Estonya 2007 Siber Saldırılarının İncelenmesi ve Ülkelerin Ulusal Siber Güvenlik Politikalarına Etkileri

An Examination of Estonia 2007 Cyber Attacks and the Effects on National Cyber Security Policies of Countries

Esma DİLEK
Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Bilgi Güvenliği Mühendisliği ABD Doktora Öğrencisi, esma.dilek@gazi.edu.tr

Özgür TALİH
Bandırma Onyedi Eylül Üniversitesi, Fen Bilimleri Enstitüsü, Akıllı Ulaşım Sistemleri ve Teknolojileri ABD Yüksek Lisans Öğrencisi, ozgurtalih@ogr.bandirma.edu.tr

Türksel KAYA BENSGHİR
Hacı Bayram Veli Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, İşletme Bölümü Öğretim Üyesi, t.bensghir@hbv.edu.tr

Bilgi Yönetimi Dergisi

Cilt: 6 Sayı: 2 Yıl: 2023

https://dergipark.org.tr/tr/pub/by

Hakemli Makaleler

Araştırma Makalesi

Makale Bilgisi

Gönderildiği tarih: 17.11.2023
Kabul tarihi: 25.12.2023
Yayınlanma tarihi: 31.12.2023

Article Info

Date submitted: 17.11.2023
Date accepted: 25.12.2023
Date published: 31.12.2023

Anahtar Sözcükler

Estonya, Siber Saldırı, Siber Savunma

Keywords

Estonia, Cyber Attack, Cyber Defense

DOI numarası

10.33721/by.1392577

ORCID

0000-0002-7994-0294 (1)
0000-0002-5899-2511 (2)
0000-0002-2313-5325 (3)

Öz

Siber saldırılar, dijitalleşmiş ve bilgi toplumuna dönüşen ülkelerde, ulusal güvenlik açısından dikkate alınması gereken önemli hususlar arasındadır. Geleneksel fiziksel saldırılardan farklı olarak siber saldırıların ne şekilde meydana geleceği, hangi saldırı yüzeylerini kullanacağı ile hangi hedeflere yöneleceği konuları beklenmedik şekillerde ve çeşitliliktedir. Siber dünyada meydana gelen savaşların sonuçları farklı boyutlarda öngörülemeyen etkilere sahip olabilmektedir. Bu durumun dünyada ses getiren örneklerinden biri, 2007 yılında Estonya'ya yönelik olarak meydana gelmiştir. Avrupa'nın en teknolojik ülkelerinden olan Estonya, o tarihe kadar tek bir ülkeye yönelik düzenlenen, koordineli, en kapsamlı siber saldırılardan birine maruz kalmıştır. Gelişmiş siber savunma yeteneklerine sahip olmanın önemini vurgulayan, Estonya'ya yönelik bu siber savaş dalgası, ulusal güvenliğin sağlanması için siber güvenlik alanında odaklanılması gereken konuları gün yüzüne çıkarmıştır. Bu çalışmada, 2007 yılında Estonya'ya düzenlenen siber saldırılar, bu saldırıların nedenleri, hedefleri, ulusal ve uluslararası etkileri, alınan siber savunma önlemleri, saldırılar sonrasında öğrenilmiş dersler incelenmiştir. Bu dersler ışığında, Uluslararası Telekomünasyon Birliği (ITU) Küresel Siber Güvenlik İndeksinde üst sıralarda yer alan ülkelerin ve Türkiye'nin güncel siber güvenlik politikaları değerlendirilmiştir.

Abstract

Cyber-attacks are among the major issues that need to be taken into consideration in terms of national security in countries that are digitalised and transforming into an information society. Unlike traditional physical attacks, the manner in which cyber attacks will occur, which attack surfaces they will use, and which targets they will be directed towards are unpredictable and varied. The consequences of attacks in the cyber space can have unpredictable effects in various dimensions. One of the most prominent examples of this issue in the world occurred in 2007 against Estonia. Estonia, one of the most technological countries in Europe, was exposed to one of the most coordinated, comprehensive cyber-attacks ever organised against a single country. This wave of cyber attacks against Estonia, which emphasised the importance of having advanced cyber defence capabilities, highlighted the issues that need to be focused on in the field of cyber security to ensure national security.

**Bu makalenin araştırma ve yayın süreci "Araştırma ve Yayın Etiğine" uygun şekilde yürütülmüştür.*

In this study, the cyber-attacks against Estonia in 2007, the reasons, targets, national and international effects of these attacks, the cyber defense measures taken, and the lessons learned after the attacks were examined. In the light of these lessons, the current cyber security policies of Türkiye and the countries ranked high in the International Telecommunication Union (ITU)'s Global Cyber Security Index were evaluated.

1. Giriş

Bilgi çağında, internet, dünya çapındaki ara bağlantı ve iletişimde etkileyici derecede büyük artışların olmasını kolaylaştırmıştır. Bu küreselleşme biçimi, gelişmekte olan dünyada yaşam standartlarının iyileştirilmesi gibi faydalar sağlamış, ancak aynı zamanda belirli siyasi önlemlere ve ideolojilere karşı çıkmak isteyen gruplar için yeni direniş silahlarının ortaya çıkmasına yol açmıştır. Bu silahlar, dijital aktivistler tarafından Nisan ve Mayıs 2007'de, Estonya'ya karşı yapılan siber saldırılarda kullanılmıştır. Estonyalılar için zulmün simgesi, Sovyetler için ise Nazilerden kurtuluşu ifade eden Bronz Asker heykelinin, Tallinn'in merkezinden alınarak daha az görünür bir yere taşınması kararı sonrasında, Nisan 2007'de, Rusça konuşan azınlıklar arasında ayaklanmalar ortaya çıkarak Estonya'nın kritik ekonomik ve siyasi altyapısını hedef alan siber terörizm tetiklenmiştir (Herzog, 2011). Estonya, 2007'nin Nisan ve Mayıs aylarında, 22 gün süren, devlet kurumlarını ve ticari kuruluşları hedef alan ülke çapında (Crandall, 2014) koordineli, siber saldırılarla karşı karşıya kalmıştır (Kaska, Talihärm, & Tikk, 2010).

Saldırılar, Estonya'nın güvenlik açıklarını ortaya çıkarmış ve siber saldırıların istendiğinde çok daha kalıcı hasarlara neden olma potansiyeli olduğunu göstermiştir. Bu olaylar aynı zamanda, Estonya'nın siber saldırılara karşı koymadaki yeteneklerini ve direncini de ortaya çıkarmıştır. Siber saldırının neden olduğu şok, Estonya, Avrupa Birliği ve NATO (North Atlantic Treaty Organization)'daki siber savunma yeteneklerinin, kurumların altyapılarının ve mevzuatın önemli ölçüde güçlendirilmesi için tetikleyici olmuştur (Thematic Area, 2007). Estonya'ya yönelik siber saldırılar; küreselleşme, karşılıklı bağımlılık ve dijital bağlanabilirlik çağında, yıkıcı internet saldırılarına ve bunların etkilerine karşı koymak ve önlemler almak için artan iş birliğine dayalı siber savunma faaliyetlerinin yürütülmesi gerektiğini (Herzog, 2011), kamu ve özel sektör faaliyetlerinin büyük bir kısmının internete dayalı olarak yürütüldüğü bir ülkede siber saldırıların çok ciddi zararlar verebileceğini ortaya koymuştur (Jackson, 2013).

Bu çalışmada, 2007 Estonya siber saldırılarının nedenleri, gelişimi, aktörleri, saldırılar sonrasında yaşanan gelişmeler, saldırıların etkileri, saldırılardan öğrenilen dersler, ülkelere tavsiyeler, siber saldırıların sonuçları ve değerlendirmeler ele alınmış, Estonya'ya yönelik siber saldırılar, farklı boyutlarıyla incelenerek bu saldırılardan öğrenilen dersler ışığında, ITU Küresel Siber Güvenlik İndeksinde üst sıralarda yer alan ülkelerin ve Türkiye'nin güncel siber güvenlik politikaları değerlendirilmiştir. Çalışmada, öncelikle 2007 Estonya siber saldırılarına genel bir bakış yapılmış, ardından bu saldırıların ulusal ve uluslararası etkileri, saldırılara karşı verilen yanıtlar ve saldırılar sonrasında ulusal ve uluslararası arenada yaşanan gelişmeler, bu saldırılardan Estonya'nın ve uluslararası kuruluşların ve ulus devletlerin öğrendikleri derslere ve tavsiyelere yer verilmiştir. Bu kapsamda, siber güvenlik alanında önemli bir milat oluşturan Estonya siber saldırılarından öğrenilen derslerden yola çıkarak günümüzün ulusal siber güvenlik politikaları incelenerek değerlendirilmiştir.

2. Estonya 2007 Siber Saldırıları

Estonya, 2007 yılında kamu kurumlarına ve özel sektör kuruluşlarına karşı eşi görülmemiş miktarda eşgüdümlü (Kaska vd., 2010), "siber şiddet" türüne maruz kalmıştır (Buresh, 2020). Esas olarak hizmet reddi (DoS, Denial of Service) ve dağıtık hizmet reddi (DDoS, Distributed Denial of Service) saldırılarını içeren siber saldırılar, Tallinn merkezindeki Tõnismägi Parkı'nda bulunan Sovyet II. Dünya Savaşı anıtının, Tallinn Merkez Mezarlığına taşınarak yerinin değiştirilmesi kararı ile tetiklenmiştir. Estonya'nın devlet kurumları, bankaları, medya kuruluşları ve özel kurumların internet siteleri hedef alınmıştır. Saldırılar sırasında, Estonya dışından kaynaklanan ve devlet kurumlarını hedef alan veri trafiği, normal veri trafiğinden yüzlerce kat daha fazla olmuştur. Saldırıların yoğunluğu veya hedef seçimi tamamen emsalsiz olmasa da kapsamı, miktarı, birleştirilen saldırıların süresi ve kullanılan koordinasyon tarzı, tek bir ulus devletin deneyimlediği, benzerleriyle karşılaştırılamayacak boyutta olmuştur. Bu nedenle, bu siber saldırılar dünya çapında hızla dikkat çekmiştir (Kaska vd.,

2010). Saldırılar 27 Nisan 2007'de başlamış, üç hafta devam ettikten sonra 18 Mayıs 2007'de sona ermiştir (Buresh, 2020).

