https://doi.org/10.52642/susbed.1348365

Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 2023; (52): 249-267
- Siber Güvenlik / Araştırma / Research -

Japonya'nın Siber Güvenlik Politikası

Fulya KÖKSOY*

ÖZ

Sürekli değişim ve dönüşüm geçiren bilgi ve iletişim teknolojileri, avantajları yanında içerisinde büyük riskleri barındırarak, güvenlik tehditlerinin yaşanmasına sebebiyet vermektedir. Bu noktada sadece devletlerin değil aynı zamanda kurumların ve bireylerin karşı karşıya kaldığı siber saldırılar, dijital çağın kırılgan yapısına işaret etmekte ve siber güvenlik kavramına alan açmaktadır. Siber güvenlik, özellikle son yıllarda üzerinde çalışılan, politikalar ve/veya stratejiler geliştirilen, sadece teorik düzeyde değil pratik boyutta da ne gibi adımlar atılabileceğinin sorgulandığı ve daha da ileri gidilerek evrensel bir mekanizma oluşturulabilir mi? sorusuna cevap aranan popüler bir konuyu yansıtmaktadır. Siber güvenliğin sağlanması konusunun bu denli önem arz etmesi ekseninde Japonya'da dijital dünya kaynaklı tehditlere yönelik farkındalık taşımakta ve siber güvenliğe ilişkin politikalar geliştirmeye çalışmaktadır. Nitekim Japonya'nın bu alana ilişkin politikalarını geliştirilmesinde genel olarak her yıl milyonlarca siber saldırı yaşaması etkili olurken bu saldırıların özellikle Çin, Kuzey Kore ve Rusya kaynaklı olduğu belirtilmektedir. Bu minvalden hareketle söz konusu çalışmada Japonya'nın siber güvenlik politikaları analiz edilmektedir. Ayrıca, betimsel analiz yöntemiyle oluşturulan ve Japonya'nın siber güvenliğinin sağlanmasına yönelik politikalarını inceleyen bu çalışma, elde edilen çıktılar üzerine tarihsel kurumsalcılık teorisi ve iş birliği modeli ekseninde bir okuma yapmaktadır.

Anahtar Kelimeler: Siber Güvenlik, Japonya, Tarihsel Kurumsalcılık, İş Birliği Modeli.

The Cyber Security Policy of Japan

ABSTRACT

Information and communication technologies, which are constantly changing and transforming, besides their advantages, contain great risks and pose security threats. At this point, the cyberattacks that not only states but also institutions and individuals face point to the fragile nature of the digital age and open up space for the concept of cyber security. Cybersecurity, especially in recent years, has become a popular topic on which policies and/or strategies have been developed, questioning what steps can be taken not only at the theoretical level but also at the practical level and seeking an answer to the question "Can a universal mechanism be created?" by going further. In line with the importance of providing cyber security, Japan is aware of the threats originating from the digital world and is trying to develop a policy regarding cyber security. As a matter of fact, the millions of cyberattacks experienced every year are effective in the development of Japan's policies in this field, while it is stated that these attacks especially originate from China, North Korea, and Russia. From this point of view, in this study, Japan's cyber security policies are analyzed. In addition, this study, which was created by descriptive analysis and examines the policies of Japan's cyber security, makes a reading on the outputs in the axis of historical institutionalism theory and cooperation model.

Keywords: Cyber Security, Japan, Historical Insitutionalism, Cooperation Model.

1. Giriş

Siber uzay/alan, modern dünyanın en popüler kavramlarından birini teşkil etmektedir. Bilgi ve iletişim teknolojilerinin yüksek yoğunluklu olarak değişim ve dönüşüm geçirmesi hem birçok avantaja neden olmakta hem de siber tehdit kaynaklı güvenlik açıklarının oluşmasına yol açmaktadır. Öyle ki değişen ve dönüşen dünya kompozisyonu ve hız kesmeden büyüyen teknolojik küreselleşme çerçevesinde siber uzay kaynaklı avantaj ve dezavantajların yaşandığı bilinen bir realitedir. Siber tehdit kaynaklı güvenlik açıklarının yüksek ölçekli yaşanmaya devam etmesi ise tehdit-güvenlik arasında kurulması gereken dengeyi aşındırmakta ve siber güvenlik kavramına alan açmaktadır.

