Yunanistan Telekomünikasyon ve Posta Komisyonu Başkanı Konstantinos Louropoulos, Avrupa Birliği (AB) ve Yunanistan'ın Siber Güvenlik Tecrübeleri konusunda yapılan çalışmalar hakkında bilgi verdi.

ITU-T Siber Güvenlik Çalışma Grubu Raportörü Dr. Youki Kadobayashi, inanılmaz hızla ilerleyen teknolojinin korunması için kritik bilgilerin de muhafazasının çok önemli olduğunu belirtti.

Ayrıca etkinliğin ilk gününde siber güvenlikte uluslararası farkındalığın arttırılması amacıyla Çocukların İnternetin Zararlı Etkilerinden Korunması, Mobil Güvenlik ile Adli Bilişim ve Siber Soruşturma konularında çalıştaylar gerçekleştirildi (BTK, 2014).

Tatbikat Programı

Programın ikinci gününde İtalya Başbakanının siber güvenlik danışmanı Andrea Rigoni bir açılış konuşması yaptı.

İtalya Başbakanının siber güvenlik danışmanı Andrea Rigoni bir açılış konuşması yaptığı tatbikat programında ülkelerin ulusal siber olaylara müdahale ekiplerinin (CERT) yer aldığı gruplar oluşturularak siber güvenlik tatbikatı gerçekleştirildi.

"Tatbikat kapsamında, siber olaylara müdahale ekipleri tarafından yazılı mesajlarla iletilen siber senaryolara cevaplar verilmesi şeklinde uygulamalar gerçekleştirilerek ekiplerin siber cevap saldırılara verme yetenekleri test edildi" (BTK, 2014). Bunun yanı sıra da 2 farklı senaryondan oluşan siber tatbikat da "Senaryoların konusu sisteme yetkisiz erişim sonucunda sistemin değiştirilmesinin

ve Mobil cihazda Android Sistemin incelenmesi konularından oluşmaktadır" (BTK, 2014). Her bir senaryo için ayırılan süre 120 dakikadır.

Kapanışta BTK adına konuşan Bilgi Teknolojileri Dairesi Başkanı K. Sacid Sarıkaya, etkinliğin ülkemizde ilk defa düzenlenmesi ve 20 ülkeden temsilcilerin katılması ve böyle bir tatbikata ev sahibi olarak yer vermekten mutlu olduklarını ifade etti ve bu ve buna benzer etkinliklerin de devamını geleceğini sinyallerini verdi (BTK, 2014).

2.16.5. Kilitli Kalkan (Locked Shield) Tatbikatı - 2014

Siber olaylara karşı NATO ülkeleri arasında işbirliğini tesis etmek, bilgi paylaşımını sağlamak ve mevcut yetenekleri değerlendirmek maksadıyla, 20-23 Mayıs 2014 tarihleri arasında Kilitli Kalkan (Locked Shield-2014) Tatbikatı icra edilmiştir.

Sanal bir ağ üzerinden icra edilen bu tatbikat; Tatbikat Kontrol Merkezi, NATO Siber Savunma Mükemmeliyet Merkezi (Tallinn/ESTONYA)'nde oyuncu statüsünde bulunan 12 takımın (NATO NCIRIC, Danimarka-Hollanda, İtalya, Estonya, Avusturya-Letonya, Polonya, Türkiye, Macaristan, İspanya, Çek Cumhuriyeti-Litvanya, Finlandiya, Fransa) Yerel Kontrol Merkezlerinin bulundukları coğrafyada tesis edilmiştir.

Türkiye adına tatbikata; TSK Siber Savunma Komutanlığı ve TÜBİTAK Siber Güvenlik Enstitüsü'nden oluşturulan müşterek takım ile katılım sağlanmış ve Yerel Kontrol Merkezi TSK Siber Savunma Komutanlığında tesis edilmiştir.

Tatbikata; MSB, Dışişleri Bakanlığı ile Ulaştırma, Denizcilik ve Haberleşme Bakanlığından da gözlemciler katılmıştır.

Tatbikatta, TSK Siber Savunma Komutanlığı'nın siber olaylara müdahale yetenekleri ve diğer NATO ülkeleri ile işbirliği faaliyetleri başarılı olarak test edilmiştir (Sibersavunma, 2014).

ÜÇÜNCÜ BÖLÜM
YÖNTEM VE MATERYAL

Bu bölüm altı alt baslıktan oluşmaktadır. Bu alt baslıklar sırasıyla *araştırmanın yöntemi*, *çalışma grubu*, *veri toplama aracının geliştirilmesi süreci*, *verilerin analiz yöntemi, verilerin analiz süreci* ve son olarak *veri analizinde kullanılan kategoriler* şeklinde ele alınmıştır.

3.1. Araştırmanın Yöntemi

Bu bölümde araştırmanın yöntemi ele alınmaktadır. Literatüre bakıldığında araştırılan olayı anlamlandırmada genel olarak kullanılan iki yöntem öne çıkmaktadır: nicel araştırma yöntemleri ve nitel araştırma yöntemleri. Nicel araştırma, basamakları ve sınırları açık bir biçimde belirlenmiş bir süreçtir. Nitel araştırmada ise duruma göre farklılık gösteren bir süreç yürümektedir (Yıldırım ve Şimşek, 2006). Yıldırım ve Şimşek (2006) nitel araştırmanın, araştırmacıya çalışmalarında esnek bir hareket alanı sağladığını, araştırmanın çeşitli basamaklarının birbiriyle tutarlı olmasına fırsat verdiğini belirtmektedir. Bu iki farklı araştırma yöntemlerinden birinin diğerine tercih edilmesi her şeyden önce araştırma konusuyla ilişkilidir. Nitel araştırma sürecinin aşamaları aşağıdaki şekilde özetlenmiştir.

Şekil 3. 1. Nitel Araştırma Sürecinin Adımları (Yıldırım ve Şimşek, 2006)

Bu tez çalışmasında Türk Silahlı Kuvvetler personelinin "Bilişim Suçlarına" yönelik algılarının ve görüşlerinin belirlenmesi ile teknolojiye yönelik bilgi düzeylerinin değerlendirilmesi amaçlanmaktadır. Bu tür bir çalışmanın ise derinlemesine analiz gerektirdiği, söz konusu kavrama yönelik algıların belirlenmesi ve bunlar arasındaki ilişkilerin ortaya konulması ve bilişim teknolojileri ile siber uzay, siber saldırı, siber terör siber savaş gibi kavramlara yönelik bakış açısını incelemek için araştırmacının kendi bakış açısıyla yaklaşımını gerekli kıldığı açıktır. Bu çalışma sürecinde incelenen olgular ve çalışmanın amaçları düşünüldüğünde bu çalışmanın nitel bir çalışma olması gerektiği söylenebilir. Çünkü ancak nitel bir çalışma ile ayrıntılı olarak yapılan analizler sonucunda, TSK personelinde bilişim suçlarına yönelik algılarının neler olduğunun belirlenmesi mümkündür.

Araştırmaların yöntem bakımından nitel araştırma ve nicel araştırma olarak ikiye ayrıldığı gibi amaçları bakımından da sınıflandırılabildikleri görülmektedir. Bunlar; açıklayıcı (explanatory), betimleyici (descriptive) ve anlamlandırıcı (exploratory) olarak üçe ayrılabilir (Robson, 1993). Açıklayıcı amaca yönelik yapılan araştırmalarda, bir durum ya da problem açıklanmaya çalışılırken sebep-sonuç ilişkileri göz önünde bulundurulur. Betimleyici amaca yönelik yapılan bir araştırmayı yürüten bir çalışmacı ise insanların, olayların ya da durumların profillerini eksiksiz ve gerçekçi bir şekilde ortaya çıkarmayı amaçlar. Son olarak anlamlandırıcı araştırmalarda ise çalışmanın amacı olan biteni anlamak, yeni derinliklere ulaşmak ve herhangi bir olguyu yeni bakış açıları ile değerlendirebilmektir. Bir araştırmanın tek bir amaçla yapılabileceği gibi iki veya daha çok amaçla yapılabileceği de ileri sürülmektedir. Çoğunlukla bu üç tür araştırma amaçlarından biri diğerlerine nazaran daha baskın olmaktadır (Robson, 1993). Bu tez çalışmasında TSK personelinin bilişim teknolojileri ve bilişim suçları kavramlarına yönelik algıları ve bilgi alt yapıları belirlenmek istendiği için betimleyici bir araştırma özelliklerini taşıdığı söylenebilir.

3.2. Çalışma Grubu

Gaziantep ilinde halen çalışmakta olan 1 albay, 1 yarbay, 3 yüzbaşı, 1 üsteğmen, 1 hukukçu asteğmen, 4 başçavuş, 1 kıdemli üstçavuş, 1 kıdemli uzman çavuş, 2 uzman çavuş olmak üzere toplam 15 Türk Silahlı Kuvvetleri personelinden

oluşmaktadır. Hizmet yılları 2-22 yıl arasında değişen bu personellerin katılımı tamamen gönüllülük esasına dayanmaktadır. Bu çalışma grubuna ulaşabildiği için araştırma bu çalışma grubu üzerinde yapılmıştır. Gerçekleştirildiği dönem açısından, 2014-2015 eğitim yılının ilk yarısında gerçekleştirilmiştir.

Araştırmaya katılan çalışma grubundaki kişiler okuyucu tarafından ayırt edilebilmesi için rastgele isimlerle kodlanmıştır. Bu 15 personelin kodları; Başçavuş Abdullah, Başçavuş Ahmet, Başçavuş İdris, Başçavuş Mesut, Uzman Çavuş Bayram, Uzman Çavuş Mehmet, Kıdemli Uzman Çavuş Murat, Kıdemli Üstçavuş Sinan, Asteğmen Burak, Asteğmen Ferhat, Yüzbaşı Bayram, Yüzbaşı Emir, Yüzbaşı Mehmet, Yarbay Hakkı, Albay Halit olarak belirlenmiştir.

3.2.1. Araştırmaya Katılan TSK Personelinin Genel Özellikleri

Görüşme sürecinde Gaziantep ilinde görev yapan 15 TSK personeliyle görüşülmüştür. Görüşme yapılan TSK personelinin rütbeleri, mesleki kıdem süreleri, yaş, eğitim durumları ve medeni durumları tablo ve grafikler aracılığı ile anlatılacaktır.

3.2.1.1. Araştırmaya Katılan TSK Personelinin Rütbeleri

Gaziantep ilinde halen çalışmakta olan 1 albay, 1 yarbay, 3 yüzbaşı, 1 üsteğmen, 1 hukukçu asteğmen, 4 başçavuş, 1 kıdemli üstçavuş, 1 kıdemli uzman çavuş, 2 uzman çavuş olmak üzere toplam 15 Türk Silahlı Kuvvetleri personelinden oluşmaktadır

Tablo 3. 1. Araştırmaya Katılan TSK Personelinin Rütbeleri

Görüşülen TSK Personelinin Rütbeleri	**f**
Albay	1
Yarbay	1
Yüzbaşı	3
Üsteğmen	1
Asteğmen (Avukat)	1
Başçavuş	4
Kıdemli Üstçavuş	1
Kıdemli Uzman Çavuş	1
Uzman Çavuş	2
TOPLAM	**15**

3.2.1.2. Araştırmaya Katılan TSK Personelinin Yaşları

Araştırmaya katılan TSK personelinin 4'ü yani yaklaşık %26,6'sı 20-29 yaş arası, 7'si (%46,6) 30-39 yaş arası ve 4'ü (%26,6) 40 ve üstü yaş aralığındadır.

Tablo 3. 2. Araştırmaya Katılan TSK Personelinin Yaşları

Yaş Aralığı	TSK Personel Sayısı	Yüzde
20-29	4	%26,6
30-39	7	%46,6
40 ve üstü	4	%26,6
Toplam	**15**	**%100**

3.2.1.3. Araştırmaya Katılan TSK Personelinin Mesleki Kıdem Durumu

Araştırmaya katılan TSK personelinin 4'ü yani yaklaşık %26,6'sı 1-9 yıl arası, 10'u (%66,6) 10-19 yıl arası ve 1'i (%'6,6) 20 ve üstü yıl süredir TSK'da görev yapmaktadır.