Bu ilk önemli siber saldırı, Estonya için normal yaşam koşullarının aksamasına ve ekonomik maliyetlerin oluşmasına neden olmasına rağmen, hiçbir zaman geri dönüşü olmayan ve kalıcı hasarlara yol açmak amaçlanmamıştır. Siber silahlar kullanılarak finansal transferler, haberler, e-posta gibi veri akışını kesintiye uğratarak bir devletin etkin bir şekilde tecrit edilebileceği görülmüştür. Yaşanan siber saldırılar, izolasyonun hiçbir uyarı olmadan başlatılabileceğinin ve manevra yapılmasının imkânsız olabileceğinin örneği olmuştur (Thematic Area, 2007). Estonya, medyada yaygın olarak "siber savaş" olarak belirtilen ve Estonya Cumhurbaşkanı'nın "Birinci Web Savaşı" olarak tanımladığı, büyük ölçekli DDoS saldırılarına maruz kalan ilk ulus devlet olmuştur (Haataja, 2017). Saldırılar, Estonya'nın ağlarını daha güvenli hale getirmek için tasarlanmış yasal düzenlemelerden, Siber Güvenlik Stratejisi ve Siber Savunma Ligi'nin oluşturulmasına kadar uzanan bir dizi köklü politika değişikliğinin fitilini ateşlemiştir (Jackson, 2013). Saldırılar, bir ulus devlete ve genel olarak bilgi teknolojisine giderek daha fazla bağımlı hale gelen modern bilgi toplumlarına yönelik siyasi amaçlı ve koordineli siber saldırılar hakkında, uluslararası farkındalığı artırma ihtiyacına güçlü bir şekilde dikkat çekmiştir (Ottis, 2008).

2.1. Saldırıların Arka Planı

Estonya, II. Dünya Savaşı öncesinde, önemli sayıda etnik Rus'un yaşadığı, savaşın başı ve sonrasındaki dönemde Sovyet Sosyalist Cumhuriyetler Birliği (SSCB)'nin bir uydu devleti olmuştur. Savaştan sonra Estonya, Moskova tarafından, Rusya doğumlu Estonyalı valiler aracılığıyla yönetilmiştir (Czosseck, Ottis, & Talihärm, 2011). Estonya'ya yönelik siber saldırılar ise Rusya ile yoğun siyasi çatışmaların olduğu bir zamana denk gelmiştir. Estonya 1990'da Sovyetler Birliği'nden ayrılarak bağımsızlığını yeniden kazandıktan sonra siyasi, ekonomik, politik, sosyal, kültürel alanlarda Sovyet etkisinden kurtulma ile ilgili çabaları ifade eden de-Sovyetleşme (Zhu, 2023) sürecine ve modernleşme dönemine girmiştir. Bu durum Estonya'da yaşayan etnik Rus azınlıklar için zaman zaman gerilim oluşturan bir süreç olmuştur (Jackson, 2013).

Bronz Asker heykeli hakkındaki anlaşmazlık, 1991'de Estonya'nın diğer birçok uydu devlet gibi Sovyet boyunduruğundan kurtulmasıyla ortaya çıkmıştır. Etnik Rus azınlığa göre bu heykel, Estonya'daki meşruiyetlerinin ve haklarının bir simgesidir. Ancak bu heykel, bazı Estonyalılar için Sovyetlerin baskısını ve ülkenin acımasızca ele geçirmesini temsil ettiğinden, 2006'da Tallinn Belediye Meclisine, heykelin yıkılmasına yönelik dilekçe verilmiştir. Söz konusu heykel için karar verme süreçleri devam ederken sokak isyanları baş göstermiş, mağazaların yağmalanması ve mülklerin tahrip edilmesi gibi ölümcül ayaklanma ve yağmalara dönüşen fiziksel saldırılar söz konusu olmuştur. Estonya hükümeti konuyu kapatmak ve ayaklanmayı dağıtmak için bronz heykeli sökmeye karar vermiştir (Jackson, 2013).

Olayların patlak verdiği 27 Nisan 2007 Cuma günü, birkaç Estonya hükümet yetkilisi iş yerinde e-postalarına erişememiş, Microsoft Outlook tabanlı sistemler e-posta gönderip alamamış ve genel ağ bağlantısı yavaşlamıştır. Bu tür olaylar oldukça yaygın ve genellikle kısa süreli olduğundan, birçok Estonyalı yetkili, hatanın birkaç dakika veya saat içinde düzeltileceğini düşünmüştür. Ancak günler ve haftalar geçtikçe, Estonya'nın bir dizi siber saldırı altında olduğu ortaya çıkmıştır (Jackson, 2013).

Siber saldırıların yanı sıra, Moskova'daki Estonya büyükelçiliğinde de dikkat çekici olaylar yaşanmıştır. Kremlin yanlısı gençlik grupları, günlerce iyi organize edilmiş ve donanımlı protestolar düzenlemiş ve zaman zaman Estonya büyükelçiliği çalışanlarının ve diplomatların binaya girmesini veya binadan çıkmasını engellemiştir. 2 Mayıs'ta Estonya büyükelçisi, bir basın toplantısı sırasında fiziksel saldırıya uğramıştır (Ottis, 2008).

Diğer yandan 2007 yılında eyalet çapında siber saldırıların düzenlendiği dönemde, Estonya, toplumun her alanında bilgi ve iletişim teknolojisinin (BİT) kullanımı konusunda Avrupa'nın en gelişmiş ülkelerinden biriydi. Çok çeşitli ticari faaliyetleri yürütmek için internet üzerinden yapılan işlemler yaygın bir uygulamaydı ve hâlâ da öyledir. Ülkede, tüm bankacılık işlemlerinin %99'u elektronik ortamda yapılmakta ve kamu hizmetleri e-hizmet olarak internet üzerinden sunulmaktadır. Dünyadaki ilk çevrimiçi parlamento seçimleri Estonya tarafından yapılmıştır. Ancak doğal olarak, bir toplum

BİT'e ne kadar bağımlıysa, siber saldırılara karşı o kadar savunmasız hale geldiğinden (Czosseck vd., 2011), Estonya siber saldırılarının etkisi yoğun ve şiddetli olmuştur.

2.2. Saldırıların Hedefleri ve Kullanılan Yöntemler

Sosyal güvenlik ve vergi beyanlarına kadar birçok kamusal hizmete, internet tabanlı dijital çözümleri entegre eden Estonya, 2007 yılında siber saldırı tehditlerine karşı savunmasız hale gelmiştir. Kamu ve özel sektör ile İnternet Servis Sağlayıcıları (ISP, Internet Service Provider) dahil olmak üzere çeşitli Estonya internet siteleri, siber saldırıların hedefi olmuştur. Ayrıca, ulusal Alan Adı Hizmeti (DNS, Domain Name Service) ve çeşitli ISP'ler tarafından işletilen DNS'ler gibi Estonya'nın internet altyapısı ve bilgi sistemleri hedef alınmıştır (Haataja, 2017). Bu saldırıların, iletişim altyapısı unsurlarını ve erişilen çevrim içi hizmetleri adreslediği görülmektedir.

Siber saldırganlar, Estonya hükümeti, şirket ve kurumlarına karşı şu yöntemleri kullanarak saldırılar gerçekleştirmiştir (Thematic Area, 2007), (Buresh, 2020): (i) DDoS saldırıları, (ii) İnternet Kontrol Mesaj Protokolü (ICMP, Internet Control Message Protocol) taşkınları, (iii) Web sitesi tahribatı, (iv) DNS sunucuları saldırıları, (v) İstenmeyen toplu e-postalar. Ayrıca, SQL (Structured Query Language) enjeksiyonu gibi sistemlere sızmak için daha karmaşık birkaç girişimde daha bulunulmuştur. Bu saldırıların bazıları, kritik olmayan sitelerde başarılı olmuştur (Ottis, 2008). Kullanılan saldırı yöntemlerinin bilişim altyapısını bozma, kesintiye uğratma, aksatma, durdurma gibi etkileri görülmüştür.

2.3. Siber Saldırıların Aşamaları ve İlerlemesi

Siber saldırılar ilk olarak 27 Nisan 2007'de başlamıştır. Bilgisayar korsanları, 29 Nisan'da, iktidardaki Reform Partisi'nin internet sitesine sızarak ziyaretçileri farklı alıntılara yönlendirme yöntemiyle diğer web sitelerini manipüle etmiştir (Jackson, 2013). İkinci aşama 4 Mayıs'ta başlamış ve saldırılar yabancı ülkelerde bulunan vekil (proxy) sunucularından yapılmıştır. Saldırıların Estonya devlet internet sitelerine ve DNS sunucularına sızmaya yönelik saldırıları içerdiği ve botnetleri kullandığı görülmüştür. İkinci dalga, 9 Mayıs'tan 11 Mayıs'a kadar sürmüştür. Estonya'nın en büyük bankası olan Hansapank, DDoS saldırılarından etkilenmiştir (Buresh, 2020). Saldırılar sırasında, politik olarak anlamlı günlerde saldırıların yoğunlaştığı fark edilmiştir (Kaska vd., 2010). Saldırıların ikinci bölümü merkezi bir yerden kontrol ediliyor gibi görünmesine rağmen, ancak yalnızca birkaç kişi saldırıların sorumluluğunu üstlenmiş ve Rus hükümeti siber saldırılara karıştığını yalanlamıştır (Buresh, 2020). Çok sayıda botnetin dahil olduğu, daha sistematik, koordineli ve karmaşık olan üçüncü dalga (Kaska vd., 2010), 15 Mayıs tarihi öğlen saatlerinden gece yarısına kadar devam etmiş, Estonya'nın en büyük ikinci ticari bankası olan SEB Eesti Ühispank'ın internet sitesini ve müşterilerini etkilemiştir (Buresh, 2020). 18 Mayıs'ta gerçekleşen dördüncü dalga sırasında, devlet kurumları ve bankacılık hizmeti sunan internet siteleri, DDoS saldırılarından zarar görmüştür. Siber saldırıların yapıldığı dönemde Estonya'daki güvenlik açıkları nedeniyle temel hükümet işlevleri haftalarca olumsuz etkilenmiştir.