Günümüzün öncelikli risk unsurlarından biri olan siber tehditler; devletleri, uluslararası örgütleri ve bireyleri etkilemekte, bu doğrultuda söz konusu aktörlerin bu tehditlere karşı önlem almalarını bir zorunluluk hâline getirmektedir. En önemli spesifik özelliği kaynağının belirsiz olması olan siber saldırıları bertaraf etmek ve dijital ortamda güvenliği sağlamak konusunda politikalar ve/veya stratejiler formüle

* **Corresponding Author/Sorumlu Yazar,** Doç. Dr./Assoc. Prof. Dr., Batman Üniversitesi/Batman University, fulya.koksoy@batman.edu.tr
Makale Gönderim ve Kabul Tarihleri/Article Submission and Acceptance Dates: 23.08.2023-26.10.2023

Citation/Atıf: Köksoy, F. (2023). Japonya'nın siber güvenlik politikası. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 52*, 249-267. https://doi.org/10.52642/susbed.1348365

edilmesine yol açmaktadır. Bu noktada Asya Pasifik devletlerinden biri olan, Çin ve Kuzey Kore ile sürekli siber çatışma yaşayan ve topyekûn olarak her yıl milyonlarca siber saldırıya maruz kalan bilgi ve teknoloji toplumu Japonya da siber güvenliğini daha sağlam bir zemine oturtmaya çalışmaktadır. Japonya her ne kadar siber güç kategorisi altında tanımlanmasa da siber güvenliğin sağlanması konusunda harcadığı yoğun çabalar ve her geçen gün bu alana yönelik etkin politikalar geliştirmeye devam etmesi noktasında önem teşkil etmektedir. Bu minvalden hareketle söz konusu çalışmada Japonya'nın siber alan kaynaklı yaşadığı tehditler karşısında ne yönde politikalar izlediği analiz edilmektedir. Öte yandan, Türkçe yazın incelendiği takdirde bu konuda ortaya konulmuş bir çalışma olmadığı görülmektedir. Söz konusu boşluğun kapatılması amacıyla kaleme alınan ve betimsel analiz yöntemiyle oluşturulan bu çalışma zarfında öncelikle Japonya'nın 2000'lerin başından günümüze siber güvenlik alanında yaşadığı kurumsallaşma süreci incelenmektedir. Akabinde 2022 yılında yayımlanan Yeni Ulusal Güvenlik Strateji Belgesi ele alınarak, söz konusu belge çerçevesinde siber güvenliğe yaklaşılmaktadır. Diğer taraftan mevzubahis konu, siber güvenlik bağlamında rol oynayan aktörler ve yapılan harcamalar boyutuna taşınmaktadır. Bununla beraber, Japonya'nın siber alanda gerçekleştirdiği iş birlikleri ele alınmaktadır. Son olarak elde edilen tüm bu veriler, teorik düzleme aktarılarak, Japonya'nın siber güvenlik politikaları tarihsel kurumsalcılığın ve iş birliği modelinin çıktılarıyla ne ölçüde örtüşmektedir sorusuna cevap aranmaktadır.

2. 2000'lerin Başından Günümüze Kurumsallaşma

1999 yılından önce siber güvenliğe odaklanmayan[1] bilgi ve teknoloji toplumu Japonya'nın, 2000'li yıllarla beraber bilgi ve ulusal güvenliği birbiriyle ilişkili olarak tanımladığı ve bu noktada siber alana ilişkin kurumsal yapısını güçlendirme eğiliminde olduğu görülmektedir. Bu noktadan hareketle bilgi ve telekomünikasyon ağ bağlantılarının oluşturulması ve güçlendirilmesi, hükûmet ile yerel yönetimlerin sorumluluklarının ortaya konulması hedeflerini ön plana çıkaran ve yoğunluklu olarak bilgi teknolojileri kullanımının siber tehditlerin yaygınlaşmasına sebebiyet vermesi ekseninde ulusal güvenliğin korunması için siber tehditlere ilişkin önlem alınması gerekliliği üzerinde duran "Bilgi Teknolojileri Temel Yasası" 2000 yılında yürürlüğe girmiştir (Basic Act on Information and Telecommunications Network Society, 2000). Bununla beraber, söz konusu kanun ekseninde Bilgi Güvenliği Politika Konseyi[2] koordinasyonu altında, Bilgi Güvenliği Kültürü Uzmanlar Kurulu ve Bilgi Toplumu Stratejisi Uzmanlar Kurulu'nun faaliyetleri doğrultusunda 2006 yılında "Ulusal Bilgi Güvenliği Strateji Belgesi[3]" yayımlamıştır. Diğer taraftan, ilk kez siber saldırılar çerçevesinde devlet ve devlet dışı aktörlere atıf yapan, dijital ekonominin önemini vurgulayan ancak hem toplumun günlük yaşantısını hem de topyekûn ulusal güvenliği olumsuz yönde etkileyen siber tehditlerin altını somut olarak çizmeyen ikinci "Bilgi Güvenliği Strateji Belgesi[4]" 2009 yılında yayımlanmıştır (Gady, 2017, ss. 10-11).