Tablo 3. 3. Araştırmaya Katılan TSK Personelinin Mesleki Kıdem Durumu

Yıl Aralığı	TSK Personel Sayısı	Yüzde
1-9	4	%26,6
10-19	10	%66,6
20 ve üstü	1	%6,6
Toplam	**15**	**%100**

3.2.1.4. Araştırmaya Katılan TSK Personelinin Eğitim Durumu

Araştırmaya katılan TSK personelinin 2'si yani yaklaşık olarak %13,3'ü lise mezunu, diğer 2'si (%13,3) yüksekokul mezunu, 9'u (%60) lisans mezunu ve son olarak 2'si (%13,3) lisansüstü eğitim mezunudur. Bu sonuçlara dayanarak araştırmaya katılan TSK personelinin büyük çoğunluğunun fakülte mezunu olduğunu söylenebilir.

Tablo 3. 4. Araştırmaya Katılan TSK Personelinin Eğitim Durumu

Eğitim Durumu	TSK Personel Sayısı	Yüzde
Lise	2	%13,3
Yüksekokul	2	%13,3
Lisans	9	%60
Yüksek Lisans	2	%13,3
Toplam	**15**	**%100**

3.2.1.5. Araştırmaya Katılan TSK Personelinin Medeni Durumu

Araştırmaya katılan TSK personelinin 13'ü yani yaklaşık olarak, %86,6'sı evli, 2'si ise (%13,4) bekârdır.

Tablo 3. 5. Araştırmaya Katılan TSK Personelinin Medeni Durumu

Medeni Durum	TSK Personel Sayısı	Yüzde
Evli	13	%86,6
Bekâr	2	%13,4
Toplam	**15**	**%100**

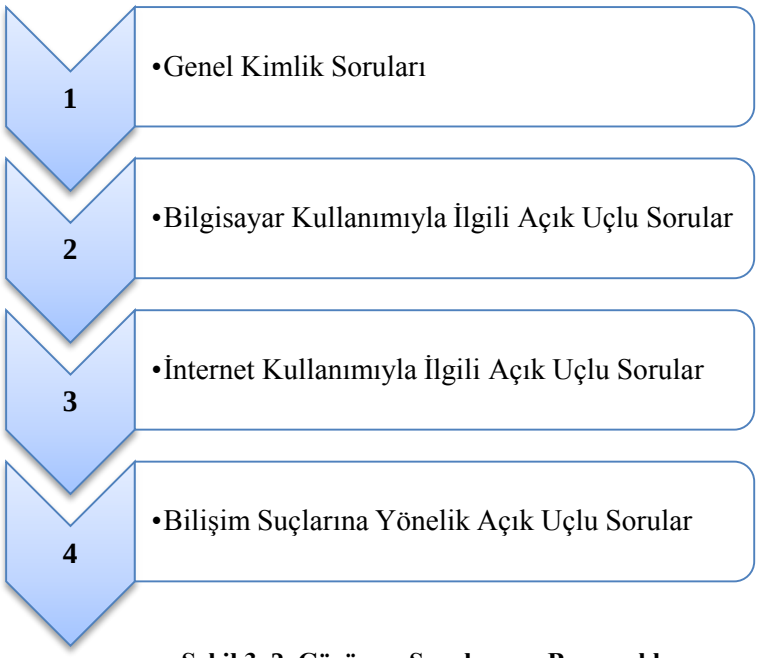
Bu sonuçlara dayanarak araştırmaya katılan TSK personelinin büyük çoğunluğunun evli olduğunu söylenebilir.

3.3. Veri Toplama Aracının Geliştirilmesi Süreci

Bu tez çalışmasında katılımcıların bilişim teknolojileri ve bilişim suçlarına ilişkin görüşlerini öğrenmek amacıyla açık uçlu sorulardan oluşan bir görüşme formu veri kaynağı olarak kullanılmıştır. Kullanılan görüşme formu ile ilgili ayrıntılı bilgi vermeden önce görüşme soruları hakkında genel bir bilgi verilmesi yararlı olacaktır.

Görüşme soruları; bilişim teknolojileri ve bilişim suçları kavramları göz önüne alınarak hazırlanmış olan soru havuzundan elenerek seçilmiştir. Görüşme soruları dört basamaktan oluşmuştur. Birinci basamak soruları genel kimlik sorularından oluşmaktadır. İkinci basamak soruları bilgisayar kullanımıyla ilgili sorulardan oluşmaktadır. Üçüncü basamak soruları internet kullanımıyla ilgili sorulardan oluşmaktadır. Son olarak dördüncü basamak soruları ise bilişim suçları ile ilgili sorulardan oluşmaktadır (bkz. Şekil 3.2). Uzman görüşü alınarak sorulara son

şekli verilmiştir. Katılımcılara yöneltilen sorular ekler tablosunda yer almaktadır (Ek-A).



Şekil 3. 2. Görüşme Sorularının Basamakları

Tüm bu açıklamalardan sonra, bu çalışmada veri toplama amaçlı kullanılmış olan soruların, katılımcıların var olan bilgilerini ve görüşlerini ortaya koymak ya da diğer bir söylemle sahip oldukları bilgiyi ölçmek ve konuya olan yaklaşımlarını belirlemek amaçlı kullanılan sorular içerdiği görülmektedir. Bu sorular yüz yüze görüşme yöntemiyle birebir cevaplanmış ve ses kayıt cihazıyla kayıt altına alınmıştır. Görüşmeye katılan katılımcılardan sorular üzerine bireysel olarak düşünüp kendi fikirlerini belirtmeleri istenmiş ve bu uygulama için herhangi bir zaman kısıtlaması verilmemiştir. Daha sonra bu kayıtlar bilgisayar ortamında yazıya dökülmüştür. Tüm katılımcılara sorulara verdikleri yanıtlar okutularak onayları alınmıştır.

Görüşme formunda yer alan sorular açık uçlu soru tipini yansıtmaktadır. Bu tür soruların tercih edilmesiyle, araştırmacının beklemediği veya planlamadığı cevapları da alabilmesi ve böylece konu hakkında daha geniş ve ayrıntılı bilgiye sahip olunabilmesi amaçlanmaktadır. Ayrıca açık uçlu soru sorma yöntemi, sorulara verilen cevapların kodlanarak analiz edilmesinde yaşanan güçlüklere rağmen daha detaylı bilgiye ulaşılmasına fırsat tanıması açısından avantajlı sayılmıştır.

3.4. Verilerin Analiz Yöntemi

Literatürde içerik analizi ile ilgili pek çok tanım ve açıklama mevcuttur (Açıl, 2011). İçerik analizi, bir metinin ya da görsel, işitsel bir materyalin; nesnel, niceliksel ve sistematik olarak çözümlenmesindir (Kayaoğlu, 2009). Çözümlenen verilerin kavramsallaştırılmasından sonra ortaya çıkan kavramlara göre mantıklı bir örüntü oluşturulur ve veriyi açıklayan tema saptanır (Yıldırım ve Şimşek, 2006).

Birçok araştırmacıya göre içerik analizinin tanımı farklı olsa da, hepsinin vurguladığı iki önemli nokta, yöntemin *sistematik* ve *tarafsız* olması gerektiğidir (Kayaoğlu, 2009; Koçak ve Arun, 2006; Yıldırım ve Şimşek, 2006). İçerik analizi her ne kadar yansız ve sistematik bilgi sunmayı amaçlasa da diğer yöntemler gibi, olumlu yönlerinin yanında olumsuz yönlerinin de olduğu belirtilmektedir (Açıl, 2011). Çalışmalarında içerik analizi yöntemini kullanan araştırmacılar 4 önemli yöntemsel sorunla karşılaşmaktadır: analiz biriminin seçilmesi, analiz edilecek kategorinin tanımlanması, geçerliliğin ve güvenirliliğin sağlanması ve örneklem sorunu (Koçak ve Arun, 2006). İçerik analizinin bu basamaklarına kısaca değinilecektir.

3.4.1. Analiz Biriminin Seçilmesi

İçerik analizi bir ifadenin doğruluğunu belirleyemez, bir metnin içeriğini yorumlayamaz fakat bir metnin içeriğini açığa çıkarabilir (Neuman, 2008). Bu nedenle araştırmacı metni doğrudan incelemelidir. Bunun için ilk olarak araştırmacı inceleyeceği analiz birimini belirlemelidir. Yani analiz biriminin belirlenmesi analize başlamanın ilk adımıdır ve bu nedenle çok önemlidir. Analiz birimi genel bir ifadeyle, bir kodun tayin edildiği metin miktarıdır (Neuman, 2008). Analiz birimi; bir kelime, bir cümle, bir tema veya bir hikâye olmak üzere geniş bir yelpaze sergileyebilir ve analiz birimi olarak kabul edilebilir. Ancak nitel çalışmalarda iki tür analiz biriminden bahsedilmektedir: sözcükler veya cümleler.

Bu çalışmada elde edilen verilerin analizlerinde, katılımcılardan alınan cevaplarda kurulan cümle ya da cümlecikler analiz birimi olarak kabul edilmiştir. Örneğin, bir katılımcının **‘Meslek içinde bilişim suçları ile ilgili herhangi bir eğitim aldınız mı?’** sorusuna yönelik vermiş olduğu cevap şöyledir:

> "…….Şimdi duyduğumuz kadarıyla mesleğimiz açısında da burada işte bize tatbikatlar filan da yapıldı Karanet ağı üzerinden. Onun haricinde sadece bilgilendirme amaçlı yazılar aldık. Onun haricinde eğitim gibi bir şey olmadı. ……."

Bu örnek cevapta yer alan cümle analiz birimi olarak kabul edilmiştir ve bu cevap **'Eğitim'** kategorisi altında değerlendirilmiştir.

3.4.2. Analiz Edilecek Kategorilerin Belirlenmesi

İçerik analizinde elde edilen kavramların birbirleriyle bağlantılı olarak belirli bir konu altında sınıflandırılmasına kategori denmektedir (Yıldırım ve Şimşek, 2006). Yıldırım ve Şimşek'e (2006) göre kavramların incelenmesi sonucunda bu kavramların birbirleri ile olan ilişkileri çıkarılır ve bu ilişkiler daha üst bir kategori ile açıklanır. Kategoriler elde edilen kavramlardan daha geneldir. Nitel araştırmalarda kategorilerin ayrı bir önemi vardır. Bu önem yazılı bir metnin çalışma açısından anlamlı hale getirilmesi gereğinden kaynaklanmaktadır.

Kodlama bir metinde yer alan anlamlı bölümlere (bir sözcük veya bir cümle vb.) kod verilmesi sürecidir (Bilgin, 2006). Kodlama çeşitli yöntemlerle yapılmaktadır. Bunlardan biri metinlerden çıkarılan kavramlara göre yapılan kodlama işlemidir. Bu araştırmada da böyle bir kodlama süreci uygulanmıştır. Araştırmacı tarafından, öncelikle, metinler satır satır okunmuş ve araştırmanın amacı çerçevesinde önemli görülen yerler belirlenmeye çalışılmıştır.

3.4.3. Geçerliliğin ve Güvenirliğin Sağlanması

İnandırıcılık, bilimsel araştırmalarda en önemli ölçütlerden biri olarak kabul edilmektedir. Bu açıdan geçerlilik ve güvenirlilik araştırmacılar için oldukça önemlidir. İçerik analizinin geçerliliği, çalışmanın amaçları ve araçları arasındaki uygunlukla ilgilidir (Bilgin, 2006). Yani geçerlilik ölçme aracının ölçmeyi amaçladığı nesneyi doğru ölçüp ölçmediği ile ilgilenir ve sonuçların doğruluğunu konu edinir. İçerik analizinin güvenirliliği ise kodlama işlemiyle ilgilidir (Ghuiglione ve Matalon, 1978). Bu durum kodlayıcıların ya da kodlama kategorilerinin güvenirliliğine bağlıdır. Kodlayıcıların güvenilirliği, aynı kodlayıcının aynı metni farklı zamanlarda aynı şekilde kodlaması veya aynı metnin farklı kodlayıcılar tarafından aynı şekilde kodlanması anlamına gelmektedir. Kategorilerin güvenilirliği

ise anlamlarının açık olmasıyla ilişkilidir. Yani bir kategori başlığı herkes tarafından aynı şekilde anlaşılmalıdır.

Bu çalışmada ise ilk olarak yazılı hale getirilen katılımcı cevapları üzerine ait olduğu kod/kodlar not edilmiştir. Sonra farklı bir zaman diliminde aynı araştırmacı tarafından bu kodlamalar tekrar yapılmıştır. İnceleme sonunda kodlar için genel olarak bir bütünlüğe varılmasına rağmen aynı cevap için verilen farklı kodlamaların da olduğu görülmüştür. Bunun için araştırmacı tekrar bu farklı kodlamalar üzerinde dikkatli bir değerlendirme ile son kararını vermiştir. Bu süreç sonunda ortaya çıkan kategoriler ve sıklıkları belirlenmiştir. Böylelikle araştırmanın kodlayıcı güvenirliliği sağlanmış olmaktadır.