2.4. Saldırıların Aktörleri

Saldırıların bir bölümü Rus İnternet Protokolü (IP, Internet Protocol) adreslerine kadar takip edildiğinden, Estonya, başlangıçta saldırılardan Rusya'yı sorumlu tutmuştur. Estonyalı yetkililerin, saldırılardan Rusya'nın sorumlu olduğu yönündeki ilk iddialarına ve IP adreslerini Vladimir Putin'in yönetimindeki yerlere kadar takip edebilmelerine rağmen, Rusya bu iddiaları reddetmiştir (Crandall, 2014; Haataja, 2017). 1993 yılında Estonya ve Rusya arasında imzalanan Karşılıklı Adli Yardım Anlaşması'nın 3. Maddesi uyarınca, Estonya Cumhuriyet Savcılığı, 2007 siber saldırılarının soruşturulması sırasında 10 Mayıs 2007 tarihinde Rusya Federasyonu'na istinabe mektubu sunmuştur. İstinabe yazısında; Ceza Kanunu'nun bilgisayarla sabotaj, bilgisayarla bağlantıya zarar verme, bilgisayar ağı ve bilgisayar virüslerinin yayılması suçlarına ilişkin hükümlerine istinaden, cezai bir meselede, "kişinin tespiti" olarak tanımlı usulen bir faaliyet için ön soruşturma yapılması konusunda yardım istenmiştir (Tikk & Kaska, 2010). Rusya Cumhuriyet Başsavcılığı'nın Estonya'nın hukuki iş birliği talebini geri çevirmesi de Rusya'nın saldırılarla ilgili masumiyeti konusunda şüphe uyandırmıştır (Crandall, 2014).

Estonya hükümetinin sunucularına ve kritik altyapısına yönelik 2007'deki büyük ölçekli siber saldırıları Rusya'nın başlattığı ve gerçekleştirdiği bir kanı olarak görülse de mevcut veriler incelendiğinde saldırıların bir bölümünün gönüllü olarak, sıradan vatandaşlar ve internet kullanıcıları tarafından verilen talimatları izleyerek ve internet forumlarında deneyimlerini paylaşarak yapıldığı anlaşılmaktadır. Bununla birlikte, her ne kadar siber saldırıların Estonya ve Rusya arasındaki genel siyasi çatışmayla bağlantılı olduğu değerlendirilse (Ottis, 2008) de siyasi düzeydeki spekülasyonlara rağmen herhangi bir hükümetin saldırılardaki rolü doğrulanamamıştır (Kaska vd., 2010).

Bazı uzmanlar tarafından, siber saldırı eylemlerinin Rus hükümeti tarafından desteklendiği değerlendirilirken, diğerleri mevcut bilgilere dayanarak saldırıların sorumlularının kimliklerinin kanıtlanmasının imkânsız olduğu kanaatine varmışlardır (Haataja, 2017). Dolayısıyla saldırıların sorumluluğunu üstlenen birkaç kişi dışında (Kaska vd., 2010), Estonya'ya yönelik 2007 yılında düzenlenen siber saldırıların aktörleri net olarak ortaya koyulamamıştır.

3. Saldırıların Etkileri

Estonya'ya yönelik siber saldırılar, rastgele suç eylemlerinden daha fazlası olarak kabul edilmiştir. Estonya'nın küçük boyutu ve bilgi sistemlerine olan bağımlılığı göz önüne alındığında, saldırılar, ülke için önemli bir tehdit oluşturmuştur (Czosseck vd., 2011).

3.1. Kamuoyunda Yansımaları ve Vatandaşa Etkileri

Estonya, olayları silahlı bir saldırı olarak görmemiş ve bu nedenle NATO Antlaşması'nın 5. Maddesi kapsamında destek talep etmekten kaçınmıştır. Bunun yerine saldırılar, sadece bireysel siber suçlar veya tanınmış bir bilgi güvenliği analisti Dorothy Denning tarafından ortaya konduğu şekliyle "hacktivizm" olarak kabul edilmiştir (Czosseck vd., 2011). Muhafazakâr bir avukatın bakış açısına göre, Estonya'daki 2007 siber saldırıları bir dizi siber suçtan öteye geçmese de medya, saldırıları "I. Siber Savaş" olarak etiketlemiştir. Güvenlik analistleri, diğer DoS ve DDoS saldırılarına kıyasla Estonya saldırılarının boyutunun çığır açıcı olmadığını savunmuştur (Kaska vd., 2010).

Siber saldırıların, farklı dil ve etnik kökene sahip Estonya vatandaşları arasında herhangi bir iç çatışma veya bölünmeler içeren önemli bir etkisinin olmadığı değerlendirilmektedir. Estonya'ya yönelik siber saldırılar, askeri ve siyasi otoritenin sahip olduğu geleneksel fiziksel güç unsurlarını kullanmadan da bir savaşın pahalı, maliyetli, yıkıcı ve benzeri birçok maddi ve manevi olumsuz sonuçları olabileceğini göstermiştir. Bu saldırılar ile bir yandan bilgisayar korsanları tarafından asimetrik hasara yol açılabileceği, bir yandan da Estonya halkının askeri ve güvenlik sistemine olan itimadının zayıflatılabileceği mesajı verilmiştir (Thematic Area, 2007). Saldırılar sonunda, kamuoyu farkındalığı artmış ve Estonya gelecekte bu tür saldırıları önlemek için diğer ülkelerle iş birliği yapmaya başlamıştır. Böylece siber suç faaliyetlerine ilişkin uluslararası bilinç ve farkındalık artmıştır (Buresh, 2020).

3.2. Psikolojik Etkileri

Estonyalılar, saldırılar sırasında kendilerini ihlal edilmiş ve savunmasız hissetmiştir. Yapılan bir anket çalışması, Estonyalıların %65'inin bu küçük Baltık devleti için en büyük tehdidin siber olaylar olduğuna inandığını ve %55'inin ise yabancı müdahalenin Estonya'nın egemenliğini tehdit ettiğini düşündüklerini göstermiştir (Buresh, 2020).

3.3. Teknik Etkileri

Saldırıların teknik olarak birincil etkisi yıkıcı olmuştur. Birçok internet sitesine erişim ve dolayısıyla sağladıkları hizmetler kesintiye uğratılmış, devlet iletişim ve haberleşme kanallarının işleyişi etkilenmiştir. Ayrıca mobil ağlarda ve acil servis hattında hafif kesintiler yaşanmıştır. Kesintilerin; bankalar, devlet daireleri, medya şirketleri, küçük ve orta işletmeler dahil olmak üzere, çeşitli kuruluşların günlük işleyişini ciddi şekilde etkilediği bildirilmiştir (Buresh, 2020; Haataja, 2017).

3.4. Politik Etkileri

Devlet ile Estonyalılar arasındaki çevrimiçi iletişim kanallar, geçici olarak devre dışı kalmıştır. Önemli kamu hizmetlerine yalnızca çevrim içi olarak erişilebildiği göz önüne alındığında, bu hizmetlere erişimin olmaması, birçok insan için "fark edilebilir bir etki" oluşturmuştur (Haataja, 2017). Meşru internet trafiğinin sıkışık olması nedeniyle diğer ülkelerle bilgi akışı da önemli ölçüde engellenmiştir (Buresh, 2020). NATO için siber saldırılar açık bir askerî harekât oluşturmadığından, saldırılar NATO müttefiklerinin yanıt vermek zorunda olmadığı anlamına gelmiştir (Crandall, 2014). Bu eşgüdümlü çevrimiçi protestoların; iş dünyası, hükümet ve toplum üzerindeki etkisi hissedilir derecede olsa da yıkıcı sonuçları olmamıştır. Bu olayın uzun vadeli en önemli sonucu ise NATO'nun, Tallinn'de İşbirlikçi Siber Savunma Mükemmeliyet Merkezi (CCDCoE, Cooperative Cyber Defence Centre of Excellence) birimini, Estonya'nın girişimi ile kalıcı bir birim olarak kurması olmuştur (Rid, 2012). Estonya; NATO'nun siber saldırılar yaşanırken gerekli tepkiyi verememesiyle bir başka önemli etkiyi yaşamış ve bunun sonucunda CCDCoE'yu kritik öneme sahip bir merkeze dönüştürmüştür. Bu durum Estonya'yı AB (Avrupa Birliği), ABD (Amerika Birleşik Devletleri) ve NATO'ya daha da yakınlaştırmıştır (Buresh, 2020).

3.5. Ekonomik Etkileri

Rus makamları tarafından Estonya'ya resmi olarak doğrudan herhangi bir ekonomik yaptırım uygulanmazken, ticari ilişkiler kötüleşmiştir. Estonya'daki birçok şirket, Rus ticaretinden gelir kaybetmiştir (Ottis, 2008). Rusya tarafından Estonya'ya uygulanan dolaylı ekonomik yaptırımlar (Czosseck vd., 2011), bazı tahminlere göre 27 ila 40 milyon ABD doları arasında olmuştur (Haataja, 2017).

3.6. Uluslararası Hukuk Çalışmalarına Etkileri

Siber saldırılar karşısında, uluslararası toplum, bu son derece karmaşık yasal konulara düzen getirme arzusuyla ilk kez siber operasyonları ve siber savaşı kapsamlı bir şekilde ele almış (Buresh, 2020) ve uluslararası hukuk çalışmalarına katkı sağlamak için rehberler hazırlanmıştır. Yaklaşık yirmi kişiden oluşan Uluslararası Uzmanlar Grubu tarafından mevcut uluslararası hukuk normlarının bu yeni savaş biçimine nasıl uygulanacağı incelenmiş ve üç yıllık bir çabanın sonucunda, resmi bir belge olmayan Tallinn Siber Savaşa Uygulanan Uluslarararası Hukuk El Kitabı (Tallinn El Kitabı) hazırlanmıştır (CCDCOE, 2013). Tallinn El kitabı, resmi bir NATO normlar bütünü olmamakla birlikte, siber uzayda ortaya çıkabilecek durumlar için önemli bir rehberdir. Bu rehber, 1868 Petersburg Deklarasyonu ve 1949 Cenevre Sözleşmeleri gibi mevcut uluslararası silahlı çatışma normlarını ele alarak bunları siber uzaya uygulamaktadır. Bu kitabın yayınlanmasından sonra, bu alanda yeni yasalara ihtiyaç olduğunun farkında olan Rusya gibi ülkeler, belgenin siber savaş kavramını tamamen meşrulaştıracağını belirtmiştir (Fonseca vd., 2014).

