ULUSAL VE ULUSLARARASI BOYUTLARIYLA SİBER GÜVENLİK

Mustafa ÜNVER
munver@btk.gov.tr

Cafer CANBAY
ccanbay@btk.gov.tr

1. Giriş

Bireyler, toplumlar ve devletlerin öncelikli ve ortak hedefi; var olmak, kendini korumak, kendine karşı oluşabilecek tehlikelere karşı tedbirler almak, varlığını sürdürebilmek; kısacası güvenliğini sağlamaktır. Bu itibarla güvenlik, insanoğlunun hiçbir surette vazgeçemeyeceği bir ihtiyaçtır. İnsanoğlu güvenliği için tarih boyu pek çok defalar temel hak ve hürriyetlerinden feragat etmiş ve bu hak ve hürriyetlerinin sınırlanmasına dahi izin vermiştir[1].

Klasik güvenlik anlayışı çerçevesinde bireyler, toplumlar ve devletler, kendileri için hayati önem taşıyan güvenliği sağlayabilmek için hukuki düzenlemeler yapmış, ordular ve polis teşkilatları gibi kurumlar oluşturmuş, güvenlik ihlallerine karşı silahlanma gibi tedbirler almışlardır. Ancak, hayat dinamiktir ve sürekli bir değişim içindedir. Dinamik bir hayatta statik bir anlayışla güvenliğin sağlanması da mümkün değildir. Politik, ekonomik, sosyal, kültürel ve teknolojik gelişmeler güvenlik anlayışını da etkilemekte ve bu etkiye bağlı olarak alınacak tedbirlerin de değiştirilmesini gerektirmektedir.

1990 sonrası Bilgi ve İletişim Teknolojilerinin (BİT) hızla gelişmesi, 2000'li yıllarla birlikte BİT'lerin tüm dünya çapında yayılması, buna paralel olarak gerek kamu gerekse de özel kesimin uygulamalarını elektronik ortama aktarmaları, hayatı bir anlamda BİT'lere bağımlı hale getirmiştir. İnsanoğlu için çok büyük yararlar sağlayan bu gelişmelerin kötü niyetli bazı kişiler tarafından suiistimal edilmesi, siber ortamın tehdit, saldırı, cana ve mala zarar verme gibi amaçlarla kullanılması ve siber saldırılar dolayısıyla kişilerin ve ülkelerin gördüğü zararların büyük boyutlara ulaşması güvenlik anlayışında değişikliklere yol açmış ve siber güvenlik konusu bireylerin, kurumların, ülkelerin ve uluslar arası kuruluşların gündeminin en önemli gündem maddelerinden biri haline gelmiştir.

Bu çalışmada, günümüzün en önemli sorunlarından biri haline gelen siber güvenlik konusu ele alınacaktır. Öncelikle, BİT'lerin ve e-uygulamaların gelişimi ile kritik altyapılar üzerinde durulacak, müteakiben siber tehdit araçları ve bunların gelişimi hususlarına değinilecektir. Siber güvenliğin sağlanması için atılması gereken zorunlu adımların değerlendirilmesinden sonra Bilgi Teknolojileri ve İletişim Kurumu

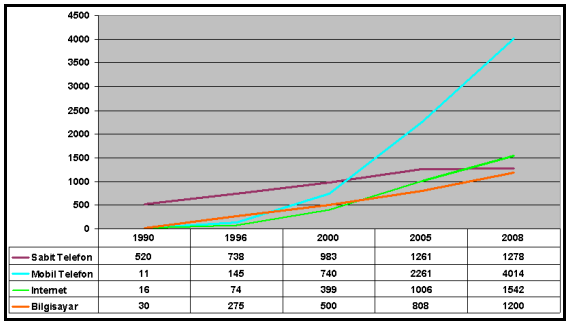
[1] Canbay, C., Güvenliğin Sağlanmasında İletişimin Rolü, E-Akademi, Eylül 2009, Sayı 91.

(BTK)'nun siber güvenlik konusundaki çalışmaları hakkında bilgi verilecektir.

2. Bilgi ve İletişim Teknolojilerinin Gelişimi

İnsan yaşamının en önemli unsurlarından biri iletişimdir. İnsanoğlu tarih boyunca farklı yöntemler ve araçlar kullanarak iletişim sağlamıştır. Duvarlara çizilen resimlerden ve dumanla haberleşmeden, posta güvercini ve ulak kullanmaya kadar bir dizi yöntem kullanarak haberleşen insanoğlu 19. yüzyılda önce telgrafın sonra da telefonun icadıyla elektronik ortamda haberleşmeye başlamıştır. 20. yüzyılın ilk yarısında radyo ve televizyonun icadı ile de kitlesel iletişim sağlanmaya başlamıştır. Bununla birlikte insanoğlunun yaşamını en fazla etkileyen ve değiştiren araçlar ise 20. yüzyılın ikinci yarısında bilgisayarların, mobil iletişim araçlarının ve İnternetin icadı ile bu araçların 1990'lardan sonra hızla ticarileşerek gelişmesi ve tüm dünya çapında yayılması olmuştur. Bu yayılmaya paralel olarak dünyamız milyonlarca kilometre uzunluğunda fiber optik kablo ile kaplanmış ve bine yakın uydu ile çevrelenmiştir.

BİT'lerin günümüzdeki kullanım verilerine bakıldığında bu yayılımın ne boyutlara ulaştığı rahatlıkla görülebilmektedir (Şekil 1).



	1990	1996	2000	2005	2008
Sabit Telefon	520	738	983	1261	1278
Mobil Telefon	11	145	740	2261	4014
İnternet	16	74	399	1006	1542
Bilgisayar	30	275	500	808	1200

Şekil 1. Elektronik Haberleşme Araçlarının Kullanımı[2]

[2] ITU, Açık İstatistikler, http://www.itu.int/ITU-D/icteye/Indicators/Indicators.aspx