3.4.4. Çalışma Grubu Sorunu

Nitel araştırmalarda genelleme endişesi olmadığı için evren parametresine bakılmamıştır. Nitekim sınırlılık başlığında da bundan bahsedilmiştir. Ulaşılabilen çalışma grubu üzerinden araştırma yapılmıştır.

3.5. Verilerin Analiz Süreci

Araştırmanın bu kısmında görüşme formundaki sorulardan elde edilen verilerin nasıl analiz edildiğine yer verilecektir.

Araştırma kapsamındaki TSK personelinin bilgi teknolojileri ve bilişim suçları konusundaki var olan bilgilerini yoklamak için hazırlanan bu görüşme formu 4 basamaktan oluşmaktadır. İlk basamak soruları genel kimlik sorularından oluşmaktadır. İkinci basamak soruları bilgisayar kullanımı üzerine sorulardır. Üçüncü basamak soruları internet kullanımı üzerinedir. Son basamak olan dördüncü basamak ise bilişim suçları üzerine hazırlanmış sorulardan oluşmaktadır (bkz. Şekil 3.2.). İlk üç basamak araştırmaya katılan kişilerin bilgi teknolojileri ile ilgili bilgilerini ölçmek için kullanılmıştır. Son basamak ise personellerin bilişim suçlarına karşı yaklaşımlarını ölçmek için kullanılmıştır. Bu sorulara ilişkin 15 katılımcı personelin verdiği cevapların analizleri içerik analizi yaklaşımı benimsenerek gerçekleştirilmiştir. Dolayısıyla öncelikle tüm personellerin sorulara verdikleri cevaplar teker teker incelenmiştir. Bu inceleme sırasında personellerin sorulara yapmış oldukları yorumlardan yola çıkılarak belli kategoriler ve kodlar

oluşturulmuştur. Bu kategorilere ve kodlara yönelik açıklamalar ise bir sonraki bölümde ele alınacaktır.

3.6. Veri Analizinde Kullanılan Kategoriler

İçerik analizi materyalin içeriğinin anlaşılması ve metinlerdeki kelimelerin ve cümlelerin niteliğinin belirlenmesi amacıyla kullanılır. Bu yaklaşım, çalışmada elde edilen verilerden kategorilerin oluşturulmasına olanak tanımaktadır (May, 1996). Bu tezde içerik analizi türlerinden "kategorileştirilmiş analiz" kullanılmıştır. Kategorileştirilmiş analiz, genel olarak belirli bir ifadenin önce birimlere bölünmesi ve ardından bu birimlerin daha önce belirlenmiş ölçütlere göre kategoriler hâlinde gruplandırılmasıdır (Tavşancıl ve Aslan, 2001). Kategori belirleme, özel verilerden yola çıkarak genel bir sonuç oluşturma süreci olarak açıklanmaktadır (Ely vd., 1998). Kategorileştirilmiş analizde ilk olarak veriler kodlanmakta ve bu kodlama, daha önceden belirlenmiş kavramların yanı sıra verilerin kodlanması esnasında ortaya çıkan kavramlara göre yapılmaktadır. Kodlar, soruların benzer cevaplarını tanımlayan ve verileri düzenleyip çözümlemeye yardım eden sembollerdir (Yaman ve Erdoğan, 2007). Verilerin kodlanmasından sonra bu kodları genel düzeyde açıklayan kategoriler oluşturulmaktadır.

Çalışmaya katılan TSK personelinin sorulara vermiş oldukları cevaplar ayrı ayrı incelenmiştir. Katılımcıların sorulara verdikleri cevapların değerlendirilmesiyle genel kimlik soruları haricindeki 3 basamak (Bilgisayar kullanımıyla ilgili görüşme soruları, İnternet kullanımıyla ilgili görüşme soruları ve bilişimi suçlarıyla ilgili görüşme soruları) için de ayrı ayrı kodlamalar/kategoriler ortaya çıkmıştır.

Katılımcıların bu sorulara verdikleri cevaplar ilk olarak elektronik ortamda yazılı hale getirtilmiştir. Benimsenen içerik analizi yaklaşımı gereğince katılımcıların sorulara vermiş oldukları cevaplar detaylı bir şekilde incelenmiştir. Katılımcıların bilişim suçları kavramına yönelik yapmış oldukları tanımlamalar ışığında, araştırmacı tarafından belli kodlar oluşturulmuştur. Araştırma sonucu belirlenen kodların frekans analizi oluşturulmuştur. (bkz. Tablo 3.6.). Frekans analizi oluşturulurken katılımcıların vermiş olduğu cevaplar içerisindeki kodların sayısı dikkate alınmıştır. Bu kodları genel düzeyde açıklayan kategoriler oluşturulmuş ve bu kategorilere dayalı olarak elde edilen veriler içerik analizine tabi tutulmuştur.

Bu kategoriler belirlenirken her bir kategorinin, bilişim suçlarının ne olduğuna ilişkin belirtilen ifadeyi yansıtabilecek şekilde oluşturulmasına dikkat edilmiştir. Yazılı hale getirilen katılımcı cevapları üzerine ait olduğu kod/kategoriler not edilmiştir. Sonra farklı bir zaman diliminde araştırmacı tarafından bu kodlamalar tekrar yapılmıştır. İnceleme sonunda kodlar için son şekli verilmiştir. Böylesi bir süreç sonunda ortaya çıkan kod ve kategoriler ve sıklıkları inceleme yapan araştırmacı tarafından belirlenmiştir. Bu şekilde yürütülen analiz yöntemiyle kodlama güvenirliği sağlanmıştır (Green ve Gilhooly, 1996). Dolayısıyla bu analizler sonucunda toplam 11 farklı kategori ortaya çıkmıştır (bkz. Tablo 3.7.). Analizler sonucu ortaya çıkan bu kategorilerden bazılarına ilişkin katılımcıların vermiş oldukları cevapların bir kısmı gelişigüzel seçilmiş ve seçilen bu cevaplar okuyucuya örnek olması açısından Tablo 3.7.'in en sağında sunulmuştur.

Tablo 3. 6. Araştırma sonucu oluşturulan kodların frekans analizi

Kodlar	**f**
Araştırma	11
Sosyal Aktivite	14
Bankacılık	15
İş	18
Güvenlik	42
Eğitim	27
Yasalar	7
Önleyici Tedbir	14
Özel Birimler	4
Bilgi Kirliliği	4
Cezai Yaptırımlar	9

Tablo 3. 7. Bilişim suçları soruları için verilen cevapların analizinde kullanılan kod, kategori ve örnek cevaplar

Kodlar	Kategoriler	Örnek Cevaplar
Güvenlik	Bilgi güvenliğinin sağlanması ve korunmasına yönelik tedbirler	*"Bilgi havuzu oluşturmuş oluyoruz internet ortamında ve bu bilgi havuzuna isteyen herkes yolunu bulursa erişebiliyor. Bence çok büyük güvenlik açığı. Bu yönden çok tehlikeli olduğunu düşünüyorum."*
Eğitim	Bilişim teknolojileri ve bilişim suçlarına yönelik mesleki eğitim	*"Şimdi duyduğumuz kadarıyla mesleğimiz açısında da burada işte bize tatbikatlar filan da yapıldı karanet ağı üzerinden. Onun haricinde sadece bilgilendirme amaçlı yazılar aldık. Onun haricinde eğitim gibi bir şey olmadı."*
Yasalar	Yürüklükte olan yasaların mevcut durumu ve yapılabilecek değişiklikler	*"Öncelikle TCK da bazı değişiklikler yapılması gerekmektedir. Özellikle daha spesifik bir anlam yöneltilmeli. Farklı bir ceza kanununda farklı bir kanuna aktarılması gerekmektedir. Bu konuda bilgili kişiler yetiştirilmeli. Ve bu konuda insanlar eğitim olarak bilinçlendirilmelidir."*
Önleyici Tedbir	Suç işlenmeden veya işlenirken engellenmesi	*"… farklı suç tiplerinin bazıları doğrudan resmi kurumlar tarafından suç işlenirken ve işlemeden önce engellendiğini düşünüyorum ama bazı alanlarda da bu çalışmanın eksik olduğunu ve yetersiz olduğunu düşünmekteyim."*
Özel Birimler	Bilişim teknolojileri ve bilişim suçları konusunda uzmanlaşmış birimler	*"Özellikle de bu konuda emniyetin bence bu konuda gerekli seminerleri vermesi gerekiyor. Eğitim alanında olsun TSK da olsun farklı farklı kurumlarda. Çünkü her kurumun kendine has terimleri, suçları oluyor. Ondan dolayı. O kuruma has eğitim verilmeli. TSK'da TSK'ya ait zaten genel olarak bir giriş yapıp sonrasında kurumsallaşarak seminerler verilmeli bence."*
Bilgi Kirliliği	Sanal ortamdaki bilgilerin doğrulana bilirliğinin zor olması	*"Bir de tabi internetteki her şeyin doğru olduğuna yüzde yüz doğru bilgiler olduğuna inanmıyorum ben. Bir kişi bir konu hakkında bir sayfalık yazı yazıyor yalan dolan. Ondan sonra o konuyla ilgili ne kadar arama motorlarında arama yaparsanız yapın o sitelerde aynı bilgiler geliyor. Aynı yanlış bilgiden olabiliyor bazen."*
Cezai Yaptırımlar	Bilişim suçlarının yaptırımlarının yeterliliği	*"Yani gerçek hayatta verilen çoğu ceza bilişim suçlarıyla alakalı da olabilir diye düşünüyorum. Hapishane, tutukluluk, para cezası gerekirse bilişim ortamından uzaklaştırma. Psikiyatri tedavisi."*

DÖRDÜNCÜ BÖLÜM
BULGULAR VE TARTIŞMA

Bu bölümde öncelikle TSK personelinin bilgi teknolojileri ve bilişim suçları kavramlarına yönelik algılarının neler olduğuna ilişkin elde edilen verilerin analizi ve bu analizler sonucu ortaya çıkan bulgulara yer verilecektir. Bulguların ardından tartışma bölümüne geçilecektir. Bu bölümde ise yukarıdaki alt başlıklar kapsamında, katılımcıların cevaplarından elde edilen verilerin kritiği yapılacaktır.

4.1. Bulgular

Gaziantep ilinde görev alan TSK personelinin bilgi teknolojileri ve bilişim suçları kavramlarına yönelik bilgi alt yapıları belirlemek için yapılan görüşme bulguları aşağıda özetlenmektedir.

4.1.1. Veri Analizinde Kullanılan Kodlar

Bilgi teknolojileri ve bilişim suçları kavramına yönelik katılımcıların ne tür yaklaşımının olduğu ve bu yaklaşımların ne derece benzer olduğunu belirlemek amacıyla katılımcılara görüşme soruları yöneltilmiştir. 1 albay, 1 yarbay, 3 yüzbaşı, 1 üsteğmen, 1 hukukçu asteğmen, 4 başçavuş, 1 kıdemli üstçavuş, 1 kıdemli uzman çavuş, 2 uzman çavuş olmak üzere toplam 15 Türk Silahlı Kuvvetleri personelinin bilişim suçları kavramına yönelik sahip oldukları bilgi ve sergiledikleri yaklaşımlar kategorileştirilmiştir. Bu analizler sonucunda toplam 11 farklı kategori ortaya çıkmıştır ve sırasıyla çıkan sonuçlar yorumlanacaktır. Aşağıdaki tablolarda görüşme metinlerinde geçen kodlamalarla ilgili katılımcıların cümleleri verilmiştir. İlk dört kod ile elde edilen verilerle araştırma sorularımızın ilki olan "Türk Silahlı Kuvvetleri Personelinin bilgi teknolojileri ile ilgili bilgi düzeyleri nedir?" sorusunun

cevabını alırken diğer yedi kod ile ikinci ve son araştırma sorumuz olan "Türk Silahlı Kuvvetleri Personelinin bilişim suçlarına karşı yaklaşımı nedir?" sorusunun cevabını almaktayız.

4.1.1.1. Veri Analizinde Kullanılan Araştırma Kodu

Katılımcıların Araştırma kodu altında toplanan cevapları Tablo 4.1.'de gösterilmiştir. Katılımcılardan Başçavuş Ahmet, Başçavuş Abdullah, Uzman Çavuş Mehmet, Yüzbaşı Mehmet, Yüzbaşı Emir adlı TSK personelinin vermiş olduğu cevaplar Araştırma kodu altında toplanmıştır. Verilen cevaplara bakıldığında personel bilişim teknolojilerini araştırma amacıyla da kullandığını belirtmektedir. Herhangi bir konuda bilgi edinme amacıyla kaynaklara ulaşmak için kullanılan araçların başında bilişim teknolojileri gelmektedir.