Tallinn El Kitabı'nın 2013 yılında hazırlanan ilk versiyonu (Tallinn 1.0), siber savaşa uygulanabilecek uluslararası hukuk ilkelerini tanımlamakta, bu tür çatışmaları yöneten 95 adet katı kuralı listelemekte ve her bir kural için kapsamlı açıklamalar sunmaktadır. Tallinn El Kitabı'nın ikinci versiyonu (Tallinn 2.0) ise oldukça etkili olan ilk baskının üzerine kapsam genişletilerek 2017'de yayınlanmıştır. Tallinn 2.0, savaş eylemleri düzeyine varmayan kötü niyetli siber faaliyetleri de kapsayacak şekilde genişletilmiş olup bu tür olayları ele alan 154 adet katı kural tanımlamakta ve her biri için ayrıntılı açıklamaları içermektedir. Tallinn 2.0'da uzman yazarların yanında, birçok devletin ve elliden fazla hakem değerlendiricinin gayri resmi katkıları bulunmaktadır. Tallinn 3.0 üzerindeki çalışmalar ise halen devam etmektedir (Georgetown University Law Library, 2023).

3.7. Uluslararası Etkileri

Estonya siber saldırıları, kurum ve kuruluşların hizmetlerini sunmaları ve bireylerin bu hizmetlerden faydalanmaları noktasında zaman kayıplarına neden olurken, ayrıca toplumda dijitalleşmeyle ilgili güvenlik kaybı algısı ve endişelerine yol açmıştır. Ancak bu olayların ortaya çıkardığı etkiler, ihmal edilebilir düzeyde kalmış, yaşanan gerçek ve önemli etki ise Estonya'nın artık bir siber güvenlik merkezi olarak değerlendirilmesi olmuştur. Saldırıların karmaşıklığı, Devlet Güvenlik Komitesi (KGB, Komitet Gosudarstvennoy Bezopasnos)'nin halefi olan Rusya Federal Güvenlik Servisi (FSB,

Federal Security Service)'nin ve Amerikan Merkezi İstihbarat Teşkilatı (CIA, Central Intelligence Agency)'nın dikkatini çekmiştir (Buresh, 2020).

Estonya; 2007 saldırıları sonrasında, uluslararası düzeyde siber güvenliğin en önemli savunucularından biri haline gelmiştir. NATO, siber saldırılara karşı birleşik bir strateji geliştirmeye başlamış ve 2010'da NATO, siber saldırıları ittifak için bir tehdit olarak kabul eden ve tehditle yüzleşmek için ittifakın ve ulusların yeteneklerini geliştirmeyi tercih eden yeni stratejik konsepti benimsemiştir (Czosseck vd., 2011).

Estonya, siber suçlarla mücadele kapsamında Avrupa Konseyi gibi birçok uluslararası kuruluşa aktif destek vermiştir. Bu doğrultuda, Güneydoğu Asya Ülkeleri Birliği'nin (Association of Southeast Asian Nations) siber suçlarla ilgili yasalarının uyumlaştırılmasını sağlamış ve Birleşmiş Milletler'in Uluslararası Güvenlik Bağlamında Bilgi ve İletişim Teknolojilerinde Geliştirme (Development in Information and Communication Technology in the Context of International Security) çalışma grubuna bir uzman ile katkıda bulunmuştur (Czosseck vd., 2011). Estonya'da meydana gelen 2007 siber saldırıları, uluslararası düzeyde, saldırıları küresel olarak dikkate değer kılan siyasi ve sosyal bir motivasyon unsuru olmuştur (Kaska vd., 2010). Estonya'nın kapsamlı bir siber stratejiyi benimsemesi ve komşu ülkelerde meydana gelen benzer girişimler, çeşitli ulusların Tallinn'in liderliğini nasıl takip ettiğinin en iyi örneğini sunmuştur. Estonya'nın, Siber Güvenlik Stratejisini Mayıs 2008'de yayınlamasından bu yana, Almanya, Hollanda, Fransa ve Birleşik Krallık da dahil olmak üzere bir dizi Avrupa ülkesi benzer stratejiler yayınlamıştır (Jackson, 2013). DDoS saldırıları sırasında ve sonrasında, NATO ve Avrupa Birliği (AB) üye ülkeleri, dijital savaşa karıştığı tespit edilen devletler için uygun cezaları tartışmaya başlamıştır. NATO, Nisan 2008'deki Bükreş Zirvesi'nde, siber savunma konusunda birleşik bir politika benimsemiş ve siber savunma operasyonel yeteneklerini ittifak genelinde merkezileştirmek için Brüksel merkezli Siber Savunma Yönetim Otoritesi (CDMA, Cyber Defence Management Authority)'ni kurmuştur (Herzog, 2011). AB tarafından Kasım 2010'da İç Güvenlik Stratejisi yayınlamıştır. NATO, 2011 yılı Kasım ayında Lizbon'da, ittifakın güçlü, entegre internet savunma yetenekleri geliştirmek için adımlar atacağını belirten yeni bir Stratejik Kavramı kabul etmiştir.

3.8. Sektörel Etkileri

Saldırılar öncesinde, Estonya'daki büyük bankaların çoğunun sahipliği, başta İsveç olmak üzere yabancı ülkelere aitti. Bu yapı, Estonya bankalarını, İsveç topraklarında barındırma sunucuları da dahil olmak üzere, kurumlarını, İsveç bankalarıyla daha yakından entegre etmeye teşvik etmiştir. Ancak, 2007 saldırılarından sonra, Estonya bankalarının Estonya topraklarındaki sunucularının varlığının, bankaların kendilerini koruma ve bir saldırıdan hızlı bir şekilde kurtulma yeteneği için gerekli olduğunu ortaya çıkmıştır. Sonuç olarak hükümet, hangi bankaların ve diğer kritik işletmelerin sunucularının barındırılabileceğine ve veri depolama boyutuna ilişkin düzenlemeler oluşturmaya başlamıştır. Siber saldırılardan etkilenen Estonya bankaları, devlete ait kurumların ağlarını daha güvenli hale getirme çabalarını desteklemiştir (Jackson, 2013).

4. Siber Saldırılara Müdahale

4.1. Teknik Müdahale

Estonya Bilgisayar Acil Müdahale Ekibi (CERT, Computer Emergency Response Team) saldırılara yanıt vermek için koordinasyon organı haline gelmiştir. Estonya CERT'in acil müdahale programı, olayın ciddiyetini analiz etmeyi, yurtdışındaki hizmet sağlayıcılara kötüye kullanım raporları göndermeyi ve etkilenen kuruluşlar ile hizmet sağlayıcılar arasında bilgi alışverişini kolaylaştırmayı içermiştir. NATO gibi uluslararası kuruluşlardan da başta istişare şeklinde olmak üzere bir miktar yardım alınmıştır.

Estonya, internet sitelerine yapılan kötü niyetli saldırılara aldırmadan, yerel internet trafiğini sürdürmeye çalışmış ve yabancı internet sitelerine ziyaretler çoğunlukla mümkün olmuştur. Kamu sektörü internet sitelerinin çoğuna yerel kullanıcılar tarafından erişilirken yurtdışı internet kullanıcılarına kısıtlamalar uygulanmıştır (Kaska vd., 2010).

4. 2. Uluslararası Müdahale

Estonya'ya yönelik siber terörizm, kamu hizmetlerini, ticareti ve hükümet operasyonlarını durdurabilecek yeni bir dijital şiddet biçiminin bir versiyonu olmuştur. Estonya'ya yönelik saldırıların ciddiyeti, hızlı bir uluslararası tepki oluşturmuştur (Herzog, 2011).

Estonya'nın geleneksel terör eylemlerine karşı koyma çerçevesi dışında çok az resmi siber savunma hazırlığı vardı. Hükümet CERT'i; ağ operasyonlarının yeniden normale dönmesini sağlamak için Finlandiya, Almanya, İsrail ve Slovenya'nın yardımına ihtiyaç duymuştur. NATO CERT'leri ek yardım sağlarken AB'nin Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA, European Network and Information Security Agency), gelişen duruma ilişkin uzman teknik değerlendirmeler sunmuştur. Ayrıca, kriz sırasında batılı ülkeler arasında yüksek düzeyde istihbarat paylaşımı gerçekleşmiştir. Rusça konuşan bilgisayar korsanları, interneti bir silah ve seferberlik aracı olarak kullanırken, Estonya ve müttefikleri, saldırılara başarılı bir şekilde karşı koymak için dijital ağları kullanmışlardır (Herzog, 2011).

2007'de Estonya'ya yönelik saldırılara verilen çok uluslu tepkiler, devletlerin veya devlet dışı aktörlerin interneti bir silah olarak kullanarak müttefiklerinin egemenliğini tehdit etmesi nedeniyle ülkelerin tarafsız ve kayıtsız kalmayacaklarını göstermiştir. Ancak Çin, konuyu Estonya'nın iç güvenlik ikilemi olarak ele almış ve bunun sonucunda ortaya çıkan uluslararası siber güvenliğe karışmaktan kaçınmıştır. Moskova ve Pekin, herhangi bir gizli suç ortaklığı veya katılımcısı olmasına bakmaksızın, Estonya siber saldırılarının durum analizini yapmıştır. Böylece Tallinn'in güvenlik açıkları ile batılı tepkileri değerlendirerek kendilerinin siber savaş yeteneklerini ve stratejilerini geliştirmişlerdir (Herzog, 2011).

5. Siber Güvenlik Alanında Yaşanan Gelişmeler

Estonya 2007 saldırıları, ülkede yasal, kurumsal organizasyon ve politik yapı ile ilgili birçok düzenlemeye yönelik çalışmaları tetikleyerek bazı durumlarda zaten yapılmakta olan değişiklikleri desteklemiş veya geliştirmiştir (Kaska vd., 2010; Czosseck vd., 2011). Bu değişikliklerin bir bölümü 2007-2010 yılları arasında hayata geçirilmiş, bir bölümü ise halen uygulanmaya devam etmektedir (Kaska vd., 2010).