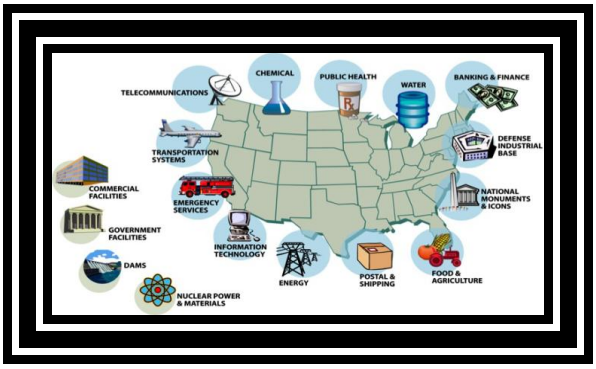
BİT'lerin yaygınlaşması ve kullanımının artışıyla birlikte klasik usullerle yapılan iş ve işlemler elektronik ortama aktarılmaya ve insanoğlunun yaşamında büyük köklü değişiklikler meydana gelmeye başlamıştır. Mektupların yerini elektronik posta almıştır. Bankacılık işlemleri, sermaye piyasalarının takibi, vergi ve fatura ödemeleri, sınav ve pasaport başvuruları, araç tescil işlemleri, günlük gelişmelerin izlenmesi, otel ve seyahat ayarlamaları ve daha pek çok iş ve işlem herhangi bir yere gitmeye, zaman kaybetmeye ve bir maliyete katlanmaya gerek kalmadan, bulunulan mekânda ve çok kısa bir zaman içinde elektronik ortamda yapılabilir hale gelmiştir. Fiziksel alanın yerini siber alana bırakmasıyla zamana ve mekana bağlılık önemli ölçüde azalmış, doğallığın yerini teknoloji ve hiyerarşik yapının yerini demokratik yapı almaya başlamıştır. Kısacası günümüzde yaşam BİT'lere bağımlı hale gelmiştir ve bu bağımlılık da giderek artmaktadır.

Bu gelişmeler bir yandan insanoğlunun yaşamını ciddi oranda kolaylaştırıp rahatlaştırırken diğer yandan da "siber güvenlik" başta olmak üzere bir kısım sorunların ortaya çıkmasına yol açmaktadır. Özellikle kritik altyapıların günümüzde tamamıyla BİT'lere bağımlı hale gelmesi gerek bireyler gerek ülkeler gerekse de uluslar arası toplum açısından hayati önem arz etmektedir.

3. Kritik Altyapılar ve Türkiye

Kritik altyapılar, Avrupa Komisyonu tarafından, zarar görmesi veya yok olması halinde, vatandaşların sağlığına, emniyetine, güvenliğine, ekonomik refahına ve hükümetin etkin ve verimli işleyişine ciddi olumsuz etki edecek, fiziki ve bilgi teknolojileri tesisleri, şebekeler, hizmetler ve varlıklar olarak

tanımlanmaktadır[3]. ABD tarafından 17 (Şekil 2) ve AB tarafından ise 11 (Şekil 3) sektör kritik olarak belirlenmiştir[4].



Şekil 2. ABD'nin Kritik Altyapıları

Şekil 3. AB'nin Kritik Altyapıları

Kritik altyapıların neler olduğu ülkeden ülkeye değişmekle birlikte, çoğunlukla kamu idaresi, sağlık, BİT, ulaştırma, bankacılık ve finans, enerji, acil hizmetler, gıda ve su ile savunma sektörlerinin kritik sektör olduğu kabul edilmektedir[5]. Farklı ülkeler tarafından belirlenmiş olan kritik altyapıların tamamı esas itibariyle BİT'lere bağımlı olduğundan BİT'lerin en kritik altyapı olduğu değerlendirilmektedir.

Ülkemizdeki duruma bakıldığında henüz bu konuda sonuçlanmış bir çalışma bulunmadığı ve kritik sektörlerin belirlenmediği görülmektedir. Bununla birlikte, ülkemizde gerek doğal gaz, petrol, su ve elektrik nakil şebekelerinin, barajların, hava kontrol sistemlerinin, sağlık hizmetlerinin BİT'lere bağımlı hale gelmesi gerekse de son yıllarda sayıları gittikçe artan UYAP, MERNİS, ASAL, TAKBİS ve MEBBİS gibi vatandaşlara ait büyük miktarda bilgi içeren bilişim sistemlerinin geliştirilmesi ülkemizin diğer ülkelerden farklı olmadığını ve bahse konu altyapıların ülkemiz açısından da kritik olduğunu göstermektedir.

4. Siber Tehdit, Tehlike ve Saldırılar

Siber ortamda gerek bireyler gerek toplumlar gerekse de ülkeler açısından çok hayati bilgilerin yer alması, siber ortamı kötü niyetli kişi, kurum ve devletler için açık bir hedef haline getirmiştir. Kötü niyetli bu taraflar;

- ✓ Virüsler
- ✓ Kurtçuk (worm)
- ✓ Truva atı (trojan)
- ✓ Zombi ve Botnetler
- ✓ Yemleme (phishing)
- ✓ İstem dışı elektronik posta (spam)
- ✓ Hizmetin engellenmesi saldırıları (DoS, DDoS)
- ✓ Klavye izleme yazılımları (key logger)
- ✓ Casus / köstebek yazılımlar (spyware)
- ✓ Şebeke trafiğinin dinlenmesi (sniffing ve monitoring)

gibi araçlar ve yöntemler kullanarak 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[6].

[3] Avrupa Komisyonu, "Terörle Mücadelede Kritik Altyapıların Korunması", 20.01.2004, Brüksel, s. 3 http://ec.europa.eu/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf

[4] Canbay, C., Kritik Altyapıların ve Sektörlerin Korunması, IstSec 2009 Konferansı, İstanbul, http://www.istsec.org/

[5] ITU, "Siber Güvenliğe Ulusal Yaklaşım üzerine En İyi Uygulamalar Raporu, Ulusal Siber Güvenlik Çalışmalarının Organize Edilmesi için bir Yönetim Çerçeve Modeli", Ocak 2008, s. 6

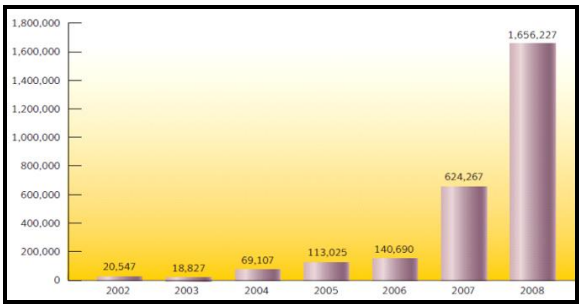
[6] BTK, Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler,

Konu ile ilgili yapılan araştırmalar siber ortamdaki tehdit, tehlike ve saldırıların korkunç boyutlara ulaştığını gözler önüne sermektedir. Araştırmalar;