Tablo 4. 1. Araştırmaya Katılan TSK Personelinin Araştırma Kodu Altında Verdiği Cevaplar

TSK Personeli	**Verilen Cevaplar**
Başçavuş Ahmet	*"Gerekli araştırma, merak ettiğim konuları evdeki bilgisayarımdan araştırıyorum"*
Yüzbaşı Mehmet	*"Bilgi alışverişi ve araştırma veya faydalanma konusunda kullanıyorum."*
Yüzbaşı Emir	*"Onun dışında böyle bir de çok fazla olmamakla birlikte araştırma yapmak için kullanıyorum. Bu maksatla."*
Başçavuş Abdullah	*"Adamın bir şey aklına geliyor hemen internetten yazıyor öğreniyor. Ondan sonra harita diyor, haritayı açıyor internetten hemen şu şuraydı bu buradaydı yolu tarif ediyor."*
Uzman Çavuş Mehmet	*"Evde ve işte internet bağlantım var genelde araştırma amacıyla kullanıyorum."*

4.1.1.2. Veri Analizinde Kullanılan Sosyal Aktivite Kodu

Katılımcıların Sosyal Aktivite kodu altında toplanan cevapları Tablo 4.2.'de gösterilmiştir. Katılımcılardan Başçavuş Ahmet, Başçavuş İdris, Uzman Çavuş Mehmet, Başçavuş Mesut Üstçavuş Sinan, Uzman Çavuş Murat, Asteğmen Burak adlı TSK personelinin vermiş olduğu cevaplar sosyal aktivite kodu altında toplanmıştır. Katılımcıların vermiş olduğu cevaplar incelendiğinde sosyal medyanın, internet kullanımından arda kalan zamanda yaygın ve düzenli bir şekilde kullanıldığı anlaşılmaktadır. Katılımcı Başçavuş İdris ve Üstçavuş Sinan sosyal medya kullanımında bilgisayarlardan ziyade akıllı cihazların Android uygulamalarından yararlandıklarını belirtmişlerdir.

Tablo 4. 2. Araştırmaya Katılan TSK Personelinin Sosyal Aktivite Kodu Altında Verdiği Cevaplar

TSK Personeli	Verilen Cevaplar
Başçavuş Ahmet	*"Diğer taraftan sosyal medyayı kullanıyorum. İyi bir sosyal medya takipçisiyim. Bu siteleri kullanıyorum."*
Başçavuş İdris	*"Vakit kalırsa sosyal paylaşım ağlarındaki hesaplarıma bakıyorum. Bazen video izliyorum akıllı cihazları kullanıyorum"*
Uzman Çavuş Mehmet	*"Çalışma, günlük işlerim için kullanıyorum. Evde sosyal amaçlı geri kalan işleri takip etmek amacıyla kullanıyorum."*
Başçavuş Mesut	*"Evde daha çok sosyal paylaşım amaçlı kullanıyorum."*
Üstçavuş Sinan	*"…bir de sosyal paylaşım sitelerine bakmada daha ziyade kullanıyorum bu da genellikle cep telefonundan Android uygulama sayesinde olmakta.."*
Uzman Çavuş Murat	*"İnterneti sosyal medyayı takip için…"*
Asteğmen Burak	*"Mail alışverişinde mesajlaşmada sosyal sitelerde kullanıyorum"*

4.1.1.3. Veri Analizinde Kullanılan Bankacılık Kodu

Katılımcıların Bankacılık kodu altında toplanan cevapları Tablo 4.3.'de gösterilmiştir. Katılımcılardan Başçavuş Ahmet, Başçavuş İdris, Başçavuş Abdullah, Uzman Çavuş Bayram, Başçavuş Mesut, Kıdemli Üstçavuş Sinan, Yüzbaşı Emir' in vermiş olduğu cevaplar incelendiğinde bankaların şubelerinde sıra bekleyerek işlemlerini zaman kaybı yaşamadan, kısa sürede ve diledikleri zaman yapabildiklerini belirtmişlerdir. İnternet bankacılığının akıllı cihazlarla ortak hareket eden güvenlik uygulamaları internet kullanımını tercih ettirdiği anlaşılmaktadır.

Tablo 4. 3. Araştırmaya Katılan TSK Personelinin Bankacılık Kodu Altında Verdiği Cevaplar

TSK Personeli	Verilen Cevaplar
Başçavuş Ahmet	*"Öncelikle bankacılık işlemlerimi bilgisayar üzerinden yapıyorum. "*
Başçavuş İdris	*"Genellikle haberleşme, internet bankacılığı ve bunun dışında alışveriş, sosyal paylaşım ağları, e-posta adresi mail kutumu kontrol etmek için düzenli olarak internet bağlantım var."*
Başçavuş Abdullah	*"İnternet bankacılığını kullanıyorum…"*
Uzman Çavuş Bayram	*"Bankacılık ve haberleşme işlemleri oluyor. Bunlarla da özellikle bankacılık işleri olsun güvenlik sorusunun telefona bağlı bir şekilde gelmesi benim için rahat oluyor…"*
Başçavuş Mesut	*"Daha çok internet bankacılığında kullanıyorum zaman ve zaman açısından daha doğrusu zaman kaybolmasın diye onu kullanıyorum"*
Kıdemli Üstçavuş Sinan	*"…banka hesaplarımı kontrol maksatlı kullanıyorum."*
Yüzbaşı Emir	*"Genellikle banka işlerinde kullanıyorum"*

4.1.1.4. Veri Analizinde Kullanılan İş Kodu

Katılımcıların İş kodu altında toplanan cevapları Tablo 4.4.'de gösterilmiştir. Katılımcılardan Başçavuş Ahmet, İdris Başçavuş, Albay Halit, Başçavuş Mesut, Kıdemli Üstçavuş Sinan, Kıdemli Uzman Çavuş Murat, Yüzbaşı Mehmet adlı TSK personellerinin yanıtları incelendiğinde katılımcıların mesleklerinin gerekleri olan faaliyetleri icra ederken kara ağını ve Microsoft Office Programlarını düzenli ve yaygın olarak kullandıkları anlaşılmaktadır.

Tablo 4. 4. Araştırmaya Katılan TSK Personelinin İş Kodu Altında Verdiği Cevaplar

TSK Personeli	Verilen Cevaplar
Başçavuş Ahmet	*"İşyerinden başlamak istiyorum. İşyerinde yazışmalar, yapacağımız işlerle ilgili dokumanlar bilgisayarda mevcut. İş yerindeki bilgisayar kullanımım bu şekilde."*
İdris Başçavuş	*"Karanet programı var. Diğer taraftan Word Excel var. Onları kullanıyoruz."*
Albay Halit	*"İşyerinde işlemleri bilgisayar üzerinden intranet üzerinden yapıyoruz."*
Başçavuş Mesut	*"İşyerinde daha çok işle alakalı. Excel Word Office programları"*
Kıdemli Üstçavuş Sinan	*"Genelde işyerinde sistem kurma üzerine kullanıyorum"*
Kıdemli Uzman Çavuş Murat	*"İşyerinde işyeriyle alakalı kayıttır, personel kaydı."*
Yüzbaşı Mehmet	*"İşyerinde işimle alakalı özelliklede Word Excel PowerPoint Office programlarını kullanıyorum."*

4.1.1.5. Veri Analizinde Kullanılan Güvenlik Kodu

Katılımcıların güvenlik kodu altında toplanan cevapları Tablo 4.5.'da gösterilmiştir. Katılımcılardan Başçavuş Ahmet, Başçavuş İdris, Başçavuş Mesut ve Kıdemli Üstçavuş Sinan isimli TSK personelinin cevapları güvenlik kodu altında toplanmıştır. Aşağıdaki tabloda örnekleri verilen cümleler ışığında bakıldığı zaman

güvenlik probleminin çözülmesiyle beraber bilişim teknolojilerinin daha sağlıklı ve işlevsel hale geleceği belirtilmektedir. Karanet ve yıllık siber savunma tatbikatlarıyla alınan güvenlik tedbirlerinin yanında TSK'nın konuyla ilgili olarak daha fazla tedbir alması gerektiği katılımcıların görüşlerinden anlaşılmaktadır.

Tablo 4. 5. Araştırmaya Katılan TSK Personelinin Güvenlik Kodu Altında Verdiği Cevaplar

TSK Personeli	Verilen Cevaplar
Başçavuş Ahmet	*"En başta güvenlik sorunu var. Güvenlik sorunu için bir şekilde önlem alındığında bilişim teknolojisinin kullanımı da daha faydalı olacaktır."*
Başçavuş İdris	*"Bilgi havuzu oluşturmuş oluyoruz internet ortamında ve bu bilgi havuzuna isteyen herkes yolunu bulursa erişebiliyor. Bence çok büyük güvenlik açığı. Bu yönden çok tehlikeli olduğunu düşünüyorum."*
Başçavuş Mesut	*"TSK bünyesinde kurulan bazı birimler var artı bizde yine Karanet ağı üzerinden kurulmuş şifrelendirme işlemleri var. Dışarından gelecek bir saldırıya karşı bu tür şeylerde ağımızı koruyoruz yani olay bu."*
Kıdemli Üstçavuş Sinan	*"Kesinlikle mesleğimiz icabı sene de bir siber savunma tatbikatı oluyor. Biz buna bilgi sistemci olduğumuz için hazırlıklıyız ancak gördüğümüz şu ki vatandaş olarak siber saldırıya hazırlıklı değiliz."*

4.1.1.6. Veri Analizinde Kullanılan Eğitim Kodu

Katılımcıların eğitim kodu altında toplanan cevapları Tablo 4.6.'da gösterilmiştir. Katılımcılardan; Başçavuş Ahmet, Başçavuş Abdullah, Kıdemli Uzman Çavuş Murat, Asteğmen Burak, Yüzbaşı Mehmet, Yüzbaşı Bayram, Yüzbaşı Emir ve Yarbay Hakkı isimli TSK personelinin cevapları eğitim kodu altında toplanmıştır. Katılımcıların verdikleri cevaptan TSK bünyesinden bilişim suçlarına ve siber saldırılara yönelik tatbikatlar, bilgilendirme yazıları, merkezden bağımsız yerel eğitim faaliyetleriyle bir takım önlemlerin alındığı anlaşılmaktadır. Ancak düzenli bir biçimde rütbe ve kışla ayırt etmeksizin bilişim teknolojileri ve siber savunma konusunda eğitim verilmediği görülmüştür.

Tablo 4. 6. Araştırmaya Katılan TSK Personelinin Eğitim Kodu Altında Verdiği Cevaplar

TSK Personeli	Verilen Cevaplar
Başçavuş Ahmet	*"Şöyle ki; bu tarz bir suç ile şimdiye kadar karşılaşmadım. Ama bu kavramlara aşinayım. Üniversitede derslerimde de siber konularla alakalı bilişim dersimiz vardı. Bilişim dersinde siber suçlarla ilgili konuları okudum"*
Başçavuş Abdullah	*"Kışla içinde genel bir bilişimle ilgili işte bu siber saldırılarıyla ilgili brifinglere katıldım."*
Kıdemli Uzman Çavuş Murat	*"Meslek içerisinde almadım. Bu bizim çalıştığımız kurum için çok büyük bir eksiklik. Ben mesela meslek için şöyle bir şey düşünebilirim; bizim mesleğimizin lider eğitim saati var lider eğitiminde mesela biz 18 yıldır aynı şeyleri görüyoruz. Harita, pusula yani askeri şeyler. Bence bunun yerine lider eğitiminde bu tür tüketici hakları; araban çalında ne yaparsın, banka seni dolandırdı ne yaparsın, işte bu tür bilişim suçlarıyla karşılaştın ne yaparsın. Bu tür eğitimlerin verilerek bizim gibi mesleği sadece askerlik olana sabah girip akşam çıkan adamlara daha faydalı olacağını düşünüyorum."*
Asteğmen Burak	*"Sosyal hayatta da zaten insan bilgisayarla uğraşan her insan bir yerde hacker olmaya meyillidir. Bu da bilişim suçlarını doğuruyor sonuç olarak. Bununla alakalı yapılması gereken insanlara bilişim ahlakı aşılamak. Etik değerleri sadece günlük hayatta değil bilgisayar ortamında da verebilmek. Hani insanlar sosyal ağda başka kimlik adı altında farklı karakterler geliştirebiliyorlar."*
Yüzbaşı Mehmet	*"Siber saldırı zaten mesleğim gereği bizde çok önemli konu. Bununla ilgili silahlı kuvvetlerde tatbikatlar yapılıyor ve diğer devlet kurumlarında da bunla ilgili çalışmalar olduğunu biliyorum."*
Yüzbaşı Bayram	*"Şimdi duyduğumuz kadarıyla mesleğimiz açısında da burada işte bize tatbikatları filan da yapıldı Karanet ağı üzerinden. / Sadece bilgilendirme amaçlı bilgilendirme amaçlı yazı aldık. Onun haricinde eğitim gibi bir şey olmadı."*
Yüzbaşı Emir	*"Tabi ki yani yok bu konuyla bilişim suçlarıyla ilgili eğitim verilmedi ama şeyle ilgili biliyoruz. Yazılar geliyor onlardan okuduğumuz kadarıyla. Öncelikle eğitim sürecine girmedik."*
Yarbay Hakkı	*"Siber saldırı siber savaş. Bunların dersini gördük. Silahlı kuvvetlerde siber saldırıyla ilgili bilmem ne kurulmuş durumda. Bunu duyuyoruz. Yine bilim ve teknoloji bakanlığında bununla ilgili şeyler var. Yani çeşitli kamu kurum ve kuruluşların bu konuda faaliyet gösterdiğini biliyoruz. Buna Türk Silahlı Kuvvetleri de dahil. Yine ders kapsamında ya da zaman zaman gazetelerden filan ya da ders kapsamında zaten ilk tanışıklığımız. 2010-2011 gibi o zaman akademideydik. O zaman işte şimdi örnek olarak İran'ın İsrail İHA'sını, siber savunma dersleri gördük.*

	Yine İsrail'in yapmış olduğu siber saldırılar. Bu kapsamda barajdan tutun da yer altı ve yer üstü tüm sistemler siber saldırı ile çökertilebilir."