5.1. Politik Gelişmeler

Siber saldırılar sonrasındaki gelişmelerin temel taşı, Mayıs 2008'de kabul edilen, Estonya'nın ilk Ulusal Siber Güvenlik Stratejisidir. Stratejide belirlenen hedeflere ulaşmak için kritik bilgi altyapısının korunması, bilgi güvenliğinin genel yetkinliği, ilgili yasal çerçeve, uluslararası iş birliği ve siber güvenlik konularında farkındalık gibi yüksek öncelikli alanlarda, bir dizi somut ölçülebilir eylemi öngören uygulama belgesi onaylanmıştır (Kaska vd., 2010).

Siber Güvenlik Stratejisi, Savunma Bakanlığı liderliğindeki çok kurumlu bir konsey tarafından oluşturulmuş (Jackson, 2013) ve beş stratejik politika hedefini gerçekleştirmeyi amaçlamıştır. Bunlar, (i) bir güvenlik sisteminin geliştirilmesi ve geniş ölçekte uygulanması, (ii) siber güvenlikte yetkinliğin arttırılması, (iii) siber güvenliğin desteklenmesine yönelik yasal çerçevenin iyileştirilmesi, (iv) uluslararası iş birliğinin desteklenmesi ve (v) siber güvenlik konusunda farkındalık oluşturulmasıdır.

Mayıs 2010'da güncellenen ve onaylanan Ulusal Güvenlik Konsepti (Estonia, 2010), Estonya hükümetinin ikinci büyük siber güvenlik politikası tepkisini temsil etmektedir. Siber güvenliğin, *"[...] kritik bilgi sistemlerinin ve veri iletişim bağlantılarının zafiyetlerinin azaltılması*" ile sağlanacağı ifade edilmekte, kritik sistemlerin; yabancı ülkelerle bağlantı geçici olarak arızalansa veya çalışmasa bile çalışır durumda kalması, bu eylemleri desteklemek için gerekli mevzuatın geliştirilmesi ve kamuoyunun bilinçlendirilmesi gerektiği belirtilmektedir (Estonia, 2010).

Ulusal Güvenlik Konsepti, Ekim 2010'da yayınlanan ve 2018 yılına kadar revize edilen Suç Politikasının Geliştirilmesine İlişkin Kılavuz'un hazırlanmasına öncülük etmiştir. Polisin, kötü amaçlı yazılımların yayılması ve artan sayıda bilgisayar korsanlığı olaylarını önlemeye odaklanması, ayrıca siber suçların daha etkin bir şekilde sınırlandırılması için kolluk kuvvetlerinde yeterli sayıda bilişim uzmanının bulunmasının sağlanması konuları, hazırlanan çalışmalarda yer almıştır (Czosseck vd.,

2011). Ayrıca, siber uzayda yürütülen savaşlara yönelik olarak adını Estonya'nın başkentinden alan, ülkeler arası ilk siber saldırının derlendiği ve uygulamasının değerlendirildiği Tallinn El Kitabı, Nisan 2013'te hazırlanmıştır (Fonseca vd., 2014).

Bilgi güvenliği alanında farkındalığı ve en iyi uygulamaların anlaşılmasını artırmayı amaçlayan uluslararası bir araştırma konsorsiyumu olan CCDCoE'nin oluşturulması, önemli bir politika gelişmesi olmuştur. Estonya, bu konsorsiyum içinde siber güvenlik sorunlarını çözmek için uluslararası iş birliğini teşvik edebilmektedir (Jackson, 2013).

5.2. Yasal Gelişmeler

Saldırılardan üç yıl sonra, Estonya 2007 siber saldırıları gibi sınır ötesi siber olayların, farklı hukuk alanlarının hukuk normlarına dokunduğu giderek daha belirgin hale gelmiştir. Bu nedenle, Silahlı Çatışma Hukuku, Ceza Hukuku ve Bilgi Teknolojileri (BT) yasal çerçevesinin üçlü prizmasından ele alınarak bu alana kapsamlı yaklaşımın desteklenmesi gerektiği görülmüştür (Kaska vd., 2010). Belirlenen strateji doğrultusunda derhal gözden geçirilmesi ve güncellenmesi gereken üç yasal alan belirlenmiştir. Bunlar, (i) siber suçlarla mücadele için yasal düzenleme, (ii) Kritik Bilgi Altyapısını Koruma Dairesi Başkanlığı (CIIP, Department for Critical Information Infrastructure Protection)'nın hazır halde bulunmasını destekleme, (iii) kritik bilgi sistemleri için bilgi güvenliği standartlarının belirlenmesidir. Bu alanlardan yola çıkarak temel mevzuat değişiklikleri iki kanun çıkarılması ile sonuçlanmıştır: (i) hem maddi hem de usul açısından kanun değişikliklerinin Parlamento tarafından Mart 2008'de kabul edildiği "Ceza Kanunu" ve (ii) kritik bilgi altyapısına yönelik tehditleri barındıran, 2009'da kabul edilen yeni "Acil Durum Kanunu"dur (Kaska vd., 2010). Elektronik Haberleşme Kanunu gibi diğer kanunlar da güncellenmiştir, ancak siber güvenlik bağlamında önemli değişiklikler içermemiş olup siber güvenlikle ilgili kanunlar (Czosseck vd., 2011) tarafından detaylı bir şekilde ele alınmıştır.

5.3. Kurumsal Gelişmeler

Estonya Bilişim Merkezi (EIC, Estonian Informatics Centre), kamu bilgi hizmetlerini ve sistemlerini yönetmekten ve geliştirmekten sorumlu bir devlet kurumu olup ayrıca bu hizmetler ve sistemler için siber güvenliği sağlamakla da görevlidir. 2006 yılında ulusal EIC'nin bir birimi olarak CERT kurulmuş olmasına rağmen, saldırılar sırasında yetenekleri ve deneyimi mütevazi düzeyde olmuştur (Czosseck vd., 2011). Ulusal Siber Güvenlik Stratejisi sonucunda, 2010 yılında, Estonya ulusal CERT'inin yanı sıra hükümet bilgi sistemlerinden sorumlu merkezi bir hükümet organı olan EIC'ye, CIIP isimli yeni bir birim eklenmiştir. Yeni departmanın görevleri arasında Estonya'nın kritik bilgi altyapısı için bir savunma sistemi oluşturmak ve hem kamu hem de özel sektördeki önemli BT sistemlerinin korunmasını sağlamak yer almıştır (Kaska vd., 2010).

Siber saldırılar sırasında, Estonya CERT'ine gönüllü siber güvenlik uzmanlarından oluşan gayri resmi bir ağ da yardım etmiştir. Bu ağ, artan durumsal farkındalık, analiz yeteneği, hedeflenen varlıklar arasında savunma tekniklerinin hızlı paylaşımı ve uluslararası ortaklarla genişletilmiş bir doğrudan temas ağı gibi çok ihtiyaç duyulan ek yetenekleri sağlamıştır (Czosseck vd., 2011). Bu konsept 2008 Siber Güvenlik Stratejisinde desteklenmiş ve Siber Savunma Ligi (CDL, Cyber Defence League)'nin ilk birimleri 2009'un başlarında etkinleştirilmiştir. Siber Savunma Ligi, 1918'de kurulmuş (1990'da restore edilmiş) gönüllü bir askeri ulusal savunma örgütü olan Savunma Ligi'nin bir parçası olarak faaliyet göstermektedir. Siber Savunma Ligi, ülkenin yüksek teknolojili yaşam tarzını korumak, bilgi altyapısını savunmak ve farkındalığı artırmak, en iyi uygulamaları paylaşmak, özel sektör ve kamu sektörü arasında iş birliğini geliştirmek ve bir uzmanlar ağı oluşturmak için gönüllü olan bilgi teknolojisi uzmanlarından oluşturulmuştur. Bu gönüllüler, 2010'dan önce Estonya ağlarını savunmak için esnek bir şekilde birlikte çalışmışlardır. 2006'da Estonya CERT'in oluşturulmasının yanı sıra bilgi paylaşımına ilişkin geliştirilen yeni politikalar, bu gruplar arasındaki iş birliğini artırmıştır. 2007 saldırılarından sonra Estonya, bir siber saldırı sırasında ülkeyi daha etkin ve uyumlu bir şekilde savunabilmesi için bu birimin kamu kurumu olmasına karar vermiştir. Kurtarma hizmeti ve polis gibi sivil yapıları destekleyen CDL, askeri tehdit durumu dahil olmak üzere, bir siber olay durumunda hafifletme çabalarını destekleyebilmeyi, ulusun bağımsızlığını ve anayasal düzenini savunmada hazırlığı artırmayı hedeflemektedir (Kaska vd., 2010), (Jackson, 2013). CDL'nin temel faaliyetleri

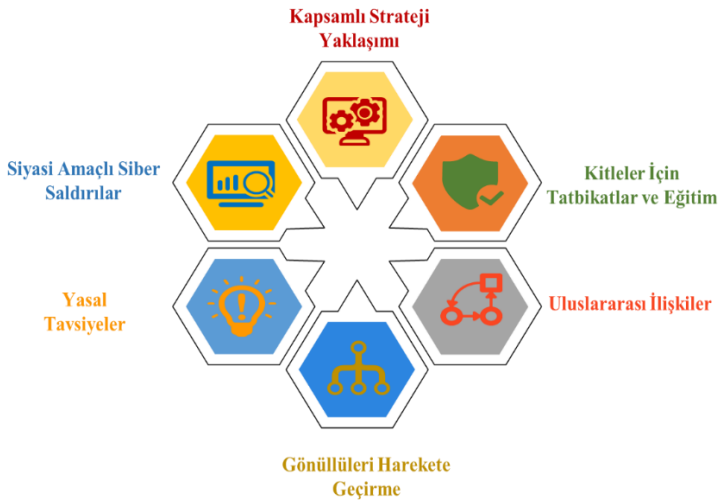
arasında eğitim ve farkındalık etkinliklerinin yanı sıra siber savunma tatbikatları düzenlemek yer almaktadır (Czosseck vd., 2011).