- "I Love You" adlı virüsün dünya çapında yaklaşık 45 milyon bilgisayara bulaştığını ve yaklaşık 10 milyar USD'lik zarara sebep olduğunu,
- "Nimda" kurtçuğunun dünya çapında yaklaşık 3 milyar USD'lik, "Love Bug"ın ise 10 milyar USD'lik zarara sebep olduğunu,
- "MyDoom" adlı truva atının 4,8 milyar USD civarında zarara sebep olduğunu,
- "Sapphire/Slammer" solucanının 2003'te internete bağlı bilgisayarların % 90'ına 10 dakika içinde bulaştığını,
- 2005'in ilk altı ayında zarar gören bilgisayar sayısı bir önceki yıla göre % 63 arttığını,
- ABD'li tüketicilerin son iki yılda bilgisayar tamiri ve yenilemesi için 7.8 milyar USD harcadığını,
- Güvenlik yazılımlarının pazar payının yıllık % 16 civarında arttığını

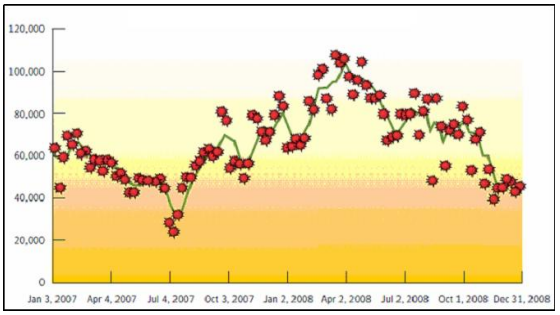
göstermektedir[7].

Symantec verilerine göre 2002 yılında 20 bin dolayında olan zararlı yazılım sayısı, 2008 sonu itibariyle 1.65 milyonu aşmıştır[8] (Şekil 4).



Şekil 4. Zararlı Yazılımların Artışı

Sayıları hızla artan zararlı yazılımlar siber ortamda bilgisayarlara ve bilişim sistemlerine farkedilmeden yüklenmekte ve bunları sahibinin bilgisi ve rızası dışında kullanılan zombi adı verilen bilgisayarlara dönüştürmektedir. Symantec'in verilerine göre günlük olarak zombi hale getirilen bilgisayar sayısı 2008 yılında 20 bin ile 110 bin arasında değişmiştir[9] (Şekil 5).



Şekil 5. Zombi Bilgisayar Sayısının Günlük Artışı

Zombi bilgisayarlar biraraya getirilerek oluşturulan "botnet" adı verilen yapıların sayısı artmakta, bu botnetlerce kontrol altında tutulan bilgisayar sayısı büyümekte ve kontrol altındaki bilgisayarlar dünyanın dört bir yanından olabilmektedir. Günümüzde bilinen en büyük botnet 300 bin civarında bilgisayarı yönetme kapasitesine ulaştığı tespit edilen Srizbi adlı botnettir (Şekil 6). Srizbi'den sonraki en büyük botnetler 180 bin civarında bilgisayarı kontrol ettiği düşünülen Torpig ve 150 bin civarında bilgisayarı kontrol ettiği düşünülen Rustogdur[10].

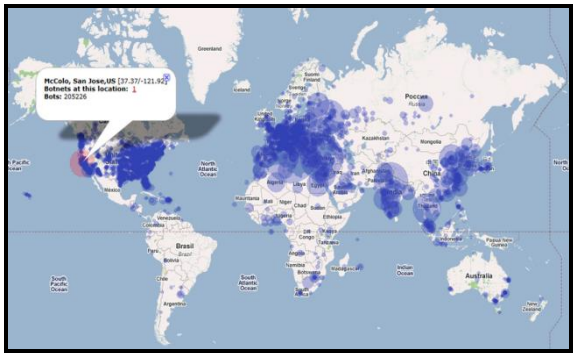
2009, s. 8, http://www.btk.gov.tr/bt/sg/dokumanlar/sg.pdf

[7] Beydoğan, T. A., Canbay, C., Siber Güvenliğin Sağlanması ve Kritik Bilgi ve Altyapıların Korunması: Gelişmekte Olan Ülkeler İçin Yol Haritası, 17. ITS Konferansı, Montreal – Kanada, 24 – 27 Haziran 2008, s. 4 – 5

[8] Symantec, Internet Güvenliği Tehdit Raporu 2008 Eğilimleri, Sayı 14, Nisan 2009, s. 7

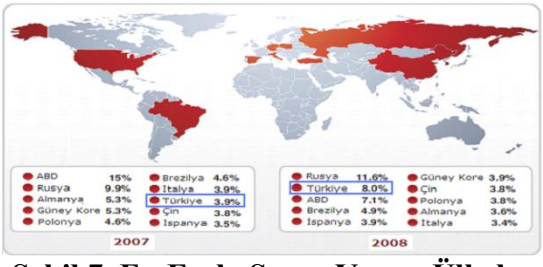
[9] Symantec, Kamu İnternet Güvenliği Tehdit Raporu 2008 Eğilimleri, Sayı 14, Nisan 2009, s. 33

[10] Bkz.: Yuk. 9, s. 35



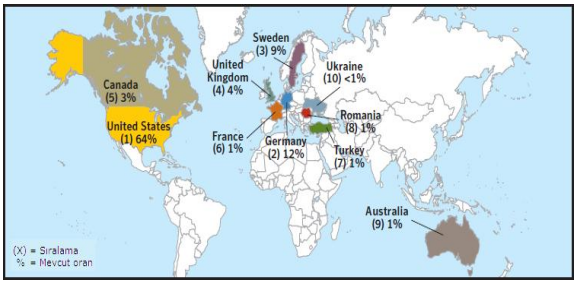
Şekil 6. Srizbi Botnetine Bağlı Zombi Bilgisayarların Dağılımı (17/11/2008 itibariyle)
(Kaynak:http://www.fireeye.com)

Zombi bilgisayar ve botnetler, onları kontrol eden kişilerce, farklı amaçlarla kullanılabilmektedir. Bu amaçların başında pek çok ülkede yasaklanan ve suç olarak belirlenen istekdışı elektronik posta gönderme gelmektedir. İstekdışı elektronik postalar genelde virüs, solucan, truva atı gibi kötücül yazılımların yayılımını sağlamak, yemleme yapmak ve hizmetin engellenmesi saldırılarını gerçekleştirmek amacıyla kullanılmaktadır. Günümüzde dünya elektronik posta trafiğinin % 87'sini istekdışı elektronik postalar oluşturmaktadır[11]. İstekdışı elektronik postaları yayan ülkelere bakıldığında ülkemizin en önde gelen ülkelerden olduğu görülmektedir[12] (Şekil 7).



Şekil 7. En Fazla Spam Yayan Ülkeler

İstekdışı elektronik postalar kullanılarak, kötücül yazılımlar yayılmakta, kötücül yazılımların bulaştığı bilgisayarlar zombiye dönüşmekte, zombi bilgisayarlar kullanılarak kişilere ait özel bilgiler çalınmakta ve bu bilgiler yer altı siber ekonomide alınıp satılmaktadır. Bu bilgilerin başında da kredi kartı bilgileri, banka hesap bilgileri, e-posta hesap bilgileri ve vatandaşlık numaraları gibi bilgiler gelmektedir[13]. Yer altı siber ekonomide pay sahibi ülkelere bakıldığında ülkemizin % 1'lik oranda dünya sıralamasında 7. sırada olduğu görülmektedir[14] (Şekil 8).