4.1.1.7. Veri Analizinde Kullanılan Yasalar Kodu

Katılımcıların yasalar kodu altında toplanan cevapları Tablo 4.7.'da gösterilmiştir. Katılımcılardan Başçavuş Ahmet, Asteğmen Ferhat ve Uzman Çavuş Murat isimli TSK personelinin cevapları yasalar kodu altında toplanmıştır. Başçavuş Ahmet ve Asteğmen Ferhat mevcut hükümlerin yeterli olmadığını yasal düzenlemeler yapılması gerekliliğini vurgulamıştır. Asteğmen Ferhat bilişim suçları için ayrı bir ceza kanunun yapılması gerekliliğini vurgulamıştır. Uzman Çavuş Murat ise yasal düzenlemelerden ziyade eğitime ve yetişmiş personele vurgu yapmıştır.

Tablo 4. 7. Araştırmaya Katılan TSK Personelinin Yasalar Kodu Altında Verdiği Cevaplar

TSK Personeli	**Verilen Cevaplar**
Başçavuş Ahmet	*"Bilişim suçlarıyla ilgili açık hükümler de mevcut. O şekilde kanuni düzenlemeler de tabi ki ileriki bazda bilişim suçlarına yönelik kanuni düzenlemeler yapılarak daha iyi boyuta taşınabilir.."*
Asteğmen Ferhat	*"Öncelikle TCK da bazı değişiklikler yapılması gerekmektedir. Özellikle daha spesifik bir anlam yöneltilmeli. Farklı bir ceza kanununda farklı bir kanuna aktarılması gerekmektedir. Bu konuda bilgili kişiler yetiştirilmeli. Ve bu konuda insanlar eğitim olarak bilinçlendirilmelidir."*
Kıdemli Uzman Çavuş Murat	*"insan olan yerde çok insanın elinin dediği şeyde istediğin kadar yasakla, yasakla hiçbir şey çözüm değil. İnsanları eğitmek lazım."*

4.1.1.8. Veri Analizinde Kullanılan Önleyici Tedbir Kodu

Katılımcıların önleyici tedbir kodu altında toplanan cevapları Tablo 4.8.'da gösterilmiştir. Katılımcılardan yalnızca Başçavuş Ahmet adlı TSK personelinin cevabı yasalar kodu altında toplanmıştır. Katılımcı diğer katılımcılardan farklı olarak suç işlenmeden veya suç sonuçlanmadan müdahale edilmesinin önemini vurgulamıştır.

Tablo 4. 8. Araştırmaya Katılan TSK Personelinin Önleyici Tedbir Kodu Altında Verdiği Cevaplar

TSK Personeli	Verilen Cevaplar
Başçavuş Ahmet	*"... farklı suç tiplerinin bazıları doğrudan resmi kurumlar tarafından suç işlenirken ve işlemeden önce engellendiğini düşünüyorum ama bazı alanlarda da bu çalışmanın eksik olduğunu ve yetersiz olduğunu düşünmekteyim."*

4.1.1.9. Veri Analizinde Kullanılan Özel Birimler Kodu

Katılımcıların özel birimler kodu altında toplanan cevapları Tablo 4.9.'da gösterilmiştir. Katılımcılardan Başçavuş Ahmet ve Asteğmen Burak adlı TSK personelinin cevapları özel birimler kodu altında toplanmıştır. Katılımcılar bilişim suçları ve siber saldırılara karşı ilgili kurumlarda uzman personellerden oluşan özel birimlerin oluşturulması gerekliliğini vurgulamıştır.

Tablo 4. 9. Araştırmaya Katılan TSK Personelinin Özel Birimler Kodu Altında Verdiği Cevaplar

TSK Personeli	Verilen Cevaplar
Başçavuş Ahmet	*"... ilgili kurumlarda başta olmak üzere bilişim suçlarına yönelik gerekli ekibini uzman kadrosunu oluşturarak bunların takibini yapılmalıdır."*
Asteğmen Burak	*"Özellikle de bu konuda emniyetin bence bu konuda gerekli seminerleri vermesi gerekiyor. Eğitim alanında olsun TSK'da olsun farklı farklı kurumlarda. Çünkü her kurumun kendine has terimleri, suçları oluyor. Ondan dolayı. O kuruma has eğitim verilmeli. TSK'da TSK'ya ait zaten genel olarak bir giriş yapıp sonrasında kurumsallaşarak seminerler verilmeli bence."*

4.1.1.10. Veri Analizinde Kullanılan Bilgi Kirliliği Kodu

Katılımcıların Bilgi Kirliliği kodu altında toplanan cevapları Tablo 4.10.'de gösterilmiştir. Katılımcılardan Albay Halit, Asteğmen Burak ve Yüzbaşı Bayram isimli TSK personelinin cevapları bilgi kirliliği kodu altında toplanmıştır. Katılımcılar sanal ortamdaki bilgilerin güvenilir olmadığını vurgulamıştır. Arama motorlarında ve internet sayfalarındaki her bilginin doğru olmadığını, isteyenin istediği bilgiyi istediği başlık altında verebildiği bu sebepten dolayı internetin bilgi güvenirliği noktasında büyük endişelerinin olduğu anlaşılmaktadır.

Tablo 4. 10. Araştırmaya Katılan TSK Personelinin Bilgi Kirliliği Kodu Altında Verdiği Cevaplar

TSK Personeli	Verilen Cevaplar
Albay Halit	*"Bir de tabi internetteki her şeyin doğru olduğuna yüzde yüz doğru bilgiler olduğuna inanmıyorum ben. Bir kişi bir konu hakkında bir sayfalık yazı yazıyor yalan dolan. Ondan sonra o konuyla ilgili ne kadar arama motorlarında arama yaparsanız yapın o sitelerde aynı bilgiler geliyor. Aynı yanlış bilgiden olabiliyor bazen."*
Asteğmen Burak	*"Veriler çok gerçekçi olmayabiliyor. Bundan dolayı dikkat etmemiz gerekiyor. Tabiri caiz ise çöplük diyorlar. İnternetteki özellikle bilgi ağlarının olduğu kısımlar çöplük diye nitelendiriliyor. Çok fazla teferruat var. Ulaşmak isteğimize zor ulaşıyoruz."*
Yüzbaşı Bayram	*"Örnek verelim bir arkadaşın eşi hamile. İnternete girdiğin zaman o kadar çok şey var ki hamilelikle ilgili. Hangisi doğru hangisi yanlış. İnsanların bu tür hassas konularda sonuçta hamile. Okuduğun her şeye kendine pay biçiyor kendine yoruyor. Sonuçta üzülüyor. Yani bu tür bilgi kirliliği fazlasıyla var."*

4.1.1.11 Veri Analizinde Kullanılan Cezai Yaptırımlar Kodu

Katılımcıların cezai yaptırımlar kodu altında toplanan cevapları Tablo 4.11.'de gösterilmiştir. Katılımcılardan Başçavuş Abdullah, Kıdemli Üstçavuş Sinan, Asteğmen Ferhat, Asteğmen Burak ve Yüzbaşı Mehmet adlı TSK personelinin cevapları cezai yaptırımlar kodu altında toplanmıştır. Ortak görüşe göre bilişim suçlarına yönelik verilen cezaların yetersiz olduğu caydırıcılık özelliğinin olmadığı

bu haliyle yasaların ihtiyaca cevap vermediği ve geliştirilmesi gerektiği noktasında hemfikir oldukları görülmektedir. Bu açıdan bakıldığında katılımcıların cezai yaptırımlar noktasında önbilgiye sahip oldukları konuya yabancı olmadıkları anlaşılmaktadır.

Tablo 4. 11. Araştırmaya Katılan TSK Personelinin Cezai Yaptırımlar Kodu Altında Verdiği Cevaplar

TSK Personeli	**Verilen Cevaplar**
Başçavuş Abdullah	*"Cezaların hafif kaldığı ve o cezalardan sonra aynı hatalara tekrardan düştüğü ve bunların önüne geçilebilmesi için cezaların arttırılması ve gerektiğinde daha farklı cezai işlemler uygulanabilir. Yani bu cezalar para cezası ile kalmamalı. Yeri geldiğinde erişimlerin engellenmesi hatta gerekiyorsa hapis cezaları verilmesi gerektiğini düşünüyorum"*
Kıdemli Üstçavuş Sinan	*"Örneğin bir internet hakkı engellenebilir bireysel olarak. Türk Ceza Kanunun 53. Maddesinden bahsedildiği gibi bir takım engellemeler konulabilir. Örneğin internet erişimi yasaklanabilir. Ne bileyim daha diğer cezai yaptırımlar para cezasıdır gibi cezalar yapılabilir."*
Asteğmen Ferhat	*"Az önce de belirttiğim gibi 5237 sayılı kanunun 243 ve ilgili maddelerinde düzenlenmiştir. Fakat cezaların alt sınırlarına ve üst sınırlarına baktığınızda bunlar adli para cezası veya 2 ila 6 yıl gibi çok düşük bir ceza öngörülmektedir. Soyut ceza öngörülmektedir. Tabi ki buna kişinin cezasal durumuna baktığımızda 231 sayılı kanunun 5. yan hükmünün açıklanmasının geri bırakılması cezası verilmekte yani kişinin resmen serbest bırakılması anlamına gelmektedir. Bu yüzden TCK'daki düzenlemeler yapılmalıdır. Cezaların soyut sınırları üst sınırları artırılmalıdır."*
Asteğmen Burak	*"Yani gerçek hayatta verilen çoğu ceza, bilişim suçlarıyla alakalı da olabilir diye düşünüyorum. Hapishane, tutukluluk, para cezası gerekirse bilişim ortamından uzaklaştırma. Psikiyatri tedavisi."*
Yüzbaşı Mehmet	*"Yani suçun nevine cinsine göre değişebilir. Çok gizli bir bilgiye ulaşıp paylaşan kişi veya hackerlik yapan kişilerle ilgili suç belli bir seviyede iken çok daha basit bilişim suçu işleyen insana kamu hizmeti veya para cezası verilebilir."*