6. Öğrenilmiş Dersler ve Ülkelere Tavsiyeler

Siber saldırılar sonrasında Estonya'nın öğrendiği dersler, Estonya'nın ulusal sınırlarının ötesinde performans gösteren ulusal güvenlik planlamacılarına çeşitli öneriler ile ülkelere siber güvenlik alanında tavsiyeler Şekil 1'de gösterilmiş olup aşağıdaki bölümlerde özetlenmiştir.

Şekil 1

Öğrenilmiş Dersler ve Ülkelere Tavsiyeler



6. 1. Kapsamlı Strateji Yaklaşımı

Estonya'nın 2007 siber saldırılarını dikkate aldığı ve kendine dersler çıkardığı açıkça görülmektedir. Atılan en önemli adım, ulusal Siber Güvenlik Stratejisinin benimsenmesine ve ardından uygulanmasına giden kapsamlı bir politikanın hızlı bir şekilde oluşturulmasıdır. 2007 saldırıları Estonya'da siber güvenlik stratejisinin hazırlanmasını tetiklemiştir; ancak ülkeler bu tür tetikleyicileri beklememeli ve proaktif olarak siber altyapılarının güçlü olmasını sağlamalı ve kapsamlı bir risk değerlendirmesini yapmalıdır. Ayrıca, saldırının suç, casusluk, terörizm veya askeri motivasyonla başlatılıp başlatılmadığını genellikle yalnızca bağlam ve ek bilgiler ortaya çıkarabileceğinden, ilgili kurumlar arasındaki yakın iş birliği, siber güvenlik alanında başarının olmazsa olmazı olarak değerlendirilmektedir (Czosseck vd., 2011).

6. 2. Siyasi Amaçlı Siber Saldırılar

Önceleri siber güvenliğin odak noktasını suç ve casusluk saldırıları oluştururken sonraki yıllarda siyasi güdümlü siber saldırılarda artış olduğu gözlenmiştir. Siyasi olarak motive olmuş aktörler, kritik altyapıya yönelik yüksek profilli saldırılardan, bir devleti uzun bir süre boyunca zayıflatabilecek saldırılara kadar tüm siber saldırı yelpazesini kapsayabilmektedir. Ulusal güvenliği tehdit eden siyasi güdümlü saldırı tehdidinin yakın gelecekte ortadan kalkması muhtemel olmadığından, siber güvenlik konusu, politika yapıcıların dikkatini çekmek için bir ulusal güvenlik sorunu olarak ele alınmalıdır (Czosseck vd., 2011).

6. 3. Yasal Tavsiyeler

Estonya hukuk düzeninin bilgi ve haberleşme teknolojilerine yönelik bölümlerinin analizi, güvenli bir bilgi toplumunun çeşitli hukuk disiplinlerini içeren normlar tarafından kapsamlı bir şekilde desteklenmesi gerektiğinin altını çizmektedir. Estonya yasal çerçevesi tarafından ortaya koyulan geniş yaklaşım, özel hukuk ve kamu hukuku alanlarını bir araya getirmekte ve ceza hukuku, kriz yönetimi düzenlemesi ve savaş zamanı hukuku/ulusal savunma hukuk düzenini devreye sokarak siber olay

düzenlemesi yelpazesini tamamlamaktadır. Ülkelerin; uluslararası siber güvenlik düzenlemesinin çok çeşitli yasal alanları kapsadığını, ilgili düzenleyici çerçevelerin gözden geçirilmesi gerektiğini ve olası ele alınmamış gri alanların belirlenmesinin tavsiye edildiğini anlaması hayati önem taşımaktadır. Avrupa Konseyi Siber Suçlar Sözleşmesi (Council of Europe Convention on Cybercrime)'nin geniş ve kapsayıcı ulusal uygulamasının, özellikle siber suçların sınır ötesi doğası göz önüne alındığında çok önemli olduğu değerlendirilmektedir. Estonya deneyimi, tüm bilgisayar kullanıcıları, bilgi sistemleri ve kritik altyapı şirketleri için ortak güvenlik standartları oluşturma (Czosseck vd., 2011) ve hukuksal düzenleme ihtiyacını ortaya koymuştur.

6. 4. Kitleler İçin Tatbikatlar ve Eğitim

Ulusal siber güvenliği geliştirmenin önemli bir bileşeni, siber güvenlik bilinci ve eğitimidir. Bu, devlet kurumlarındaki veya özel kurumlardaki profesyonellerle sınırlı kalmamalı, her düzeyde ihtiyaç duyulan beceri ve bilgiler göz önünde bulundurularak günlük yaşamında BİT kullanan bir vatandaştan, üst düzey politika yapıcılara kadar tüm spektrumu kapsamalıdır. Buna, kolluk kuvvetleri ve özellikle siber güvenliğin düzenleyici yönlerini yorumlamada merkezi bir role sahip olan yargı sistemi dahildir. Her grup için uygun farklı çözümler geliştirilerek geniş ve kapsamlı bir siber güvenlik kültürü oluşturulmalıdır.

Hem ulusal hem de uluslararası seviyede düzenlenen siber güvenlik tatbikatları, siber saldırılara karşı etkin bir hazırlık görevi üstlenmektedir (Czosseck vd., 2011). Siber tatbikatlar; teknik, masaüstü, prosedürel, haberleşme ve hibrit formatlar olarak organize edilebilmektedir. Bu tatbikatların, uluslararası düzeyde organize edilenleri arasında Çapraz Kılıçlar (Crossed Swords), Siber Koalisyon (Cyber Coalition) ve Kilitli Kalkanlar (Locked Shields) örnek olarak gösterilebilir (NÚKIB, 2023).

Siber Koalisyon, 2008 yılından bu yana uygulanan, NATO'nun en önemli yıllık kolektif siber savunma tatbikatıdır. Askeri Komite'nin yönetimi altında Müttefik Dönüşüm Komutanlığı tarafından planlanarak yürütülen, dünyadaki en kapsamlı siber savunma tatbikatlarından biridir. Siber Koalisyon tatbikatı, Estonya Siber Güvenlik Tatbikatları ve Eğitim Merkezi veya Tallinn'in NATO müttefikleri ve ortaklarına siber güvenlik alanında destek sunan en yeni yazılım tabanlı sanal ortam olan CR14 (Cyber Ranges) aracılığıyla yürütülmektedir. Eğitim katılımcıları ve yerel eğitmenler, sanal ağlar aracılığıyla kendi ülkelerinden ve kuruluşlarından katılım sağlarken, Estonya'da küçük bir tatbikat kontrol grubu toplanarak tatbikatın yürütülmesini organize etmektedir (NATO OTAN, 2023).

Kilitli Kalkanlar, birçok NATO üyesi devletin katıldığı, dünyadaki en karmaşık teknik canlı saldırı mücadelesini sunan benzersiz bir uluslararası siber savunma tatbikatı olup 2010 yılından itibaren CCDCoE tarafından organize edilerek düzenli olarak yapılmaktadır. Estonya siber saldırıları sonrasında, uluslararası iş birliği daha fazla desteklenmiştir ve tatbikatlara katılan NATO ekipleri, siber savunma uzmanlıklarını geliştirmektedir (Boeke, 2017; CCDCOE, 2022).

Yıllık olarak düzenlenen Çapraz Kılıçlar; sızma testi, dijital adli tıp ve durumsal farkındalık uzmanlarının eğitimine odaklanan, teknik bir siber tatbikat olup tam ölçekli siber operasyonları önleme, tespit etme ve bunlara yanıt verme becerilerini geliştirmeyi amaçlamaktadır. Tatbikat, NATO CCDCOE tarafından 2016 yılından bu yana düzenlenmektedir ve tatbikata katılanların çoğu daha sonra Kilitli Kalkanlar'ın kırmızı ekibinin bir parçası olmaktadır (NÚKIB, 2023; CCDCOE, 2021).

6. 5. Uluslararası İlişkiler

Estonya'ya yönelik saldırılar, siber tehditlere yanıt verme konusunda bir ülkenin tek başına çok az şey yapabileceğinin daha da belirgin hale gelmesiyle uluslararası iş birliğinin öneminin anlaşılmasını sağlamıştır. Ayrıca, siber suç düzenlemelerini dünya çapında uyumlu hale getirmeyi amaçlayan Avrupa Konseyi Siber Suçlar Sözleşmesi gibi belgelerin onaylanması desteklenmeli ve teşvik edilmelidir. İş birliğine yönelik siyasi iradenin yanı sıra, ulusal ikili ve çok taraflı anlaşmalar, bilgi paylaşım anlaşmaları, kolluk kuvvetlerinin iş birliği, ortak soruşturma ekipleri, uluslararası tatbikatlar, resmi ve gayri resmi ağlar ve diğer uluslararası girişimler, siber suçların etkin bir şekilde kovuşturulması ve soruşturulması için büyük önem taşımaktadır (Czosseck vd., 2011).

6. 6. Gönüllüleri Harekete Geçirme

İnternet altyapısının çoğunun özel sektöre ait olduğu ve işletildiği bilinmektedir. Özel sektördeki konumlarından bağımsız olarak ulusal siber güvenliğe önemli katkı sağlayabilecek özel sektör çalışanlarından oluşan uzmanlar havuzu bulunmaktadır. Bu durum, aynı zamanda kendi uzmanlık alanlarında çalışmayan kamu sektöründeki uzmanları da içermektedir. Uygun yasal, politik ve operasyonel çerçeveler oluşturularak gönüllü olan siber güvenlik uzmanları harekete geçirilebilir ve gönüllülerin ulusal siber güvenlik kapasitesini önemli ölçüde artırması sağlanabilir (Czosseck vd., 2011).

7. Günümüz Ulusal Siber Güvenlik Politikalarına Bakış

ITU'nun Küresel Siber Güvenlik İndeksi (ITU, 2020) sonuçları, ülkelerin, günümüzde dijital evrendeki siber güvenlik tehditlerinin farkında olarak birçok çalışma yürüttüğünü ortaya koymaktadır. Estonya siber saldırıları başta olmak üzere, dünyada yaşanan siber savaşlar ve siber olaylar sonrasında, artık dünya ülkelerinin birçoğunun Bilgisayar Olayına Müdahale Ekibi (CIRT, Computer Incident Response Team) bulunmaktadır. Ayrıca birçok ülkenin siber güvenlik alanında çalışmalarına, ulusal siber güvenlik stratejileri rehberlik etmektedir.