Şekil 8. Yer Altı Siber Ekonomide Pay Sahibi Ülkeler

Gerek en fazla istekdışı elektronik posta yayan ülkelerden gerekse de yer altı siber ekonomide önem pay sahibi olması dolayısıyla ülkemiz hem kötü amaçlı siber faaliyetlerin hem de hükümetlere yönelik saldırıların kaynağı olan ülkelerin başında gelmektedir. Symantec verilerine göre ülkemiz bu sıralamalarda dünyada 9. gelmektedir[15].

Ülkemizin siber tehdit ve saldırı araçlarına kaynaklık etmesi ülkemizdeki bilişim suçlarının artışına da yol açmaktadır. Örneğin, 2003 yılında kayıtlı bir bilişim suçu ve dolandırıcılığı olmamasına rağmen 2008 yılına geldiğimizde 560 olayın gerçekleştiği ve şüpheli kişi sayısının 842'ye çıktığı görülmektedir[16].

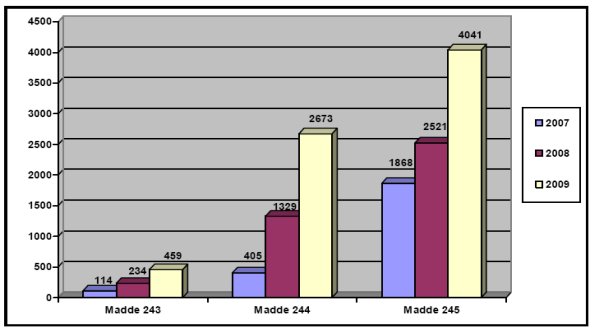
---

[11] Symantec, Spam Durumu Aylık Raporu, Kasım 2009, s. 1
[12] IBM, İnternet Güvenlik Sistemleri 2008 Eğilim ve Risk Raporu, Ocak 2009, s. 65
13 Bkz.: Yuk. 8, s. 6
[14] Symantec, İnternet Güvenlik Tehditleri Raporu, 2007, Sayı 12, Eylül 2007, s. 42
[15] Bkz.: Yuk. 9, sf. 15 – 19
[16] EGM, KOM Faaliyet Raporları, 2003 – 2008, http://www.kom.gov.tr/Tr/KonuDetay.asp?id=12&BKey=61

Olay Türü	2003		2004		2005		2006		2007		2008	
	Olay	Şüpheli	Olay	Şüpheli	Olay	Şüpheli	Olay	Şüpheli	Olay	Şüpheli	Olay	Şüpheli
Kredi Kartı Sahteciliği ve Dolandırıcılığı	80	268	146	422	195	543	310	468	594	907	830	991
Banka Dolandırıcılığı	15	49	22	72	9	33	723	1398	642	1187	1177	2114
Bilişim Suçları ve Dolandırıcılığı	0	0	16	31	91	179	178	283	416	764	560	842
Diğer					560		7	60	91	134	157	416
Toplam	95	317	184	525	855	755	1218	2209	1743	2992	2724	4363

Şekil 9. Olay ve Şüpheli Sayısındaki Gelişme

Türk Ceza Kanununda bilişim suçlarını düzenleyen 243, 244 ve 245. maddelerden açılan dava sayısının 2007 – 2009 döneminde katlanarak artması da ülkemizde bilişim suçlarının hızla arttığını ortaya koymaktadır[17].



Şekil 10. Bilişim Suçları ile İlgili Açılan Dava Sayıları

Bahsekonu bilişim suçları genel itibariyle küçük çaplı suçlardır. Bununla birlikte siber tehdit ve saldırı araç ve yöntemleri kullanılarak kritik altyapılara yönelik büyük saldırılar yapıldığı, bu altyapıların kontrolünün saldırganlarca ele geçirildiği, bu altyapıların çalışamaz hale getirildiği ve bu altyapılarda yer alan bilgilerin çalındığı da bilinmektedir. Bu hususta;

- 1998 yılında Kosova'yı işgal eden Sırplara yönelik ABD – NATO hava harekatı öncesinde Sırbistan Hava Savunma Sistemlerinin kontrolü ele geçirilmesi ve sistemin kilitlenmesi[18],
- 14 Aralık 2007'deki seçimler sırasında Kırgızistan Merkezi Seçim Komisyonun sistemlerine saldırı düzenlenmesi ve sistemlerin çalışamaz hale getirilmesi[19],
- Nisan 2008'de Der Spigel BND'nin Afganistan Sanayi ve Ticaret Bakanlığının tüm elektronik iletişimini casus yazılımlar kullanarak izlediğini haber yapması ve bu nedenle iki ülke arasında ilişkilerin gerilmesi[20],
- Mayıs 2008'de Hindistan'ın, Ulusal Bilişim Merkezi ve Dış İşleri Bakanlığının Çin tarafından izlediğini tespit ettiğini açıklaması,
- Mayıs 2008'de Belçika'nın kamu sistemlerine sızıp espiyonaj yapmakla Çin'i itham etmesi,
- Eylül 2008'de Güney Kore'nin casus yazılımlar kullanarak bilişim sistemlerine sızma ve gizli bilgilerini çalmakla Kuzey Kore'yi suçlaması,
- 4 Temmuz 2009 tarihinde Çin ve Kuzey Kore kaynaklı saldırılar ile ABD'nin ve Güney Kore'nin bir çok bilişim sisteminin kilitlenmesi ve hizmet dışı kalması,
- Eylül 2009'da Pentagon'un Çin Ordusunu bilişim sistemlerine saldırmakla suçlaması[21] ve
- Brezilya ve Paraguay'ın ortaklaşa kullandıkları Itaipu Barajı ve Hidroelektrik santraline 10 Kasım 2009'da yapılan saldırı ile barajın çalışamaz hale getirilmesi ve iki

[17] Adalet Bakanlığı, Ulusal Yargı Ağı Projesi, 2009, Ankara

18 Hancock, B., "Güvenlik Bakışları", Computers & Security, Sayı 18, 1999, s. 553 – 64

[19] Regnum, Kırgız Merkezi Seçim Komisyonunun İnternet Sitesi Estonyalı Hackerlarca Engellendi, 14 December 2007, http://www.regnum.ru/english/932354.html

[20] Der Spiegel, Alman Ajanlar Afgan Bakanlığı İzledi, 26 Nisan 2008, http://www.spiegel.de/international/germany/0,1518,549894,00.html

[21] Wikipedia, Siber Savaş, http://en.wikipedia.org/wiki/Cyberwarfare

ülkenin büyük bölümünün 22 saat karanlıkta kalması[22]

örnek olarak verilebilir.