SONUÇ ve ÖNERİLER

Gelişen ülkeler her alanda olduğu gibi siber alanda da ordular kurmakta ve siber saldırı manasında yeni siber savunma ya da siber saldırı araçları geliştirmektedir. Türk Silahlı Kuvvetleri, silahlı saldırı karşısında savunmaya ve saldırıya ne kadar hazırsa siber saldırılar karşısında da o kadar hazırlıklı olmalıdır. Bu çalışmada, ülkemizin her türlü iç ve dış savunmasından sorumlu Türk Silahlı Kuvvetlerinde görevli personelin bilgi teknolojileri kavramları çerçevesinde görüşlerini öğrenebilmek, bilişim suçlarına yönelik algıları ve bilgi alt yapısını ölçmek amaçlanmıştı. Sonuç olarak TSK personelinin bilişim teknolojilerine yatkın olduğu birçok alanda aktif şekilde kullandığı anlaşılmaktadır. Ayrıca bilişim suçlarına ve siber saldırılara yönelik tatbikatlar, bilgilendirme yazıları, merkezden bağımsız yerel eğitim faaliyetleriyle bir takım önlemlerin alındığı anlaşılmaktadır. Bu önlemlere Kara ağı ve personellerin bu ağa bağlanmak için bilgisayarlarda kullandığı kullanıcı adı ve parolası alınan güvenlik tedbirleri arasında sayabiliriz. Ancak TSK'nın personelleri için; Kara ağı ve yıllık siber savunma tatbikatlarıyla aldığı güvenlik tedbirlerinin yanında ek tedbirler alması gerektiği ortaya çıkmaktadır. Diğer taraftan siber güvenlik alanında donanımın ve yazılımın önemi vurgulanırken bütün bu altyapıyı kullanacak olan personel göz ardı edilmektedir. Kurumsal alanda güvenlik sağlamanın birinci yolu bireysel düzeyde eğitimden geçmektedir. Bu bağlamda TSK bünyesi içerisinde siber konularda eğitim almış uzman bir kadro ve eğitim ekibi oluşturulması, oluşturulan ekibin de TSK'nın her kademesindeki personele bu konuda belirli zaman dilimlerinde hizmet içi eğitim vermesi gerekmektedir. Sadece bilgisayar işletmenleriyle sınırlandırılan eğitim genele yayılmalıdır. Askeri okullarda da siber güvenlikle ilgili derslerin teorikle beraber pratiğe dayalı verilmesi personelin eğitim ve bilgi eksikliğinin giderilmesinde büyük

bir rol alacaktır. Böylelikle siber alanda eğitimli ve uzmanlaşmış bir kadro zamanla oluşacaktır. Kullanılan bilgisayarların bazı uygulamalarda donanımının ve yazılımın zayıf kalması personeli kısıtlamaktadır. Bu yüzden kurum içerisinde öncelikle altyapıyı güçlendirmek için teknik donanımın iyileştirilmesi ve yazılımların her daim güncel tutulması gerekmektedir. Bunun yanında kullanılan işletim sisteminin yerli olmaması alınan tüm tedbirlere rağmen güvenlik açığı oluşturduğu değerlendirilmektir. Uluslararası platformlarda belirlenen temel ölçütlere bağlı kalarak personellerin güvenliği için kurallar belirlenmeli; teknik ve sistematik bir güvenlik için devletin ilgili kurumları ile birlikte ortak çalışılmalıdır. E-devlet altyapısını oluşturmuş kurumlar, aralarındaki bilgi paylaşımını sağlayarak iletişim ve eşgüdüm ile siber suçlara yönelik mücadeleyi en üst düzeye çıkarmalıdır (Aydın vd., 2006).

Siber güvenliğin en önemli noktasını devlet kurumları oluşturmaktadır. Çünkü devlet tarafından hem güvenli bir ağ alt yapısı oluşturulmalı hem de bunun hukuki bir zemini sağlanmalıdır. Bu tarz suçlar konusunda bazı devletlerin olaylara ilgisiz kalmasının altında yatan temel etken de alt yapının yetersiz olması ve hukuki zeminin eksikliğidir. Ülkemizde yapılan araştırmalara göre ise Türkiye'nin siber saldırılara açık olduğu ve konunun, kamu kuruluşları tarafından yeterince ciddiye alınmadığı ortaya çıkmıştır (Bıçakçı, 2013). Araştırmamız ise bu sonucu desteklemektedir. Kanuni düzenlemeler bakımından ise mevcut hükümlerin ve cezai yaptırımların yeterli olmadığı, kanun koyucu tarafından bu konuda mevcut yasalara ek olarak özellikle siber suçlara yönelik özel bir kanunun oluşturulması gerektiği öne çıkmıştır. Sadece siber alanda görev alan yetkili birimler oluşturularak personelinin de yetiştirilmesi gerekmektedir. Yapılacak yasalar çerçevesinde siber suçlarla ilgilenen hâkim, savcı ve diğer kolluk görevlileri de birlikte hareket ederek hem suçların belgelendirilmesi hem de yakalanıp gerekli cezanın verilmesi açısından önemli bir adım olacaktır (Aydın vd., 2006). Çalışmamız kapsamında yapılan görüşmelerde de bilişim suçlarına yönelik özel bir ceza kanununun oluşturulabileceği fikri ortaya atılmıştır. Konu ile ilgili kanun maddelerinin daha kapsamlı olması, suç sayılmayan ancak siber suçlarla alakalı olup da hak ihlali oluşturan fiillerin TCK'ya alınması önerilmiştir.

Yapılan bu çalışma bilişim suçlarına yönelik algıları ve bilgi alt yapısını ölçmekte iken bundan sonra yapılacak olan çalışmalarda siber alanla ilgili eğitim ve

kanuni düzenlemeler konuları çalışılabilir. Diğer taraftan sürekli gelişme kaydeden siber alan için, bu konuda yapılacak olan çalışmalar da her zaman güncel tutularak gelişme kaydetmelidir. Çalışmamızda kullanılan görüşme yöntemi belirli bir coğrafya ve sınıftan oluşmakta ise de bundan sonra yapılacak olan çalışmalarda daha geniş yelpazede kişi sayısına ulaşarak farklı yöntemlerle de sonuca ulaşmak siber alanda yapılacak olan çalışmalara, yasal düzenlemelere ve teknik altyapının gelişmesine ışık tutacaktır. Ayrıca çalışma grubunun, ilgili kurumun bilgisayar işletmenlerinden seçilmesi yapılacak çalışmayı genelden özele indirgeyecektir.

KAYNAKÇA

Açıl, E. (2011). İlköğretim Öğretmenlerinin Etkinlik Algısı ve Uygulanışına İlişkin Görüşleri. Gaziantep: Gaziantep Üniversitesi Sosyal Bilimler Enstitüsü.

Akdağ, P. (2009). *Siber Suçlar ve Türkiye'nin Ulusal Politikası.* Ankara: Master Tezi.

Akyazı, U. (2012). Siber Hareket Ortamının Siber Güvenlik Tatbikatları Kapsamında Değerlendrilmesi. K. Canpolat, N. Bayazıt, & E. Kılınç içinde, *Siber Güvenlik* (s. 55-67). İstanbul: Harp Akademileri Basımevi.

Alpago, Ş. (2013, Haziran 23). *Cihan Haber Ajansı (CHA).* Temmuz 23, 2014 tarihinde http://www.cihan.com.tr/: http://www.cihan.com.tr/news/Guney-Kore-siber-alemde-saldiriya-ugradi-CHMTA2NjU3NS80 adresinden alındı

Andress, J., & Winterfeld, S. (2014). *Cyber Warfare Techniques, Tactics and Tools for Security Practitioners.* Waltham, MA: Elsevier.

Arseven, A. D. (1994). *Alan Araştırma Yöntemi İlkeler Teknikler Örnekler.* Ankara: Gül Yayınevi.

Asan, K. (2007). *Avrupa Birliği'nin Terörizmle Mücadelesi.* Ankara: Ankara Üniversitesi.

Atıcı, B., & Gümüş, Ç. (2003). Sanal Ortamda Gerçek Tehditler: Siber Terör. *Polis Dergisi*, 57–66.

Aydın, D. (2006). Terör Eylemlerinin Siyasal Suç Açısından Değerlendirilmesi. *Uluslararası Hukuk ve Politika*, 1-20.

Aydın, Ü., Kara, O., & Oğuz, A. (2006). Ağ Ekonomisinin Karanlık Yüzü: Siber Terör. İ. G. Yumuşak içinde, *5. Ulusal bilgi, ekonomi ve yönetim kongresi : Bildiriler Kitabı* (s. 1-14). İzmit: Kocaeli Üniversitesi İktisadi ve İdari Bilimler Fakültesi.

Bakır, E. (2013, Ocak 2). *5. Boyutta Savaş: Siber Savaşlar*. Mayıs 26, 2014 tarihinde TÜBİTAK-BİLGEM: http://www.bilgiguvenligi.gov.tr/siber-savunma/5.-boyutta-savas-siber-savaslar-ii.html adresinden alındı

Bıçakçı, S. (2013). *21.yy'da Siber Güvenlik.* İstanbul: İstanbul Bilgi Yayınevi Yayınları.

Bilgin, N. (2006). İçerik Analizi ve Metodolojisi. N. Bilgin içinde, *Sosyal Bilimlerde Nitel Araştırma Yöntemleri* (s. 11-16). Ankara: Siyasal Kitapevi.

Bircan, B. (2012). *Gelişmiş Siber Silahlar Ve Tespit Yöntemleri.* Tübitak Bilgem.

Bitdunyası. (2012, Mayıs 05). Temmuz 31, 2014 tarihinde Bilgi ve İletişim Teknolojileri Dünyası: http://www.bitdunyasi.com/tr/?Sayfa=Detay&Id=10064 adresinden alındı

BTK. (2013). *Bilgi Teknolojileri ve İletişim Kurumu 2013 Faaliyet Raporu.* Ankara: Bilgi Teknolojileri ve İletişim Kurumu.

BTK. (2014, Temmuz 1). Temmuz 2, 2014 tarihinde http://www.tk.gov.tr/: http://www.tk.gov.tr/sayfa.php?ID=328 adresinden alındı

Chip. (2009). *Tüm zamanların en ünlü 10 hackerı*. 05 11, 2014 tarihinde Chip Online: http://www.chip.com.tr/galeri/tum-zamanlarin-en-unlu-10-hacker-i_716.html adresinden alındı

Chip. (2012, Eylül 24). Temmuz 15, 2014 tarihinde chip.com.tr: 24.09.2012-http://www.chip.com.tr/haber/hacker-lar-uefı-güvenliğini –delmeyi basardi-36071.html adresinden alındı

Cnnturk. (2013, Şubat 02). Temmuz 10, 2014 tarihinde Cnnturk: www.cnnturk.com/2013/bilim.teklonoji/sosyal.medya/02/02/twitterdan.250bin.kullanıcının.Bilgisi.calındı./694915.0/index.html adresinden alındı

Çalışkan, M. (2012). Siber Saldırı Örnekleri. K. Canpolat, N. Bayazıt, & E. Kılınç içinde, *Siber G* (s. 15-31). İstanbul: Harp Akademileri Basımevi.

Defence, U. S. (2010). *Department of Defence Dictionary of Associated Terms.* Joint Chiefs of Staff.

Denning, D. E. (2001). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. J. Arquilla, & D. Ronfeldt içinde, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (s. 239-288). Georgetown: Georgetown University.

Doğan, M. (2014, Temmuz 24). *Coca Colayı kim Hackledi ?* Temmuz 31, 2014 tarihinde Mert Doğan Web Sayfası: http://mertdogan.net/coca-colayi-kim-hackledi.html adresinden alındı

Durna, Ş. D., Çalışkan, E., Gül, A. F., Onay, O., Gözükküçük, M., Taşçı, B., . . . Kaya, M. B. (2012). *Siber Güvenlik Raporu.* İstanbul: İstanbul Bilgi Üniversitesi.

Ely, M., Anzul, M., Friedman, T., Garner, D., & Steinmetz, A. (1998). *Doing qualitative research: circles within circles.* New York: Macmillan.

Erdem, L., & Enarun, D. (2011). *Aydınlatmanın Sübjektif Analizinde Kullanılan Anket Yöntemleri.* İstanbul: İstanbul Teknik Üniversitesi.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and Future of Cyber War. *Survival* (s. 23-40). içinde London: Routledge.

Ghuiglione, R., & Matalon, B. (1978). *Les Enquetes Sociologiques.* Paris: Armand-Collin.

Gibson, R., & Schuyler, E. (2006). *Google Maps Hack.* USA: O'Reily Media Inc.

Green, C., & Gilhooly, K. (1996). Protocol analysis: practical implementation. J. Richardson içinde, *Handbook of Qualitative Research Methods for Psychology and the Social Sciences* (s. 55-74). Leicester: British Psychological Society.

Günacar, G. (2011, Haziran 10). *Akıncılar Anonymous'ı hack'ledi.* Temmuz 24, 2014 tarihinde http://www.gurselgunacar.com/: http://www.gurselgunacar.com/akincilar-anonymousi-hackledi/ adresinden alındı

Gürkaynak, M., & Eren, A. A. (2011). Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler. *Süleyman Demirel Üniversitesi İktisadi ve İdari BilimlerFakültesi Dergisi*, 236-279.