Küresel perspektifte ülkelerin yasal, teknik, organizasyonel, kapasite geliştirme ve iş birliği tedbirleri çerçevesinde, siber güvenlik gelişimlerinin karşılaştırıldığı (ITU, 2020) dokümanında yer alan sonuçlar; gelişmiş ülkeler ile henüz gelişmekte olan ülkelerde özellikle kapasite açığını göz önüne sererek bu sorunun giderilmesi için bilgi ve beceri geliştirme mekanizmalarına ihtiyaç olduğunu ortaya koymaktadır. ABD, Birleşik Krallık, Estonya gibi gelişmiş ülkeler, ölçümü yapılan 194 ülke arasında indekste ilk sıralarda yer alırken henüz gelişmekte olan ya da az gelişmiş ülkeler arasında yer alan Afganistan, Dominik, Cibuti, Burundi gibi ülkeler ise listenin alt sıralarında bulunmaktadır.

Kritik altyapıları savunma, tehdit aktörlerini ortadan kaldırma, güvenliği ve dayanıklılığı artırmak için piyasa güçlerini şekillendirme, dirençli bir geleceğe yatırım yapma, ortak hedeflere ulaşmak için uluslararası ortaklıklar kurma ilkelerine dayanan ABD siber güvenlik stratejilerinin (The White House, 2023) etkin uygulanması sayesinde, ABD; ITU indeks sıralamasında dünyada ilk sırada yer almaktadır.

Avrupa'ya bakıldığında, AB üye ülkelerine, siber güvenlik tehditleri ve saldırıları ile mücadelede destek verilmesi amacıyla siber güvenliğe yönelik bir uzmanlık merkezi olan ENISA tarafından AB siber güvenlik yasasının omurgası oluşturulmuştur. Bu yasaya göre ENISA, üye devletlere ilişkin olarak ayrım gözetmeksizin siber güvenlik konusundaki ceza hukukunu dikkate almakta, üye devletlerin politika geliştirme ve uygulamalarında rehberlik yapmaktadır (Nezgitli & Benzer, 2020).

Siber güvenliği, ulusal savunma ve iç güvenliğin bir parçası olarak değerlendiren, siber uzayın fiziksel dünyadan ayrı bir şey olmadığını vurgulayan Estonya (Republic Of Estonia, 2023), sürdürülebilir dijital toplum, siber güvenlik endüstrisi araştırma ve geliştirme, uluslararası katkıda liderlik, siber okur-yazar toplum stratejileri (Republic Of Estonia, 2020) doğrultusunda, geçmişten edindiği tecrübeleri ile yürüttüğü kapsamlı ve sistematik çalışmaları sayesinde ITU indeks sıralamasında, Avrupa'da ikinci, dünyada ise üçüncü sıraya yerleşmiştir (ITU, 2020).

Birçok ülke tarafından gizlilik, yetkisiz erişim ve çevrim içi güvenlik gibi alanları adresleyen yeni siber güvenlik mevzuatı ve düzenlemeleri yapılmasına, güvenilir siber uzay oluşturmak için gerekli çalışmalar yürütülmesine rağmen, (ITU, 2020) sonuçları, hâlâ ülkelerin kapasite oluşturmak için stratejiler ve mekanizmalar geliştirmeye gereksinim duyduklarına, iş dünyasının, giderek artan siber riskler karşısında daha hazırlıklı olması ve risk azaltma politikaları izlemesi gerektiğine işaret etmektedir.

Türkiye ise siber uzaydaki varlıklarını etkili bir şekilde koruyabilmek amacıyla Ulaştırma ve Altyapı Bakanlığı (UAB) tarafından hazırlanan 2013-2014 ve 2016-2019 yıllarını kapsayan Ulusal Siber Güvenlik Stratejisi ve Eylem Planları ile siber güvenlik yol haritasını belirlemiş ve bu doğrultusunda önemli çalışmalar yapmıştır. Ulusal ölçekte siber güvenlik politikaları UAB tarafından oluşturulmakta, siber güvenlik çalışmaları, UAB koordinasyonunda, ilgili kurumların iş birliği ile yürütülmektedir. Siber güvenliğe ilişkin (i) 5237 sayılı Türk Ceza Kanunu, 5070 sayılı Elektronik İmza Kanunu, 5809

sayılı Elektronik Haberleşme Kanunu'nda yapılan düzenlemeler, (ii) 2010 yılında Avrupa Konseyi Siber Suçlar Sözleşmesine taraf olunması gibi yasal düzenlemeler, (iii) etkin bir şekilde uygulanan siber güvenlik stratejisi, (iv) Bilgi Teknolojileri ve İletişim Kurumu (BTK) bünyesinde faaliyetlerini sürdüren Ulusal Siber Olaylara Müdahale Merkezi (USOM) çalışmaları, (v) belirlenen kritik altyapı sektörleri başta olmak üzere kurum ve kuruluşlarda bulunan Siber Olaylara Müdahale Ekipleri (SOME)'nin faaliyetleri, (vi) ulusal ve uluslararası siber güvenlik tatbikatları, (vii) ulusal ve uluslararası iş birlikleri, (viii) siber istihbarat toplama ve paylaşmaya yönelik çalışmalar, (ix) AVCI, AZAD ve KASIRGA gibi yapay zekâ ve makine öğrenmesi imkânlarını kullanan hızlı tespit ve erken müdahale sistemleri gibi birçok siber güvenlik faaliyeti etkin bir şekilde yürütülmektedir (T.C. Ulaştırma ve Altyapı Bakanlığı, 2021). Türkiye, siber güvenlik alanındaki kazanımlarını daha üst seviyelere taşımak için Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023 (T.C. Ulaştırma ve Altyapı Bakanlığı, 2020)'te yer alan faaliyetleri uygulayarak ve aktif olarak yürüttüğü siber güvenlik çalışmaları sayesinde, siber güvenlik alanında Avrupa'da altıncı, dünyada on birinci sıraya yükselmiştir (ITU, 2020). Mevcut durum incelendiğinde, Türkiye'de siber güvenliğin disiplinler arası değerlendirilmesi gereken geniş kapsamlı bir alan olduğu, hâlâ gelişme alanlarının bulunduğu, özellikle yetişmiş insan kaynağı kapasitesine ihtiyaç duyulduğu görülmekte olup Şekil 2'de Türkiye'nin ulusal siber güvenlik çalışmaları ve mevcut durumu özetlenmiştir.

Şekil 2

Türkiye'de Siber Güvenliğe İlişkin Yürütülen Çalışmalar ve Mevcut Durum

8. Sonuç ve Değerlendirmeler

Estonya'nın 2007 yılında maruz kaldığı siber saldırılar, başlı başına siber savaş olarak değerlendirilmese de Estonya makamlarının mevcut siber güvenlik kavramını gözden geçirmesinde ve bilgi toplumunu korumak için kapsamlı bir strateji geliştirmesinde etkili olmuştur (Kaska vd., 2010). Estonya ile Batı arasındaki siyasi ilişkiler daha da gelişmiş olup özellikle Estonya'nın ABD, AB ve NATO'ya yaklaşmasını sağlamıştır. Rusya ile ABD, AB ve NATO arasındaki siyasi mesafe artmış, ABD ile Rusya arasındaki ilişkiler daha da gerilmiştir (Buresh, 2020). Saldırılar, siber savaşta uygulanacak uluslararası hukuk üzerine Tallinn El Kitabı'nın yayınlanmasıyla sonuçlanmış ve Tallinn El Kitabı'nın üçüncü versiyonunda, önceki baskılardaki yaklaşım tarzı korunacak şekilde hazırlık çalışmalarına devam edilmektedir (CCDCOE, 2023).

Saldırılar, Estonya hükümetinin; Estonya Savunma Bakanlığı tarafından eğitilen ve bir kamu hizmeti sağlayıcısı veya bir ISP, bir siber saldırının kurbanı olduğunda, izlenecek prosedürleri uygulayarak boş zamanlarını ülkelerini korumaya adayan, gönüllü bir CDL'yi kurması ile sonuçlanmıştır (Buresh, 2020).

Yaşanan siber olaylar, siber saldırıların tekil kurumlarla sınırlı olmadığını, ulusal güvenliği tehdit eden bir düzeye gelebileceğini göstermiştir. Estonya'ya yönelik siber saldırılar, siber uzaydan gelen tehditlerin ulusal güvenliği potansiyel olarak etkileyen tehditler olarak anlaşılmasını tetiklemiş ve dijital bilgi teknolojilerinin dikkatsiz kullanımı ile ilişkili riskler hakkında bir uyandırma çağrısı başlatmıştır. Siyasi olarak motive olmuş bireylerin oluşturduğu risklerin, siber güvenliğe yönelik ciddi bir tehdidin olası bir unsuru olarak görülmesini sağlamıştır (Czosseck vd., 2011). Siber olayların tespitinin ve müdahalenin, bilgi paylaşımı gereksinimleri ve gerekli çerçeve yaklaşımı ile ele alınması gerektiğini ortaya koymuştur (Harrison & White, 2012). BT güdümlü küreselleşme döneminde, Estonya'ya yönelik saldırılar, NATO'nun 5. Maddesi ve ABD nükleer şemsiye garantilerinin bile, bir ulus devletin siber uzaydaki egemenliğinin korunmasını sağlayamadığını göstermiştir (Herzog, 2011).

Estonya siber terörizm vakası, internetten kaynaklanan atfedilmesi zor asimetrik tehditlerin, gelecekte ulus devletlere zarar verebileceğini gözler önüne sermiştir (Herzog, 2011). Bu nedenle, siber tehditlere karşı hazırlıklı olmak için siber tatbikat değerlendirme sürecinde sistematik ve önceden tanımlanmış bir yaklaşım uygulamanın önemi anlaşılmıştır (Mäses, Maennel, Toussaint, & Rosa, 2021). Bir suçun işlenmesi sonrasında, araştırma ve inceleme faaliyetleri için uluslararası iş birliğini teşvik edici birçok araç ve mekanizma bulunmasına rağmen, siber suçların ele alınması hususunda sadece birkaç aracın tasarlandığı ve bunun birçok açıdan sorun teşkil edebileceği, ulusların kendi yasal sınırları dışında inceleme yapamadıkları, politik olarak motive olmuş suçluların karıştığı siber olayların ele alınmasında, uluslararası düzeyde kanun ve politikalara ihtiyaç olduğu görülmüştür (Tikk & Kaska, 2010).