Kritik altyapılara yönelik siber saldırılara ek olarak ülkeler arasındaki gerilimler ve savaşlar dolayısıyla siber ortamda da topyekün saldırı ve savaşlar cereyan edebilmektedir. İsrail – Filistin, Çin – Tayvan, Pakistan – Hindistan, Estonya – Rusya ve Gürcistan – Rusya arasındaki siber savaşlar bunun en güncel örneklerini teşkil etmektedir. Bu örnekler arasında yer alan Estonya – Rusya savaşı gerek ülkelerin gerekse de uluslararası kuruluşların siber tehdit ve saldırılara bakışını topyekün değiştirmiştir. 2007 yılında Estonya'nın başkenti Talinn'de bulunan Rus Meçhul Asker anıtının yerinin değiştirilmesi üzerine kamu hizmetlerinin çok büyük bölümünün elektronik ortamda verildiği Estonya'daki bilişim sistemlerine yönelik siber saldırılar başlamış ve temelde kamu hizmetlerini hedef alan bu saldırılar dolayısıyla Estonya'da hayat durma noktasına gelmiştir. Saldırılar karşısında çaresiz kalan Estonya Hükümeti NATO'yu göreve çağırmış ve bu çağrı üzerine NATO Estonya'da Siber Güvenlik Mükemmeliyet Merkezi kurmuştur[23]. Benzer bir durum 2008 yılında Gürcistan – Rusya savaşı sırasında Gürcistan'da yaşanmış ve benzer sonuçlar doğurmuştur.

5. Siber Güvenliğin Sağlanması

Siber güvenlik, siber ortamda, **kurum, kuruluş ve kullanıcıların varlıklarını korumak** amacıyla kullanılan

- araçlar,
- politikalar,
- güvenlik kavramları,
- güvenlik teminatları,
- kılavuzlar,
- risk yönetimi yaklaşımları,
- faaliyetler, eğitimler, en iyi uygulamalar ve
- teknolojiler bütünü

olarak tanımlanmaktadır. Siber güvenliğin temel amaçları da gizlilik, bütünlük, erişilebilirlik, inkâr edilemezlik ve kimlik doğrulama sağlamaktır[24].

Gerek kişilere gerek kritik altyapılara gerekse de topyekün bir şekilde ülkelere yönelik siber tehdit ve saldırıların artması ve bunların büyük mali kayıplarla birlikte kamu düzeni ve güvenliğini etkileyecek noktaya gelmesi konunun gerek ulusal gerek bölgesel gerekse de uluslararası kurum ve kuruluşlarca ele alınmasını gerektirmiştir. Bu gereklilik dolayısıyla 1990'ların sonlarında başlayan siber güvenlik çalışmaları son yıllarda hızla artmaktadır.

5.1 Siber Güvenliğin Unsurları

Bu konuda yapılan çalışmalar siber güvenlik çalışmalarının 8 önemli unsuru olduğunu ortaya koymaktadır. Bunlar:

1. Ulusal politika ve stratenin geliştirilmesi
2. Yasal çerçevenin oluşturulması
3. Teknik tedbirlerin geliştirilmesi
4. Kurumsal yapılanmanın belirlenmesi
5. Ulusal işbirliği ve koordinasyonun sağlanması
6. Kapasitenin geliştirilmesi
7. Farkındalığın artırılması
8. Uluslararası işbirliği ve uyumun sağlanmasıdır[25]

Bu 8 unsura kısaca değinmekte yarar görülmektedir.

22 Foreign Policy Journal, Brezilya'nın Gelecek Savaş Alanı: Siber Alan, 15 Kasım 2009, http://www.foreignpolicyjournal.com/2009/11/15/brazils-next-battlefield-cyberspace/

23 The Guardian, Rusya Estonya'ya Karşı Siber Savaşla Suçlanıyor, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia

[24] ITU, ITU_T X.1205 sayılı Tavsiye Kararı, Siber Güvenliğe Genel Bakış, 2008

[25] Bkz.: Yuk. 7, s. 41

Ulusal politika ve stratenin geliştirilmesi

Bir ülkede bireylerin, sivil toplum kuruluşlarının, özel sektörün ve kamu kesiminin siber güvenlik konusunda yapacakları çalışmalardan istenilen sonuçların alınabilmesi ve bu çalışmaların başarılı olabilmesi için bunların belli bir hedef doğrultusunda, belli bir anlayışla ve birbirlerini tamamlar şekilde yapılması önem arz etmektedir. Bunun sağlanabilmesi için de tüm taraflara yol gösterici mahiyette bir ulusal politika ve bu politika çerçevesinde hazırlanmış bir strateji gerekmektedir.

Yasal çerçevenin oluşturulması

Siber tehdit ve saldırıların, genellikle cana ve mala etki eden, sonuçları olmaktadır. Siber güvenliğin sağlanmasında bu sonuçların ve bu sonuçlara yol açan fiil ve yöntemlerin suç olarak tanımlanması ve cezalandırılması, özellikle siber saldırganların caydırılması noktasında, büyük önem arz etmektedir. Teknolojik gelişmelere paralel olarak siber saldırı araç ve yöntemlerinin değiştiği de göz önünde bulundurularak ülke mevzuatının gözden geçirilmesi gerek esasa gerekse de usule ilişkin varsa eksikliklerin giderilmesi gerekmektedir.

Teknik tedbirlerin geliştirilmesi

Siber güvenliğin sağlanması noktasında hukuki tedbirler gereklidir ancak yeterli değildir. Herşeyin hukuktan, yargıdan ve kolluk kuvvetlerinden beklemek de doğru bir yaklaşım olarak görülmemektedir. Bu itibarla, özellikle yazılım, donanım ve iş süreçlerinin kalitesinin artırılarak daha güvenli kılınması gerekmektedir. Bunun için de ISO/IEC 15408 ve TS ISO/IEC 27001 gibi güvenlik standartlarının, benzer nitelikteki teknik rehber ve kılavuzların geliştirilmesi, uygulanması ve kullanılması sağlanmalıdır. Yazılım, donanım ve iş süreçlerinin daha güvenli kılınmasının siber saldırganları caydırıcı etki yaratabileceği ve suçla mücadelede önleyiciliği sağlayabileceği de göz önünde bulundurulmalıdır.