Haber, M. (2012, Şubat 9). *Hacklendi; şifresi: 12345*. Temmuz 17, 2014 tarihinde Mynet: http://www.mynet.com/haber/dunya/hacklendi-sifresi-12345-615162-1 adresinden alındı

Habertürk. (2012, Eylül 5). Temmuz 15, 2014 tarihinde Habertürk Gazetesi: 05.09.2012-http://www.haberturk.com/dunya/haber/773874-el cezire-hacklendi adresinden alındı

Hekim, H., & Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi* (s. 135-158). içinde

Hildreth, S. A. (2001). *Cyberwarfare Congressional Research Service Report for Congress.* No: RL30375: Congressional Research Service & The Library of Congress.

Hürriyet. (2011, Kasım 15). Mayıs 11, 2014 tarihinde Hürriyet Gazetesi: http://www.hurriyet.com.tr/planet/21377946.asp adresinden alındı

Hürriyet. (2012, Aralık 25). Temmuz 5, 2014 tarihinde Hürriyet Gazetesi: http//hürarsiv.hürriyet.com.tr/goster/show new.aspx?id=22229501 adresinden alındı

Hürriyet. (2012, Eylül 10). Temmuz 16, 2014 tarihinde Hürriyet Gazetesi: http://hurarsiv.hurriyet.com.tr/goster/ShowNew.aspx?id=21426894 adresinden alındı

Hürriyet. (2012, Eylül 26). Temmuz 20, 2014 tarihinde Hürriyet Gazetesi: http:www.hurriyet.com.tr/teknoloj/21561577.asp adresinden alındı

Hürriyet. (2013, Temmuz 04). Haziran 15, 2014 tarihinde Hürriyet Gazetesi: http://hurarsiv.hurriyet.com.tr/goster/ShowNet.aspx?id=22987904-07.04.2013 adresinden alındı

Hürriyet. (2013, Şubat 24). Temmuz 15, 2014 tarihinde Hürriyet Gazetesi: http://hurarsiv.hurriyet.com.tr/goster/ShowNet.aspx?id=226773667 adresinden alındı

Hürriyet. (2013, Kasım 11). Temmuz 18, 2014 tarihinde Hürriyet Gazetesi: http://www.hurriyet.com.tr/teknoloji/25094002.asp adresinden alındı

Hürriyet. (2013, Mart 06). Temmuz 1, 2014 tarihinde Hürriyet Gazetesi: http://hurarsiv.com.tr/goster/ShowNet.aspx?id=22749145 adresinden alındı

Hürriyet. (2014, Temmuz 21). Temmuz 31, 2014 tarihinde Hürriyet Gazetesi: http://www.hurriyet.com.tr/teknoloji/26854331.asp adresinden alındı

İHA. (2014, Temmuz 22). Temmuz 24, 2014 tarihinde İhlas Haber Ajansı (İHA): http://www.iha.com.tr/haber-akincilardan-israil-sitelerine-siber-saldiri-375582/ adresinden alındı

iP/CyberWarrior Team, A. G. (tarih yok). *Hacked - IP/Cyber-WARRiOR Hack Team*. Temmuz 17, 2014 tarihinde www.cyber-warrior.org: http://www.cyber-warrior.org/Hacked/index.htm adresinden alındı

ITU-T, R. (2008). *Series X: Data Networks, Open System Communications and Security, Telecommunication security, Overview of cybersecurity.* International Telecomunication Union.

Jones, S. (2014, Haziran 5). *Kremlin alleged to wage cyber warfare on Kiev*. Temmuz 31, 2014 tarihinde www.ft.com: http://www.ft.com/cms/s/0/e504e278-e29d-11e3-a829-00144feabdc0.html#axzz391AbEgrt adresinden alındı

Kara, M. (2013). *Siber Saldırılar - Siber Savaşlar ve Etkileri.* İstanbul: İstanbul Bilgi Üniversitesi.

Karaarslan, E., Koç, S., & Akın, G. (2010). Vatandaşlık Numarası Bazlı E-devlet Sistemlerinde. *İzmir Bilişim Hukuku Kurultayı*, 1-8.

Kayaoğlu, H. D. (2009). İstanbul Üniversitesi Bilgi ve Belge Yönetimi Bölümü'nde Araştırma Eğilimleri 1967-2008: Lisansüstü Tezlerinin İçerik Analizi. *Türk Kütüphaneciliği, 23*(3), s. 535-562.

Keçeci, O. (2014). *Siber Suçlar ve Siber Terörizm.*

Kedikli, U. (2006). Avrupa Birliği'nin Terörizmle Mücadele Politikalari ve Hukuki Boyutu. *Uluslararası Hukuk ve Politika*, 54-79.

Klimburg, A. (2012). *National Cyber Security framework Manual.* Tallinn: NATO CCD COE Publications.

Koçak, A., & Arun, Ö. (2006). *İçerik Analizi Çalışmalarında Örneklem Sorunu* (Cilt 4). Selçuk İletişim.

Köksal, M. A., & İlbaş, Ç. (2013). *Bir İhmal Hayatinizi Nasil Degistirir*. Temmuz 23, 2014 tarihinde Teknoloji Bilinçlendirme Platformu: http://www.internetkurulu.org/images/editor/bir_ihmal_hayatinizi_nasil_degistirir.pdf adresinden alındı

Krasavin, S. (2012). *"What's Cyber Terrorism?"*. Haziran 04, 2014 tarihinde http://www.crime-research.org/lib-rary/Cyber-terrorism.htm adresinden alındı

Küçük, A., & Soğukpınar, İ. (2013). *Cyber Attacks and a Proposal for Awareness Training.*

May, T. (1996). *Social research -issues, methods and process-*. Buckingham: Open University.

Milliyet. (2013, Şubat 20). Temmuz 15, 2014 tarihinde Milliyet Gazetesi: http://ekonomi.milliyet.com.tr/facebook-unardindan–simdi-de–apple-hacklendi/ekonomi-detay/20.02.2013/1671159/default.htm adresinden alındı

Milliyet. (2013, Ekim 28). Haziran 29, 2014 tarihinde Milliyet Gazetesi: http://ekonomi.milliyet.com.tr/devlet-beyaz-saldırgan-yetistirecek/ekonomi/detay/1783213/default.htm adresinden alındı

Milliyet. (2013, Mart 19). Temmuz 27, 2014 tarihinde Milliyet Gazetesi: http://gundem.milliyet.com.tr/viruslu-mesajlarla-banka-hesaplarini-boşalttilar/gundem/gundemdetay/19.03.2013/1682387/default.htm adresinden alındı

Milliyet Gazetesi. (2013, Mayıs 29). Haziran 11, 2014 tarihinde Milliyet Gazetesi: http://dunya.milliyet.com.tr/cinliler-abd-nin-silah/dunya/detay1715625/default.htm-29.05.2013 adresinden alındı

Neuman, W. (2008). Tepkisiz Araştırma ve İkincil Analiz. *Toplumsal Araştırma Yöntemleri* (S. Özge, Çev.). içinde Ankara: Yayınodası.

Ntvmsnbc. (2012, Eylül 22). Temmuz 17, 2014 tarihinde www.ntvmsnbc.com: www.ntvmsnbc.com/id/25384168/Beyaz-Saray-siber-saldiriya-ugradi.html adresinden alındı

Oğur, G., & Tekbaş, Ö. (2003). Anket Nasıl Hazırlanır? *Sted, 12*(9), s. 336.

Olcay, E. (2013). *Siber Güvenlik.* Ankara: Bilgi Teknolojileri ve İletişim Kurumu BTD Başkanlığı.

Özcan, M. (2002). *Siber Terörizm ve Ulusal Güvenlik: İnternet ve Hukuk.* İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Özkan, T. (2006). *Siber Terörizm Bağlamında Türkiye'ye Yönelik Faaliyet Yürüten Terör Örgütlerinin İnternet Sitelerine Yönelik Bir İçerik Analizi.* Eskisehir Anadolu Üniversitesi: Master Tezi.

Özkışlalı, G. (2008). *Küreselleşme, İnternet Ve Terörizmin Değişen Yüzü; Siber Terörizm.* Ankara: Yayımlanmamış Master Tezi.

Patton, M. Q. (2002). Variety in qualitative inquiry: theoretical orientations. C. D. Laughton, V. Novak, D. E. Axelsen, K. Journey, & K. Peterson içinde, *Qualitative research & evaluation methods.* London: Thousand Oaks.

RedHack. (2013, Şubat 17). Ezber Bozanlar. (E. Erdem, Röportaj Yapan)

Robson, C. (1993). *Real World Research.* Blackwell: Oxford.

Sibersavunma. (2014, Ağustos 01). *Kilitli Kalkan (Locked Shield) Tatbikatı - 2014.* Siber Savunma Bilgi Kapısı: https://sibersavunma.tsk/icerikGoster/aspx?kaynakid=669 adresinden alındı

Stone P, J., Dunphy D, C., Marshall S, S., & Ogilvie D, M. (1966). *The General Inquirer: A Computer Approach to Content Analysis.* Massachusetts: The M.I.T. Press.

Şahin, T. (2006). *Tamer Şahin*. Ağustos 01, 2014 tarihinde Tamer Şahin Kişisel Web Sitesi: http://www.tamersahin.com/ adresinden alındı

Tavşancıl, E., & Aslan, E. (2001). *Sözel, yazılı ve diğer materyaller için içerik analizi ve uygulama örnekleri.* istanbul: Epsilon Yayınları.

TDK. (2014). *Türk Dil Kurumu.* Temmuz 15, 2014 tarihinde Büyük Türkçe Sözlük: http://tdkterim.gov.tr/bts/ adresinden alındı

Timisi, N. (2003). *Yeni İletisim Teknolojileri ve Demokrasi.* Ankara: Dost Kitabevi.

Turla, J. (2012, Mayıs 2). *Understanding the Origins of the China – Philippine Cyber War*. Temmuz 31, 2014 tarihinde www.infosecinstitute.com: http://resources.infosecinstitute.com/china-philippine-cyber-war/ adresinden alındı

TÜBİTAK. (2013, Ocak 1). Nisan 19, 2014 tarihinde http://www.tubitak.gov.tr/: http://www.tubitak.gov.tr/tr/haber/2-ulusal-siber-guvenlik-tatbikati-basariyla-tamamlandi adresinden alındı

Türkay, Ş. (2013). Siber Savaş Hukuku ve Uygulanma Sorunsalı. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 1177-1228.

Ünver, M., Canbay, C., & Mirzaoğlu, A. G. (2009). *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler.* Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı.

Wikipedia. (2012, Şubat 12). *Anonymous (hacker grubu)*. Temmuz 17, 2014 tarihinde Wikipedia, The Free Encyclopedia: http://tr.wikipedia.org/wiki/Anonymous_(hacker_grubu) adresinden alındı

Wikipedia. (2014, Mayıs 29). Temmuz 17, 2014 tarihinde Wikipedia, The Free Encyclopedia: http://tr.wikipedia.org/wiki/Bradley_Manning adresinden alındı

Wikipedia. (2014, Temmuz 17). Temmuz 18, 2014 tarihinde Wikipedia, The Free Encyclopedia: http://en.wikipedia.org/wiki/Aaron_Swartz adresinden alındı

Wikipedia. (2014, Temmuz 15). Temuz 17, 2014 tarihinde Wikipedia, the free encyclopedia: http://en.wikipedia.org/wiki/RedHack adresinden alındı

Wlingfield, T. C. (2000). *The Law of Information Conflict: National Security Law In Cyberspace 17.* Aegis Research Corp.

Yaman, H., & Erdoğan, Y. (2007). İnternet Kullanımının Türkçeye Etkileri: Nitel Bir Araştırma. *Journal of Language and Linguistic Studies, 3*(2).

Yayla, M. (2013, Ocak - Şubat). Hukuki Bir Terim Olarak "Siber Savaş". *Türkiye Barolar Birliği Dergisi*, 178-202.

Yıldırım, A., & Şimşek, H. (2006). *Sosyal Bilimlerde Nitel Araştırma Yöntemleri.* Ankara: Seçkin Yayıncılık.

Yılmaz, E. S. (2013). Uluslararası Terör İncelemelerinde Güneydoğu Asya Bölgesi. *Uluslararası Hukuk ve Politika*, 1-26.