Özellikle DDoS saldırıları, devletin ve sivil toplumun işleyişini kesintiye uğratarak, Estonya varlığına düşmanca bilgi akışları oluşturmuş ve düzgün çalışma yeteneğini baltalamıştır. Bu saldırılar, devletin etkileşim yeteneğini, özerkliğini ve bilgi varlıklarını koruma kapasitesini olumsuz etkilemiştir. Bu nedenle, fiziksel nesnelere maddi hasar veya insanlara zarar verilmemesine rağmen, Estonya varlığına karşı bir tür bilgi çalma amaçlı şiddet oluşturmuştur. Bu nedenle, bilgisel bir yaklaşım benimsenerek, Estonya'ya yönelik saldırılar gibi siber saldırıların, bir varlık olarak devletin özüne yönelik bilgisel bir şiddet biçimi olarak değerlendirilmesine yol açmıştır (Haataja, 2017). Bu saldırılar, Estonya devletinin E-Estonya sürecine geçişiyle sonuçlanmıştır (Buresh, 2020). Estonya; politik, yasal ve kurumsal yapılarında yaptığı düzenlemeler ile Avrupa'nın en güçlü, dünyanın üçüncü sıradaki siber güvenlik mekanizmalarına sahip ülkesine dönüşmüştür (ITU, 2020). Bir ulus devletin siber güvenliğinin; ancak ulusal politikaları, yasal çerçevesi ve hem kamu hem de özel sektör aktörlerini içeren organizasyonların iş birliği gözetilerek, gerekli olduğu kadar iç içe geçmiş bir yaklaşımla ve gerçekçi bir risk değerlendirmesi ile tanımlanan değişiklikler ile sağlanabileceği (Czosseck vd., 2011) görülmüştür.

Estonya hükümetinin krizi ele alış biçimi ve uluslararası paydaşlarla iş birliği içerisinde sorunu çözmeye odaklanışı, diğer ülkelerin bu konuya yaklaşımlarında farkındalık ve değişim oluşturmuştur. Son yıllarda Türkiye dahil pek çok ülke, siber saldırılarla başa çıkma konusunda ulusal kapasitesini geliştirerek tepki seçeneklerinin askeri ve yasal tedbirlerle sınırlı olmadığını, daha geniş diplomatik araçların ve tutarlı bir uluslararası birliktelik içeren önleyici tepkinin daha etkili olabileceğini öğrenmiştir. Çok yönlü ve ansızın ortaya çıkma ihtimali olan siber saldırılara karşı hazırlıklı olunması, siber güvenliğe ilişkin toplumsal farkındalığın artırılması, ulusal ve uluslararası koordinasyon ve iş birliğinin önemi gibi hususlar, dünya ülkeleri için siber uzayda alınabilecek önlemlerin temelini oluşturmuştur.

Siber alemde yaşanan gelişmeler sonrasında, birçok ülke ulusal güvenlik hassasiyetleri doğrultusunda; siber savaş, siber savunma gibi konularda etkili çözümler geliştirebilmek için iş birliklerine ihtiyaç duymaktadır. Bu çerçevede, ulusal hukuki düzenlemeler ile uluslararası hukuki düzenlemelerin uyumlaştırılması önem arz etmektedir. Ayrıca yıkıcı ve yenilikçi teknolojilerin yaşamın birçok alanına girmiş olması, siber güvenlik kapsamında da mevcut yasal düzenlemelerin, tedbirlerin, strateji ve politikaların sürekli güncellenmesi ihtiyacını ortaya çıkarmaktadır. Her geçen gün daha bağlantılı ve ilişkili hale gelen dünyada, ülkelerin siber savunma politikaları çerçevesinde sanal sınırlarını belirlemesi ve koruması önemli bir husus olarak değerlendirilmektedir.

Özetle, siber evrenin, dünya ulus devletleri arasındaki ilişkiler üzerinde oluşturduğu baskılar, siber suçlara ve siber savaş ortamına hızlı bir şekilde dönüşebildiğinden, siber güvenliğe ilişkin yapılan tüm çalışmalar tüm dünyada büyük önem arz etmekte, özellikle siber güvenlik alanında ortaya koyulan strateji, politika ve mevzuat hususları ile Ar-Ge çalışmaları, ülkelerin gündeminde sürekli yer almaktadır. Bu bağlamda, Estonya örneği, dünyada ülkelerin dersler çıkardığı, uygulamalarda referans aldığı ve önlemler geliştirmede göz önünde bulundurduğu birçok unsur içermektedir.

Etik Standartlar İle Uyumluluk

Çıkar Çatışması: Yazarlar herhangi bir çıkar çatışmasının olmadığını beyan eder.

Etik Kurul İzni: Bu çalışma için etik kurul iznine gerek yoktur.

Yazar Katkı Beyanı: Yazarlar eşit oranda katkıda bulunduklarını beyan ederler.

Finansal Destek: Yoktur.

Kaynakça

Boeke, S. (2017). National cyber crisis management: Different European approaches. *Governance-An International Journal of Policy Administration and Institutions*. https://doi.org/https://doi.org/10.1111/gove.12309

Buresh, D. L. (2020). A Critical Evaluation of the Estonian Cyber Incident. *Journal of Advanced Forensic Sciences, 1*(2), 7-14. /https://doi.org/10.14302/issn.2692-5915.jafs-20-3601

CCDCOE. (2013). The Tallinn Manual. 3, https://web.archive.org/web/20130424162717

CCDCOE. (2021). Crossed Swords. https://www.ccdcoe.org/exercises/crossed-swords/

CCDCOE. (2022). Locked Shields., https://ccdcoe.org/exercises/locked-shields/

CCDCOE. (2023). CCDCOE to Host the Tallinn Manual 3.0 Process., https://www.ccdcoe.org/exercises/crossed-swords/

Crandall, M. (2014). Soft Security Threats and Small States: The Case of Estonia. *Defence Studies, 14*(1), 30-55. https://doi.org/10.1080/14702436.2014.890334

Czosseck, C., Ottis, R., & Talihärm, A.-M. (2011). Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security. *IJCWT, 1*, 24-34, http://doi.org/10.4018/ijcwt.2011010103.

Estonia. (2010). *National Security Concept of Estonia*. https://eda.europa.eu/docs/default-source/documents/estonia---national-security-concept-of-estonia-2010.pdf

Fonseca, C. E., Perdomo, I. L., & Arozarena Gratacos, M. (2014). El manual de Tallin y la aplicabilidad del derecho internacional de la ciberguerra. Ortiz, Javier Ulises. http://cefadigital.edu.ar/handle/1847939/993

Georgetown University Law Library. (2023). International and Foreign Cyberspace Law Research Guide. https://guides.ll.georgetown.edu/cyberspace/cyber-conflicts

Haataja, S. (2017). The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach. *Law, Innovation and Technology*, *9*(2), 159-189. https://doi.org/10.1080/17579961.2017.1377914

Harrison, K., & White, G. (2012). Information sharing requirements and framework needed for community cyber incident detection and response. *2012 IEEE Conference on Technologies for Homeland Security (HST)*, 463-469. https://doi.org/10.1109/THS.2012.6459893

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Source: Journal of Strategic Security*, *4*(2), 49-60. https://doi.org/10.2307/26463926

ITU. (2020). *Global Cybersecurity Index 2020*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Jackson, C. (2013). *Estonian Cyber Policy After the 2007 Attacks: Drivers of Change and Factors for Success*.

Kaska, K., Talihärm, A.-M., & Tikk, E. (2010). Developments in the legislative, policy and organisational landscapes in Estonia since 2007. *International Cyber Security Legal and Policy Proceedings*, 40-66.

Mäses, S., Maennel, K., Toussaint, M., & Rosa, V. (2021). Success Factors for Designing a Cybersecurity Exercise on the Example of Incident Response. *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 259-268. https://doi.org/10.1109/EuroSPW54576.2021.00033

NATO OTAN. (2023). Cyber Coalition: NATO's Flagship Cyber Exercise. https://www.act.nato.int/activities/cyber-coalition/

Nezgitli, S., & Benzer, R. (2020). Avrupa Birliği Siber Güvenlik Kanunu. *Journal*, *2*(1), 10-17. https://dergipark.org.tr/tr/pub/jismar/issue/55710/659519

NÚKIB. (2023). Exercise Types. https://nukib.gov.cz/en/cyber-security/exercises/exercise-types/#:~:text=Crossed%20Swords%20is%20a%20technical,to%20full-scale%20cyber%20operations.

Ottis, R. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. *Proceedings of the 7th European Conference on Information Warfare*, 163. Academic Publishing Limited Reading, MA.

Republic Of Estonia. (2020). *Cyber Security Strategy 2019-2022*. Ministry of Economic Affairs and Communications. https://www.mkm.ee/media/703/download

Republic Of Estonia. (2023). *Cyber Security in Estonia 2023*. Information System Authority. https://www.ria.ee/media/2702/download

Rid, T. (2012). Cyber war will not take place. Journal of strategic studies, 35(1), 5-32, https://doi.org/10.1080/01402390.2011.608939.

T.C. Ulaştırma ve Altyapı Bakanlığı. (2020). *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023*., https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf

T.C. Ulaştırma ve Altyapı Bakanlığı. (2021). *12. Ulaştırma ve Haberleşme Şurası Sektör Raporları*. https://sgb.uab.gov.tr/uploads/pages/suralar/12-ulastirma-ve-haberlesme-surasi-sektor-raporlari.pdf

The White House. (2023). *National Cybersecurity Strategy*., https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Thematic Area. (2007). *2007 cyber attacks on Estonia*., https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf

Tikk, E., & Kaska, K. (2010). Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons. *9th European Conference on Information Warfare and Security 2010, ECIW 2010*.

Zhu, X. (2023). Western Studies on the Sovietization of Eastern Europe. Chinese Journal of Slavic Studies, 3(1), 15-32. https://doi.org/10.1515/cjss-2023-0008