2010'lardan başlayarak yeni yaşanan olaylar siber güvenliğin önemi bir kez daha göstermiştir. Öyle ki 2011 yılında Çinli bilgisayar korsanları tarafından Japonya'nın en önemli şirketlerinden biri olan Mitsubishi Heavy Industries'in denizaltılara, füzelere, savaş uçaklarına ve nükleer santral tesislerine yönelik gizli verileri ele geçirilmiştir (Kingston, 2016). 2011 yılında Temsilciler Meclisi'nin bir sunucusuna girilerek, tüm üyelerin şifreleri çalınmıştır. Bu noktada 2011 yılında yaşanan siber saldırılar sonrasında siber güvenliği daha sağlam bir zemine oturtmak, mevcut eksikliklerin ve sorunların bertaraf edilmesi amacıyla özellikle kamu ve özel sektör iş birliğini odak noktasına koyan ve bu doğrultuda Japonya'nın uluslararası siber uzay

[1] E-devlet yapılanmasının güçlendirildiği 1990'ların sonunda kamusal alana yönelik gerçekleştirilen bir dizi siber saldırı akabinde Japonya hükûmetinin siber güvenliğe yönelik ilgisi, 2000'li yıllarla beraber artış göstermiştir. Nitekim bu saldırılar, Japonya'nın siber politikasındaki zayıflıkları ortaya koymuş ve somut bir politikanın inşa edilmesi gerekliliğini göstermiştir (Bartlett, 2019, ss. 9-10).

[2] Ekonomi, Ticaret ve Sanayi Bakanlığı ile İçişleri ve Haberleşme Bakanlığı'nın ilgili bürokratları arasında gerçekleştirilen toplantılarda ortaya konan tavsiyeler sonucunda Mayıs 2005'te Bilgi Güvenliği Politika Konseyi'nin oluşturması kararı verilmiştir (Bartlett, 2019, s. 15).

[3] Söz konusu belge, bilgi güvenliği için üç hedef ortaya koymaktadır: 1) Japonya'nın büyük bir ekonomik güç olarak sürekli gelişiminin sağlanması, 2) Vatandaşların daha iyi yaşam standartlarına sahip olmasına yönelik politikalar takip edilmesi, 3) Ulusal güvenliğin sağlanması (Information Security Policy Council, 2006, s. 2).

[4] Mevzubahis belgenin 2006 yılında yayımlanan Bilgi Güvenliği Strateji Belgesindeki hedeflerin bir kez daha altını çizdiği görülmektedir (Information Security Policy Council, 2009). Ayrıca her iki belge de siber güvenlik konusunda kamu-özel sektör ortaklığının geliştirilmesi gerekliliğini vurgulamaktadır.