Yılmaz, T. (2013, Haziran 21). *Hürriyet.* Haziran 21, 2014 tarihinde Hürriyet Gazetesi: http://www.hurriyet.com.tr/gundem/23557059.asp adresinden alındı

EKLER

EK A. 5237 SAYILI YTCK'DA BİLİŞİM ALANINDA SUÇLAR BÖLÜMÜNDE DÜZENLENEN SUÇ TİPLERİ

A. Bilişim Alanında Suçlar Bölümünde Düzenlenen Suç Tipleri

1. Hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma suçu (m.243)

- *Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye iki yıla kadar hapis veya adli para cezası verilir.*
- *Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir.*
- *Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, iki yıldan dört yıla kadar hapis cezasına hükmolunur.*

2. Bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçu (m.244/1-2)

3. Bilişim Sistemi Aracılığıyla Hukuka Aykırı Yarar Sağlama Suçu (m.244/4)

- *Bir bilişim sisteminin işleyişini engelleyen, bozan, sisteme hukuka aykırı olarak veri yerleştiren, var olan verileri başka bir yere gönderen, erişilmez kılan, değiştiren, yok eden kimseye bir yıldan üç yıla kadar hapis cezası verilir.*
- *Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi hâlinde, verilecek ceza yarı oranında artırılır.*
- *Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adli para cezasına hükmolunur*

4. Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (m.245)

- *Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis cezası ve adli para cezası ile cezalandırılır.*
- *Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç*

oluşturmadığı takdirde, dört yıldan yedi yıla kadar hapis cezası ile cezalandırılır.

B. Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar Bölümünde Düzenlenen Suç Tipleri

1. Kişisel verilerin kaydedilmesi suçu (m.135)

- *Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.*
- *Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır.*

2. Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu (m.136)

- *Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır.*

3. Verilerin yok edilmemesi suçu (m.138)

- *Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verilir.*

C. Bilişim Sistemleri Aracılığıyla İşlenebilecek Diğer Suç Tipleri

1. Haberleşmenin engellenmesi suçu (m.124)

- *Kişiler arasındaki haberleşmenin hukuka aykırı olarak engellenmesi halinde, altı aydan iki yıla kadar hapis veya adlî para cezasına hükmolunur.*
- *Kamu kurumları arasındaki haberleşmeyi hukuka aykırı olarak engelleyen kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.*
- *Her türlü basın ve yayın organının yayınının hukuka aykırı bir şekilde engellenmesi halinde, ikinci fıkra hükmüne göre cezaya hükmolunur.*

2. Hakaret suçu (m.125)

- *Bir kimseye onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnat eden ya da yakıştırmalarda bulunmak veya sövmek suretiyle bir kimsenin onur, şeref ve saygınlığına saldıran kişi, üç aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır. Mağdurun gıyabında hakaretin*

cezalandırılabilmesi için fiilin en az üç kişiyle ihtilat ederek işlenmesi gerekir.

- *Fiilin, mağduru muhatap alan sesli, yazılı veya görüntülü bir iletiyle işlenmesi halinde, yukarıdaki fıkrada belirtilen cezaya hükmolunur.*
- *Ceza, hakaretin alenen işlenmesi halinde, altıda biri; basın ve yayın yoluyla işlenmesi halinde, üçte biri oranında artırılır.*

3. Haberleşmenin gizliliğini ihlal suçu (m.132)

- *Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, bir yıldan üç yıla kadar hapis cezasına hükmolunur.*
- *Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.*
- *Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın alenen ifşa eden kişi, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır.*
- *Kişiler arasındaki haberleşmelerin içeriğinin basın ve yayın yolu ile yayınlanması halinde, ceza yarı oranında artırılır.*

4. Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması (m.133)

- *Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki aydan altı aya kadar hapis cezası ile cezalandırılır.*
- *Yukarıdaki fıkralarda yazılı fiillerden biri işlenerek elde edildiği bilinen bilgilerden yarar sağlayan veya bunları başkalarına veren veya diğer kişilerin bilgi edinmelerini temin eden kişi, altı aydan iki yıla kadar hapis ve bin güne kadar adli para cezası ile cezalandırılır. Bu konuşmaların basın ve yayın yoluyla yayınlanması halinde de, aynı cezaya hükmolunur.*

5. Nitelikli hırsızlık suçu (m.142)

- *Bilişim sistemlerinin kullanılması suretiyle, İşlenmesi halinde, üç yıldan yedi yıla kadar hapis cezasına hükmolunur. Suçun, bu fıkranın (b) bendinde belirtilen surette, beden veya ruh bakımından kendisini savunamayacak durumda olan kimseye karşı işlenmesi halinde, verilecek ceza üçte biri oranına kadar artırılır.*

6. Nitelikli dolandırıcılık suçu (m. 158)

- *Dolandırıcılık suçunun; bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle ve/veya basın ve yayın araçlarının sağladığı kolaylıktan yararlanmak suretiyle İşlenmesi halinde, iki yıldan yedi yıla kadar hapis ve beş bin güne kadar adli para cezasına hükmolunur.*

7. Müstehcenlik suçu (m.226)

- *Bir çocuğa müstehcen görüntü, yazı veya sözleri içeren ürünleri veren ya da bunların içeriğini gösteren, okuyan, okutan veya dinleten,*
- *Bunların içeriklerini çocukların girebileceği veya görebileceği yerlerde ya da alenen gösteren, görülebilecek şekilde sergileyen, okuyan, okutan, söyleyen, söyleten,*
- *Bu ürünleri, içeriğine vakıf olunabilecek şekilde satışa veya kiraya arz eden,*
- *Bu ürünleri, bunların satışına mahsus alışveriş yerleri dışında, satışa arz eden, satan veya kiraya veren,*
- *Bu ürünleri, sair mal veya hizmet satışları yanında veya dolayısıyla bedelsiz olarak veren veya dağıtan,*
- *Bu ürünlerin reklamını yapan, kişi, altı aydan iki yıla kadar hapis ve adli para cezası ile cezalandırılır.*

8. Kumar oynanması için yer ve imkân sağlanması suçu (m.228)

- *Kumar oynanması için yer ve imkân sağlayan kişi, bir yıla kadar hapis ve adlî para cezası ile cezalandırılır.*
- *Çocukların kumar oynaması için yer ve imkân sağlanması halinde, verilecek ceza bir katı oranında artırılır.*
- *Bu suçtan dolayı, tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.*

EK B. TSK PERSONELİNİN BİLİŞİM SUÇLARINA YAKLAŞIMI ARAŞTIRMA GÖRÜŞME FORMU

Sayın ……

Gaziantep Üniversitesi Sosyal Bilimler Enstitüsü Güvenlik Stratejileri ve Yönetimi Ana Bilim Dalı Yüksek Lisans Programında yürütülen "Türk Silahlı Kuvvetleri Personelinin Bilişim Suçlarına Yönelik Yaklaşımı" başlıklı bu çalışmayla, Türk Silahlı Kuvvetleri personelinin; bilişim suçu kavramları çerçevesinde görüşlerini öğrenebilmek, bilişim suçlarına yönelik algıları ve bilgi alt yapısını ölçmek amaçlanmaktadır.

Türk silahlı kuvvetleri personelinin bilişim suçlarına yönelik yaklaşımı, mevcut bilgi düzeyi sizin ekteki soru kâğıdına vereceğiniz yanıtlarla saptanacaktır.

Vereceğiniz yanıtlar sadece araştırma amacıyla kullanılacaktır. Araştırmaya olan katkılarınızdan dolayı teşekkür eder, görevinizde başarılar dilerim.

Ali DURDU

Yüksek Lisans Öğrencisi

TSK PERSONELİNİN BİLİŞİM SUÇLARINA YAKLAŞIMI ARAŞTIRMA SORU KÂĞIDI

Ali DURDU

Gaziantep Üniversitesi Sosyal Bilimler Enstitüsü

Güvenlik Stratejileri ve Yönetimi Ana Bilim Dalı

Yüksek Lisans Öğrencisi

1. **Kimlik Soruları**

1.1. Yaşınız:……..

1.2. Medeni haliniz:…….

1.3. Ekonomik geliriniz:……..

1.4. Eğitim durumunuz:……

□ Lise

□ Üniversite Bölümü:……

□ Yüksek Lisans Bölümü:…….

□ Doktora Bölümü:……

1.5. Meslekteki kaçıncı yılınız :……..

2. **Araştırma Soruları**

Bilgisayar Kullanımıyla İlgili Açık Uçlu Sorular

2.1. Bilgisayar deneyiminizden bize bahseder misiniz?

- **a.** Evinizde veya işyerinizde bilgisayarınız var mı?
- **b.** Günde ortalama kaç saat kullanıyorsunuz?
- **c.** Bilgisayarı ne amaçla kullanıyorsunuz (iş, eğitim, serbest zaman etkinliği vb.)?
- **d.** Bilgisayarı ne derece kullandığınızı, hangi programları kullandığınızı (Word, Excel, PowerPoint, internet tarayıcıları vb.) açıklar mısınız?

2.2. Bilgisayar kullanırken sizce dikkat edilmesi gereken hususlar nelerdir?

- **a.** Örneğin evinizdeki veya işyerinizdeki bilgisayarlarınızda kullanıcı şifresi var mı?

b. Bilgisayar programlarını kullanırken lisanslı olmasına dikkat ediyor musunuz?
c. Bilgisayarlarınızda anti virüs programları kullanıyor musunuz?

İnternet Kullanımıyla İlgili Açık Uçlu Sorular

2.3. Evinizde veya işyerinizde internet bağlantınız var mı? Varsa, evinizde veya işyerinizde hangi amaçla internete bağlanıyorsunuz (internet bankacılığı, haberleşme, sosyal paylaşım vb.)?

2.4. İnternet ortamının güvenirliği hakkında neler düşünüyorsunuz?
a. Güvenliğiniz için ne tür önlemler alıyorsunuz?
b. İnternet üzerinden alışveriş, haberleşme ve bankacılık işlemlerinde nelere dikkat ediyorsunuz?
c. İnternet ortamında kişisel bilgilerinizi ne oranda kullanıyorsunuz?
d. Adres çubuğunda yazılanlara (https, .gov, .edu, .mil vb.) dikkat ediyor musunuz?
e. İnternet ortamında şifre belirlerken nelere dikkat ediyorsunuz?
f. Farklı siteler için kullandığınız parolalar değişiklik gösteriyor mu?
g. Ne sıklıkla parola değiştiriyorsunuz?

2.5. İnternet kullanımıyla ilgili yasal düzenlemeler hakkında bilginiz var mı? Bu konudaki düşünceleriniz nelerdir?

Bilişim Suçlarıyla İlgili Açık Uçlu Sorular

2.6. "Bilişim Teknolojileri" kavramından ne anlıyorsunuz?
a. Bu kavram size neyi çağrıştırıyor?
b. Bilişim teknolojilerini ne amaçla kullanıyorsunuz?
c. Bilişim teknolojilerini kullanmanın olumlu yönleri nelerdir?
d. Bununla birlikte bilişim teknolojileri kullanımında karşılaştığınız sorunlar nelerdir?
e. Nasıl çözümler buluyorsunuz?

2.7. "Bilişim Suçları" kavramı hakkında bir bilginiz var mı? Veya siber, siber uzay, siber saldırı, siber terör, siber savaş gibi kavramlardan hangisiyle daha önce karşılaştınız?
a. Meslek içinde bilişim suçları ile ilgili herhangi bir eğitim aldınız mı?
b. "Bilişim Suçları" ile ilgili bugüne kadar düzenlenen herhangi bir konferans veya seminere katıldınız mı?
c. İşyerinizde bilişim suçlarına yönelik nasıl önlemler alındığına dair bir bilginiz var mı?

2.8. Bilişim suçlarına yönelik alınan yasal önlemler nelerdir biliyor musunuz? Ve yeterli buluyor musunuz?

a. Bilişim suçlarına yönelik verilen cezai yaptırımları yeterli buluyor musunuz?
b. Bilişim suçlarına yönelik ne tür cezalar veya yaptırımlar olabilir?

ÖZGEÇMİŞ

Ali DURDU 1985 yılında Kahramanmaraş'ta doğdu. Atatürk Üniversitesi Eğitim Fakültesi Sınıf Öğretmenliği Anabilim Dalından 2007, Anadolu Üniversitesi Kamu Yönetimi Bölümünden 2012, Anadolu Üniversitesi Adalet Bölümden 2014 yılında mezun oldu. 2009 yılında Türk Silahlı Kuvvetlerinde Subay olarak göreve başlamıştır ve halen görev yapmaktadır.

VITAE

Ali Durdu was born in 1985 in Kahramanmaraş. He graduated from Atatürk University Education Faculty Classroom Teacher Training Department in 2007, Anadolu University Public Administrations Department in 2012, Anadolu University Law Department in 2014. He started his job as an officer in Turkish Armed Forces in 2009 and is currently on duty.