Kurumsal yapılanmanın belirlenmesi

Bir ülkede siber güvenliğin sağlanması için bireylere, sivil toplum kuruluşlarına, özel sektöre ve kamu kurum ve kuruluşlarına düşen görev ve sorumluluklar bulunmaktadır. Dolayısıyla siber güvenliğin sağlanması tüm tarafların işidir. Ancak bu çalışmaların başarıya ulaşabilmesi için siber güveniliğin bir tarafın **"birinci işi"** olması önem arz etmektedir. Asıl görevi siber güvenliği sağlamak olan bu kamu kurumunun görev ve sorumlulukları ile diğer paydaşlarla nasıl çalışacağı hususları yasal açıdan net olarak belirlenmelidir. Bu kurumun görevlerini layıkı veçhile yapabilmesi için gerekli olan idari, mali ve teknik imkan ve kabiliyetler sağlanmalıdır.

Ulusal işbirliği ve koordinasyonun sağlanması

Siber güvenliğin sağlanmasında tüm paydaşların kendilerine göre rol ve sorumlulukları bulunmaktadır. Her bir paydaş kendi güvenliği için müstakil çalışmalar yapabilir ve bu çalışmaları kısmen de olsa başarılı olabilir. Ancak günümüzde farklı paydaşlarca kullanılan sistemler, şebekeler ve altyapıların tamamı birbirine bağlı ve bağımlıdırlar. Bu itibarla, bunların tamamının güvenliği sağlanmadan hiçbirinin güvenli olduğu söylenemez. Topyekün güvenliğin sağlanabilmesi için de ulusal politika ve strateji göz önüne alınarak sorumlu kurum ve kuruluşun da katkılarıyla tüm paydaşlar arasında işbirliği ve koordinasyon sağlanmalıdır.

Kapasitenin geliştirilmesi

Teknolojik gelişmelere bağlı olarak yeni siber tehditler, araçlar ve yöntemler ortaya çıkmaktadır. Yeni durum karşısında yeni

politikalar, yasalar, standartlar, ürünler, çözümler gerekebilmektedir. Bu itibarla politika belirleyicilerin, hukukçuların (hakim, savcı, avukatlar), yazılım, donanım ve uygulama geliştiricilerin kapasitelerinin geliştirilerek yeni ve olası güvenlik sorunlarına ilişkin çalışmalar yapmaları ve çözümler geliştirmeleri sağlanmalıdır. Ayrıca, siber suçların niteliği de teknolojik gelişmelerle birlikte değiştiğinden yeni suçlar ve suçlularla etkili bir şekilde mücadele edilebilmesi için hakim ve savcılar ile bu suçlara ilişkin soruşturma yapan, delilleri toplayan kolluk güçlerinin de teknik ve idari kapasiteleri geliştirilmelidir.

Farkındalığın artırılması

Yine teknolojik gelişmelerle birlikte siber saldırı araçları ve yöntemleri geliştiğinden ve sürekli olarak yenilendiğinden son kullanıcı vatandaşlarımızın siber tehditler, riskler, saldırılar ve güvenlik önlemleri konusunda sürekli olarak bilgilendirilmeleri ve bu konuda farkındalık ve bilinç düzeylerinin yükseltilmesi gerekmektedir. Bu amaçla eğitim kuruluşları ve kitle iletişim araçları etkin bir şekilde kullanılmalıdır.

Uluslararası işbirliği ve uyumun sağlanması

İnternet, ağların küresel ağıdır. Günümüzde bireysel, kurumsal ve ulusal tüm altyapı, sistem ve şebekeler de bu ağa bağlı ve bağımlıdır. Bu ağın güveniliğinin tam olarak sağlanabilmesi de ancak uluslararası işbirliği ve uyum ile mümkündür. A ülkesinde yerleşik bir kişi, B, C, D ve E ülkelerindeki sistemleri kullanarak F ve G ülkelerine siber saldırı gerçekleştirebilmektedir. Bu tür saldırıların tespit edilmesi, önlenmesi, araştırılması ve soruşturulması için ülkeler arasında işbirliği gerekmektedir. İşbirliği çerçevesinde mevzuatların ve suç soruşturma ve kovuşturma usullerinin uyumlu hale getirilmesi, bilgi paylaşım mekanizmalarının oluşturulması gibi çalışmalar yapılmalıdır. İşbirliği mekanizması dışında kalan ülkelerin siber saldırı merkezlerine dönüşmesi riski bulunduğundan tüm ülkelerin bu mekanizma kapsamına alınması sağlanmalıdır.

5.2 Siber Güvenlik Çalışmalarında Dikkat Edilecek Noktalar

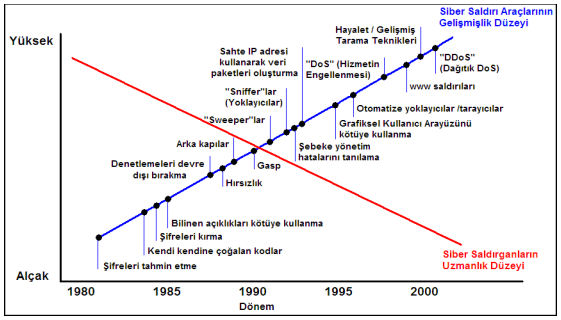
Gerek bireyler gerekse de devletler açısından hayati önem taşıyan "güvenlik" söz konusu olduğunda akan suların durabildiği bir realitedir. Bu durum zaman zaman suiistimalere yol açmakta ve güvenlik gerekçe gösterilerek temel hak ve hürriyetlerin ortadan kaldırılması veya sınırlandırılması başta olmak üzere aşırı bazı çaba ve uygulamalar ortaya çıkabilmektedir. Bu tür çaba ve uygulamalara mahal verilmemesi, istenilen sonuçlara ulaşılabilmesi ve ortaya işler bir sistemin konulabilmesi için siber güvenlik çalışmalarının belirli ilkeler doğrultusunda yürütülmesi gerekmektedir. Bu ilkeler kısaca;

- Temel hak ve hürriyetlerinin korunması
- Demokratik toplum düzeninin gereklerine uyulması
- Ölçülülük İlkesine uyulması
- Karar alma süreçlerine tüm paydaşların katılımının sağlanması
- Bütüncül bir yaklaşımla hukuki, teknik, idari, ekonomik, politik ve sosyal boyutların ele alınması
- Güvenlik ile kullanılabilirlik arasında denge kurulması
- Diğer ülke mevzuatlarının göz önünde bulundurulması ve mümkün olabildiğince uyumluluğun sağlanması
- Uluslararası işbirliğinin sağlanması

olarak ifade edilebilir[26].