normlarının geliştirilmesi gerekliliğinin altını çizen yeni "Siber Güvenlik Strateji Belgesi" 2012 yılında kabul edilmiştir (Gady, 2017, s. 13). Ancak istatistikî veriler ekseninde devlet ağları, 2012'de yaklaşık 2 milyon ve 2013 yılında 5 milyon civarında siber saldırıya uğramıştır (Nitta, t.y). Bu bağlamda siber alanda atılması planlanan adımlar konusunda oldukça kararlı olduğunu göstermek isteyen Japonya, 2013 yılında yeni bir "Siber Güvenlik Strateji Belgesi" yayımlamıştır. Mevzubahis belgede siber uzayın bir savaş alanı olduğu kabulü çerçevesinde Öz Savunma Kuvvetleri'nin savunma kapasitesinin güçlendirilmesi, Savunma Bakanlığı ile diğer bakanlıklar arasında sorumlulukların paylaşılması ve siber savunma konusunda sivil bir mekanizmadan ziyade askerileşmeye dönük bir yapılanmaya gidilmesi hedefleri ortaya konmuştur (Gady, 2017, ss. 13-14). Ancak bu noktada altı çizilmesi gereken bir husus, Japonya'nın siber savunma stratejisinin kendi yeteneklerini geliştirmeye odaklanan ve diğer aktörlere karşı saldırgan eylemler ima etmeyen bir özelliği haiz olmasıdır (Ukhanova, 2022, s. 5). Ayrıca belgede siber tehditlere karşı ortak anlayış üzerine tesis edilen iş birliğinin geliştirilmesine yapılan atıf dikkati çekmektedir (Nitta, t.y.).

Japonya, siber güvenliğe yönelik tehditlerin dünya ölçeğinde yoğunlaşması çerçevesinde siber tehditlerle mücadele edebilmek, serbest bilgi akışını sağlamak ve siber güvenliği korumak için 2014 yılında "Siber Güvenlik Temel Yasası'nı" yürürlüğe koymuştur. Etkili ve kapsamlı bir siber güvenlik politikasının teşvik edilmesi amacıyla ortaya konan yasada, ulusal siber güvenlik politikası ilkelerinin belirlenmesi ve hükûmetin, yerel yönetimlerin, ilgili diğer kamu kuruluşlarının sorumluluklarının açıklığa kavuşturulması üzerinde durulmaktadır. Güçlü bir ekonomik ve toplumsal yapının oluşması için etkin siber güvenlik politikalarının takip edilmesi, siber alana ilişkin toplumsal bilgi ve bilinçlilik düzeyinin artırılması noktasında siber güvenlik politikalarının tanıtımının yapılması ve ülke vatandaşlarının siber tehditlerden korunması için ilgili sürece katılımlarının sağlanması gerekliliğinin altı çizilmektedir. Ayrıca yasaya göre, hem ulusal hem de uluslararası toplum açısından ortak bir endişe kaynağı olan siber tehditler karşısında Japonya'nın, uluslararası normlar doğrultusunda devletlerle koordinasyon ve iş birliği içerisinde olması önem arz etmektedir. Öyle ki Japonya'nın siber güvenlik alanındaki hedefleri arasında bulunan uluslararası iş birliğinin güçlendirilmesi çerçevesinde uluslararası toplumda üstlenen rollerle siber alanda norm belirlemede aktif olması, devletlerarası bilgi paylaşımını ve teknik iş birliğini etkin hâle getirerek, siber güvenlik alanındaki kapasitenin güçlendirilmesi noktasında daha somut adımlar atması öngörülmektedir. Bununla beraber yasada vurgulandığı üzere, siber güvenlik politikalarının tesis edilmesi ve uygulanması hükûmetin sorumluluk alanında olsa da hükûmet ile birlikte ilgili bakanlıkların, yerel yönetimlerin, üniversitelerin, diğer eğitim ve araştırma kurumları ile ticari kuruluşların da aynı düzeyde ilgili alandan sorumlu olduğu ve iş birliğinin güçlendirilmesi hususu dikkati çekmektedir. Yasa çerçevesinde bir diğer vurgu, siber güvenlik konusunda araştırma yaparak, toplumun bilgilendirilmesi yoluyla alana yönelik farkındalığı artıracak uzmanlar yetiştirilmesi gerekliliği üzerine yapılmaktadır. Nitekim bu hususun hayata geçirilmesi için üniversiteler ve diğer ilgili kuruluşlarla yakın temas hâlinde olmak önem teşkil etmektedir (Global Regulation, 2016). Öte yandan, Siber Güvenlik Temel Yasası, Nisan 2016'da ve Aralık 2018'de olmak üzere iki kez revize edilmiştir. İlk revizyon, Siber Güvenlik Stratejik Merkezi ve Siber Güvenlik İçin Olay Hazırlık ve Strateji Merkezi'nin (NISC) ağ izleme yetkisi, siber güvenlik denetimi ve ciddi olayların soruşturulması gibi konularda yetkilerini genişletmekte, ikinci revizyon ise gönüllük esasına dayalı olan bir iş birliği mekanizması kurulması ekseninde Siber Güvenlik Konseyi oluşturulmasını öngörmektedir (Ogawa & Tsuchiya, 2021, s. 24). Bu bağlamda mevzubahis revizyonlar, Japonya'nın siber güvenlik konusuna verdiği önemi gözler önüne sermektedir.