[26] Bkz.: Yuk. 6, s. 23

Siber güvenlik çalışmalarının başarıya ulaşması için klasik tehditler ile siber tehditler arasındaki farklara ve siber ortamın kendi hususiyetlerine dikkat edilmesi gerekmektedir. bu noktada dikkat edilmesi gereken birinci husus zaman içinde daha az bilgi ile daha komplike saldırıların gerçekleştirilebilir hale gelmesidir. 1990 öncesinde şifre kırma, kendi kendini çoğaltan kodlar geliştirme, arka kapılar bulma gibi basit yöntemler için dahi çok yüksek düzeyde bilgi gerekirken günümüzde DDoS saldırıları, botnet kurma ve yönetme gibi karışık ve zor uygulamalar çok az bir bilgi ile yapılabilmektedir[27].



Şekil 11. Siber Saldırgan Bilgi Düzeyi – Siber Saldırı Gelişmişliği

Dikkat edilmesi gereken ikinci zorluk siber saldırıları yapan kişileri ve bu saldırıların yapıldığı yerleri tespit etmektir. Klasik tehditlerin ve bu tehditlerin kaynaklandığı yerlerin tespiti günümüzde çok da zor olmamaktadır. Örneğin, biyolojik, kimyasal veya nükleer silah tesisinin yeri, kapasitesi, tehlike boyutu günümüzde tespit edilebilmektedir. Oysaki siber saldırıları gerçekleştirenlerin elektronik ortamda kişilerin kendilerini saklayabilmelerine olanak sağlayan anonimleştirici programlar kullanmaları sebebiyle tespit edilebilmesi çok zor olmaktadır. Mobil iletişim teknolojilerinin varlığı ve sürekli gelişmesi ve botnetler gibi binlerce farklı yerdeki kontrolü ele geçirilmiş bilgisayarlar kullanılarak saldırıların gerçekleştirilebilmesi sebebiyle bu saldırılar herhangi bir mekana bağlı olmamakta ve saldırı merkezi kavramını anlamsızlaşmaktadır.

Bu konuda dikkat edilmesi gereken üçüncü nokta ise siber saldırıların erişim gücü ve menzilidir. Klasik saldırı araçlarının belli bir kapasitesi ve menzili vardır ve araçlar bu menzil içinde bir tehlike oluşturabilmektedir. Örneğin, bir füze ancak menzili içindeki şehirler, ülkeler ve bölgeler için tehdit oluşturabilmektedir. Füze gibi klasik saldırı araçlarının menzillerinin ve etkilerinin artırılabilmesi için çok ileri düzey bilgi ve tecrübe ile milyar dolarlar seviyesini bulabilen ekonomik güç gerekmektedir. Oysaki siber saldırı araçları günümüzde, yukarıda da değinildiği üzere çok az bir bilgi ve para ile geliştirilebilmekte ve internet üzerinden dünyanın doğusundan batısına, kuzeyinden güneyine her noktaya bu araçlar kullanılarak siber saldırılar gerçekleştirilebilmektedir. Bu itibarla, siber güvenlik açısından ulusal veya uluslararası boyut şeklinde bir ayrım çok anlamlı değildir.

Yukarıda ifade edilen ilkeler ve dikkat edilmesi gereken hususlar göz önünde bulundurulmadan yapılacak siber güvenlik çalışmalarının arzulanan sonuçlara ulaşmayı sağlamayacağı düşünülmektedir.

6. BTK'nın Faaliyetleri

BTK'nın siber güvenlik ile ilgili çalışmaları 3 başlık altında ele alınabilir:

1. Düzenleme ve denetleme faliyetleri,
2. Projeler,
3. Kapasite geliştirme ve farkındalık oluşturma çalışmaları.

Siber güvenliğin sağlanması noktasında büyük önem arzeden konulardan biri elektronik imzadır. Elektronik imzanın önemi elektronik ortamda bütünlük, kimlik

[27] Bkz.: Yuk. 6, s. 31

doğrulama, inkar edilemezlik ve gizlilik sağlamasıdır ki bunlar aynı zamanda siber güvenliğin amaçlarıdır. BTK, elektronik imza konusunda düzenleyici ve denetleyici kurumdur. Kurum, 5070 sayılı Elektronik İmza Kanununun çıkmasından sonra;

- Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik ve
- Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliği

hazırlayarak Resmi Gazete'de yayımlatmıştır. Elektronik imza ile ilgili düzenleyici çerçevenin oluşturulması sonrasında BTK'ya bildirimde bulunan ve gerekli şartları sağladıkları tespit edilerek faaliyete geçen dört Elektronik Sertifika Hizmet Sağlayıcı (ESHS) bulunmaktadır. Bunlar, Tübitak – KSM, E – Güven A. Ş., Turk Trust A. Ş. ve E – Tuğra A. Ş.'dir[28]. 2005 yılından sonra ülkemizde kullanımı başlayan elektronik imza e-devlet ve e-ticaret uygulamalarının azlığı dolayısıyla fazla kullanım alanı bulamamıştır. Ancak, BTK'nın 2008 yılında mobil elektronik imza ile ilgili düzenlemeleri tamamlamasından sonra mobil elektronik imza kullanımı ülkemizde hızla artmıştır. BTK, teknolojik gelişmeler çerçevesinde elektronik imza mevzuatını güncellemekte ve ESHS'leri periyodik olarak denetlemektedir.

BTK'nın konu ile ilgili ikincil bir düzenlemesi de Elektronik Haberleşme Güvenliği Yönetmeliği'dir. 20 Temmuz 2008 tarihli ve 26942 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren Yönetmelik ile elektronik haberleşme sektöründe faaliyet gösteren İşletmecilere varlıklarını belirleme; bu varlıklara ilişkin tehditler, zafiyetler ve riskleri tespit etme; fiziksel alan güvenliği, veri güvenliği, donanım-yazılım güvenliği ve personel güvenilirliği ile ilgili tedbirler alma yükümlülükleri getirilmiştir. İşletmecilere, ayrıca, 20 Temmuz 2010 tarihine kadar TS/ISO 27001 Bilgi Güvenliği Yönetim Sistemi belgesi alma şartı getirilmiştir. Böylece, İşletmecilerinin iş süreçlerinin geliştirilmesi ve altyapı, sistem ve hizmetlerinin daha güvenli hale getirilmesi sağlanacaktır.