Diğer taraftan 2015 yılında yayımlanan Siber Güvenlik Strateji Belgesi, Tokyo'nun 2013 yılında 2020 Olimpiyat ve Paralimpik Oyunlarına ev sahipliği yapmak üzere seçilmesinden sonraki strateji belgesi olması nedeniyle önem arz etmektir. Bu bağlamda belgede ortaya konduğu üzere, Japonya ulusal siber güvenlik yeteneklerini geliştirme çabalarını hızlandırmaktadır. Nitekim bu hususun altında özellikle 2012 Londra Yaz Olimpiyatları ve Paralimpik Oyunları ile 2014 Soçi Kış Olimpiyatları'nın siber saldırılarla karşı karşıya kalması bulunmaktadır (Matsubara & Mochinaga, 2021, s. 6). Belgede uluslararası kamuoyunun Tokyo Olimpiyatlarına büyük ilgi göstereceği beklentisinden yola çıkılarak, siber güvenlik önlemlerinin yüksek düzeyde alınması gerekliliği ve kamu-özel sektör ortaklığının güçlendirilmesi gibi konuların altı çizilmektedir (Cyber Security Strategy, 2015).

2018 yılında hazırlanan "2018 Siber Güvenlik Strateji Belgesi", süper akıllı toplum olarak da betimlenerek, dijitalleşme ve yapay zekânın toplumla entegrasyonu olarak tanımlanan "Toplum 5.0'a" ulaşma hedeflerine odaklanmakta ve mevzubahis gelişmenin getireceği tehdit ve güvenlik açıklarını ortaya koymaktadır. Toplum 5.0'a ulaşma hedefine ek olarak, 2020 Tokyo Olimpiyat Oyunlarını güvence altına almanın önemli bir zorunluluk olduğunun altını çizen belgede, tedarik zinciri güvenliğini ve nesnelerin internetine ilişkin güvenlik açıklarını ele almak için uygun bir modelin oluşturulması öngörülmektedir. Bununla beraber, sürdürülebilir kalkınma için siber güvenlik ekosisteminin güçlendirilmesi gerekliliğine odaklanan belge; özgür, adil ve güvenli bir siber alan inşası amacına işaret etmektedir. Bahsi geçen bu hedeflere ulaşma noktasında ise Japonya hükûmeti üç yaklaşım ortaya koymaktadır: 1) Hizmet sağlayıcılar için görev güvencesi, 2) Siber güvenliği sağlamak için risk yönetimi, 3) Katılım ve iş birliği (Cyber Security Strategy, 2018). Ek olarak strateji, uzay endüstrisinin siber güvenliğini ve uzay teknolojisinin korunmasını sağlamak için yönergeler oluşturmanın gerekliliğini kabul etmektedir (Iwamoto & Verspieren, 2023).

Kritik altyapıların güvenliğini sağlamak için gönüllülük ve paylaşım esaslı bir yaklaşım benimseyen Japonya, özel sektör aktörleri arasındaki tehdit bilgilerinin ve olaylarının değerlendirilmesi ve ciddi kritik olaylar karşısında ilgili bakanlıklarla birlikte iş birliğini teşvik eden "Kritik Altyapıların Korumasına Yönelik Siber Güvenlik Politikası'nı" 2018 yılında revize etmiştir (Cybersecurity Strategic Headquarters, 2017). Yine aynı yıl "Kritik Altyapıda Görev Güvencesi Kavramına Dayalı Risk Yönetimi Değerlendirme Rehberi" ve "Kritik Altyapı Bilgi Güvenliğine Yönelik İlkelerin Oluşturulması Kılavuzu" yeniden ele alınmıştır ki bu belgeler bilgi teknolojisi güvenliğini destekleyen mekanizmaların oluşturulması konusunda özellikle özel sektör kurumlarını desteklemek amacı taşımaktadır. Öte yandan, devlet kurumlarının bilgi güvenliğine ilişkin ortak bir standart her bakanlık tarafından belirlenirken aynı zamanda bu alandaki gelişmelerin bir parçası olarak "Siber Güvenlik Alanında İnsan Kaynağı Geliştirme Planı" ve "Siber Güvenlik Araştırma ve Geliştirme Stratejisi" ortaya konmuştur (Schuetze, 2020). Diğer taraftan, 2018 yılında daha fazla yetenek ve operasyon birimi yaratan yeni bir "Siber Savunma Stratejisi" kabul edilmiştir (Ministry of Defence, 2018). 2019 yılında ise kritik altyapıyı korumak ve Toplum 5.0'ın uygulanması konusunda Ekonomi Bakanlığı tarafından "Siber/Fiziksel Güvenlik Çerçeve Belgesi" yayımlanmıştır (Schuetze, 2020). Tüm bu belgelere ek olarak, 2021 yılında revize edilen "Siber Güvenlik Strateji Belgesi'nde" Japonya, "ulusal güvenlik çıkarlarını siber saldırılardan" korumak ve "hükûmetin siber saldırılara karşı sorunsuz yanıt verme yeteneğini" geliştirmek için "savunma, caydırıcılık ve durumsal farkındalık" yeteneklerini güvence altına almanın hayati önem taşıdığını kabul etmektedir (Cyber Security Strategy, 2021, s. 36). Ayrıca Japonya'nın uluslararası iş birliğine önem verdiği ve başından beri siber diplomasiye şu üç ilke çerçevesinde liderlik etmeye çalıştığı belirtilmektedir: 1) siber uzayda hukukun üstünlüğünün teşvik edilmesi, 2) güven artırıcı önlemlerin geliştirilmesi, 3) kapasite geliştirme konusunda iş birliğinin güçlendirilmesi (Ministry of Foreign Affairs of Japan, 2021, ss. 239–240). Diğer yandan gelişmekte olan ülkelerin yararına kapasite geliştirme konusunda, "Gelişmekte Olan Ülkeler için Siber Güvenlik Kapasite Geliştirme Desteği Temel Politikası" Aralık 2021'de yayımlanmıştır (Iwamoto & Verspieren, 2023).

Sonuç olarak, 2011 yılında Mitsubishi Heavy Industries şirketine yönelik Çinli bilgisayar korsanları tarafından gerçekleştirildiği öngörülen siber saldırı (Phys, 2011), 2012 yılında Japonya'nın, Çin ve Tayvan'ın da üzerinde hak iddia ettiği Senkaku/Diaoyu adaları konusunda yaşanan gerilim sonrasında Çin tarafından devlet kurumlarına yönelik yapıldığı düşünülen siber saldırı, 2013 yılında Güney Kore'nin finans ve medya kuruluşlarını merkez alan siber saldırıları (Kallendera & Hughes, 2017, s. 5, 10), 2015 yılında Japonya Emeklilik Hizmeti Kurumu'nu hedef alan siber saldırılar (Kingston, 2016), 2016'dan 2018'e kadar Japonya Havacılık ve Uzay Araştırma Ajansı da dâhil olmak üzere çoğunlukla havacılıkla ilgili yaklaşık 200 şirketin ve araştırma kurumunun, Çin ile bağlantılı olduğundan şüphelenilen siber saldırıların hedefi olması (Nikei Asia, 2021), 2019 ve 2020 yıllarında Mitsubishi Electric'e yapılan siber saldırılar (Cybersecurity Insiders, 2020), Mayıs 2023 tarihinde Japonya'nın ev sahipliği yaptığı G7 Zirvesi öncesinde özel ve kamu kuruluşlarına gerçekleştirilen siber saldırılar (Japan Times, 2023) gibi örnekler doğrultusunda 2011 yılından günümüze Japonya'nın siber saldırıları bertaraf edebilme kapasitesini artırmaya yönelik politika ve stratejiler geliştirdiği ve siber güvenlikle ilgili kurumsal yapısını güçlendirmeye çalıştığı görülmektedir.