BTK'nın üçüncü önemli düzenlemesi ise 6 Şubat 2004 tarihli ve 25365 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik'tir. "Kişisel veri" ve "kişisel verilerin işlenmesi" kavramlarının tanımlandığı, gizliliği sağlanacak verilerin belirlendiği, "trafik verisi" ve "yer verisi" gibi önemli kişisel verilerin işlenmesi ile ilgili hususların netleştirildiği, spam haberleşmenin düzenlendiği ve elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin konu ile ilgili hak ve yükümlülüklerinin belirlendiği bu Yönetmelik ile özellikle siber güvenliğin bir alt unsuru olan bilgi güvenliğinin sağlanması noktasında önemli gelişmeler kaydedilmektedir.

BTK'nın düzenleyici ve denetleyici faaliyetlerine ek olarak 2009 yılı içinde geliştirip uyguladığı "Spam ile Mücadele Projesi" Kurumca yapılan diğer bir önemli çalışmadır. TTNET, Çizgi Telekom, Doruknet ve Mynet başta olmak üzere çok sayıda işletmecinin katılımı ve katkılarıyla gerçekleştirilen proje çerçevesinde şebeke seviyesinde 25. port kullanıma kapatılıp onun yerine daha güvenli olan 587. port kullanıma sokulmuştur[29]. Proje sonucunda TTNET'in dünyaya yaydığı günlük spam mesaj sayısı 6.5 milyar düzeyinden 400 milyon düzeyine inmiş ve ülkemiz en çok spam yayan ülkeler sıralamasında oldukça alt sıralara düşmüştür. Bu itibarla, proje arzulanan hedeflerine ulaşmıştır.

[28] BTK, Elektronik İmza – Genel Bilgi, 2010, http://www.btk.gov.tr/bt/elektronikimza.htm

[29] TTNET, Şimdi E-posta Kutunuz Daha Güvenli!, www.ttnet.com.tr

BTK, siber ortamda en büyük tehlikelerden biri haline gelen zombi-botnet konusunu 2010 yılı çalışma takvime almış ve bu konuda ilgili paydaşlarla birlikte yütüteceği bir projenin hazırlık çalışmalarını başlatmıştır.

Kurum, kapasitenin gelişimine ve farkındalığın artırılmasına katkıda bulunmak üzere;

- Siber Güvenliğinin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler ve
- Uluslararası Kuruluşların Siber Güvenlik Faaliyetleri

başlıklı raporları hazırlayarak ilgili kurum ve kuruluşlarla birlikte kamuoyu ile paylaşmıştır. "Yemleme (Phishing)" ve "Botnet – Zombi" başlıklı raporların hazırlıkları kurum bünyesinde devam etmekte olup, 2010 yılının ilk çeyreğinde bu raporların tamamlanarak kamuoyu ile paylaşılması planlanmaktadır. Aynı saiklerle BTK, Bilgi Güvenliği ve Kriptoloji Konferansı başta olmak üzere çok sayıda etkinliğe katılmakta ve katkıda bulunmaktadır[30].

Tüm bu çalışmalara ilave olarak BTK, muhtelif kurum ve kuruluşlarca yapılan siber güvenlik ile ilişkili çalışmalara katılım ve katkı sağlamaktadır. Ulusal Bilgi Güvenliği Mevzuat Hazırlık Çalışmaları, E-Devlet ve Bilgi Toplumu Kanun Tasarısı ile Ulusal Sanal Ortam Güvenlik Politika Esaslarını belirleme çalışmaları bu çalışmalara örnek olarak verilebilir.

BTK, gerek kendisince gerekse de ülkemizde yapılan siber güvenlik ile ilgili çalışmaları ve kaydedilen gelişmeleri Uluslararası Telekomünikasyon Birliği ve Internet Yönetişim Forumu başta olmak üzere uluslararası platformalara taşımakta ve ilgili taraflarla paylaşmaktadır.

7. Sonuç

BİT'lerin gelişimine ve kullanımının artışına paralel olarak klasik usullerle yapılan iş ve işlemler elektronik ortama aktarılmaya başlanmış; bu amaçla e-devlet ve e-ticaret uygulamaları geliştirilmiştir. Bu e-uygulamalar ticari ve kamusal süreçleri elektronik ortama bağlı ve bağımlı hale getirmiştir. Teknolojik gelişmelere ve bu teknolojilerin kullanımının yaygınlaşmasına paralel olarak bu bağımlılık önümüzdeki yıllarda katlanarak artacaktır.

Günümüzde belli bir artış trendi izlese de hayatın akışını çok ciddi biçimde olumsuz etkileyecek siber saldırılar gerçekleşmemiştir. Ancak gelecek yıllarda, dünyamız büyük oranda e-dünyaya dönüştüğünde gerçekleştirilecek siber saldırıların hayal dahi edilemeyecek boyutta cana ve mala zarar vermesi kuvvetli bir olasılık olarak görülmektedir. Bu itibarla, gelecekte kıyamet senaryosu benzeri kötü durumlarla karşılaşmamak için bugünden siber güvenlik konusunda tedbirlerin alınmasında yarar görülmektedir.

Alınacak tedbirlerin başarılı olabilmesi için bunların küresel çapta olması gerekmektedir. Küresel çapta işbirliği ve koordinasyon sağlanarak ortak algı, anlayış ve kabullerin oluşturulması, sorunların önlenmesi, önlenemese dahi ortaya çıktıktan sonra hızla ve asgari zararla çözülebilmesi noktasında büyük önem arz etmektedir. Bu itibarla, tüm ülkelerin taraf olacağı sözleşmeler marifetiyle küresel bir hukuki çerçeve geliştirilmesi, bu hukuki çerçeve içinde yargı ve kolluk birimlerinin hızlı ve etkin çalışabilmelerinin temin edilmesi hayati önemi haizdir.

Küresel yaklaşım doğrultusunda Ülkelerin

- Ulusal politika ve stratejilerini geliştirmeleri,
- Bu politikalar çerçevesinde düzenlemeler ve standartlar hazırlamaları,

[30] BTK, Siber Güvenlik / Çalışmalar, http://www.btk.gov.tr/bt/sg/sgcalismalar.htm

- Siber tehdit, saldırı ve suçlarla mücadele amaçlı kurumsal yapılarını oluşturmaları ve bu kurumsal yapıların birbirleriyle uyumlu çalışmalarını sağlamaları,
- Teknolojik gelişmelere paralel olarak politika belirleyicilerin, yargı temsilcilerinin, kolluk güçlerinin, yazılım – donanım – hizmet üreticilerinin kapasitelerini sürekli geliştirecek mekanizmalar kurmaları,
- Son kullanıcıları siber tehdit ve saldırılar ile güvenlik önlemleri konusunda sürekli bilgilendirici ve bilinçlendirici mekanizmalar tesis etmeleri

siber güvenliğin sağlanabilmesi açısından zorunlu görülmektedir.