3. Yeni Ulusal Güvenlik Stratejisi Ekseninde Siber Güvenlik

Japonya hükûmeti, 16 Aralık 2022 tarihinde Ulusal Güvenlik Stratejisi (*National Security Strategy*), Ulusal Savunma Stratejisi (*National Defence Strategy*) ve Savunma Geliştirme Programı (*National Defence Program*) olmak üzere üç belgeye dayanan yeni güvenlik stratejisini kabul etmiştir. Ulusal Güvenlik Stratejisi, yeni güvenlik ortamına yanıt olarak diplomatik ve savunma stratejilerini tanımlamakta, önümüzdeki 10 yıl için Japonya'nın ulusal güvenlik stratejisinin temel ilkelerinin altını çizmektedir. Ulusal Savunma Programı Yönergesi çerçevesinde yeniden adlandırılan Ulusal Savunma Stratejisi, Japonya Öz Savunma Kuvvetleri'nin önümüzdeki on yıl için savunma stratejisini ortaya koymakta, ulusal güvenliğe yönelik hedefleri belirlemekte ve bu hedeflere ulaşılması noktasında takip edilmesi gereken yaklaşım ve araçları ana hatlarıyla ele almaktadır. Orta Vadeli Savunma Programı ekseninde yeniden adlandırılan Savunma Geliştirme Programı ise savunma kabiliyeti seviyesinin maksimum düzeye ulaştırılmasına ilişkin orta ve uzun vadeli bir plana işaret etmektedir (Köksoy & Ceyhan, 2023). Bu belgelere ek olarak, 2022 yılında "Kritik Altyapı Koruması için Siber Güvenlik Politikası'nın" yayımlandığı görülmektedir.

II. Dünya Savaşı sonrası Japonya'nın ulusal güvenlik politikasında önemli bir dönüm noktasını oluşturan yeni ulusal güvenlik stratejisi altı temel noktaya odaklanmaktadır. Birincisi, Japonya'nın güvenliği için önemli bir tehdit hâline dönüşen Çin'in askeri yükselişi ortaya konmaktadır. Bununla beraber, 2027 mali yılında savunma bütçesinin GSYİH'nın %2'sine çıkarılması çağrısında bulunulmaktadır. Üçüncüsü, yaklaşık 1.000 km menzilli ve karşı saldırı kabiliyetine sahip füzeleri tedarik etme ve siber alanda aktif siber savunmayı devreye sokma hususları planlanmaktadır. Ayrıca, farklı türlerde insansız silahlı araçların satın alınması konusu vurgulanmakta ve son olarak, savunma teçhizatı ihracatının genişletilmesini destekleyen faaliyetlerin yapılması hedeflenmektedir (Osowa, 2023).

Japonya hükûmetinin bilgi ve siber güvenliğe yeniden vurgu yaptığını gösteren söz konusu yeni ulusal güvenlik strateji belgesinin ve siber güvenlik politikasının siber alanda iki önemli değişiklik getirdiği görülmektedir: Bilgi savaşına yönelik bir tutumun geliştirilmesi ve siber güvenlik bağlamında aktif siber savunma hususunun önceliklendirilmesi. Bu durumun altında hem Japonya'nın topyekûn siber güvenliğe verdiği önem, Çin ve Kuzey Kore eksenli devam eden siber saldırıların etkisi hem de Rusya'nın Ukrayna'ya başlattığı savaşın Japonya'nın ulusal güvenlik stratejisinin revizyonu esnasında başlaması, savaşın; fiziksel muharebe, bilgi savaşı ve siber savaştan oluşan hibrit bir savaş niteliği taşıması çerçevesinde Tokyo'daki ulusal güvenlik tartışmasını büyük ölçüde etkilemesi bulunmaktadır. Bu noktada siber tehdit ve saldırılarla mücadele etme noktasında hükûmet, dezenformasyon durumunun analizi için yeni bir yapı kurulmasını öngörmektedir. Ayrıca yeni strateji ekseninde Dışişleri Bakanlığı, bilgi alanının izlenmesini iyileştirmek ve istihbarat analizini güçlendirmek için yapay zekâya başvurmayı, Savunma Bakanlığı ise bilgi savaşının durumunu kavramak için yapay zekâ teknolojisini kullanan otomatik bir bilgi toplama ve analiz sistemi tesis etmeyi planlamaktadır. Öte yandan, Savunma Geliştirme Programı'nda Japonya'nın ve ABD'nin ortak entegre caydırıcılık kabiliyetini daha da güçlendirmek için siber ve elektromanyetik operasyonlar dâhil olmak üzere alanlar arası operasyonlarda iş birliği ve birlikte çalışabilirliği daha ileri boyuta taşıması gerekliliği üzerinde durulmaktadır. Bununla beraber, Öz Savunma Kuvvetleri'nin siber birliklerinin siber tehditleri avlama yeteneklerinin güçlendirileceği belirtilmektedir ki bu da öz savunma kuvvetlerinin yakın dönemde siber karşı saldırı yeteneklerine sahip olacağı anlamı taşıdığını göstermektedir (Osowa, 2023). Öte yandan, "Kritik Altyapıların Korunmasına Yönelik Siber Güvenlik Politikası", kritik altyapı operatörlerinin üst yönetimi, stratejik yönetimi ve sistem personelini dâhil ederek kuruluş çapında müdahalelerin daha fazla teşvik edilmesine yardımcı olmaktadır. Günümüzün yeni tehditleri karşısında Japonya'nın güncellenmiş güvenlik stratejisini ortaya koyarak daha kapsamlı bir belge niteliğini haiz ulusal güvenlik stratejisi ise özellikle ülkenin siber güvenlik müdahale yeteneklerini güçlendirme ve siber güvenlikle ilgili en son uygulamaları ve teknolojileri benimseme ihtiyacını ele almaktadır (International Trade Administration, 2023).

Japonya siber müdahale stratejisini, ciddi siber saldırı olasılığını önceden ortadan kaldıran aktif siber savunma mekanizmasının devreye alınması hedefi çerçevesinde ortaya koymaktadır. Bu bağlamda aktif siber savunmayı uygulamak için "Siber Güvenlik İçin Olay Hazırlık ve Strateji Ulusal Merkezi'nin (NISC)", siber güvenlik alanındaki politikaları koordine edecek ve "Ulusal Öz Savunma Kuvvetleri'nin" siber birimlerini komuta edecek yeni bir siber güvenlik teşkilatı kurmak üzere yeniden yapılandırılacağı

belirtilmektedir. Öte yandan, aktif siber savunmayı uygulamak için Telekomünikasyon Yasası ve Yetkisiz Bilgisayar Erişimini Yasaklama Yasası gibi bazı yasaların revize edilmesi kararlaştırılmıştır. Diğer taraftan, Japonya'nın siber güvenlik alanındaki müdahale yeteneklerinin, önde gelen Batı ülkelerinin seviyesine eşit veya bu ülkelerin seviyelerini aşacak şekilde güçlendirilmesi gerekliliğinin altı çizilmektedir. Tüm bunlara ek olarak, yeni stratejik belgelerde siber güvenlik alanında geliştirilen duruş/tutum beş yıl içinde yerine getirilirse, Japonya'nın siber uzayda savaşabilecek yetenek ve kapasiteye sahip olacağı, öz savunma kuvvetlerinin siber birimlerinin, siber uzayı savunma görevini ABD ordusunun siber komutanlığı ile paylaşacağına ilişkin ortaya konan öngörü dikkati çekmektedir. (Osowa, 2023).

4. Siber Güvenlik Politikasında Rol Oynayan Aktörler ve Yapılan Harcamalar

Japonya'nın siber güvenliğinin sağlanması konusunda faaliyete geçirilen kurumlar önem arz etmektedir. Bu bağlamda siber güvenlikle ilgili yapılanmanın, Bilgi Teknolojileri Stratejik Merkezi, Siber Güvenlik Stratejik Merkezi, Milli Güvenlik Konseyi'nden oluşan üçlü bir mekanizma üzerine kurulu olduğu görülmektedir. Ayrıca söz konusu yapılanma içerisinde Kriz Yönetim Merkezi, Kabine İstihbarat Araştırma Ofisi ve Siber Güvenlik İçin Olay Hazırlık ve Strateji Ulusal Merkezi (NISC) önem teşkil etmektedir (Gady, 2017, ss. 11-12). Ek olarak 2012 yılında, acil durumlar karşısında kurumlar arası koordinasyonu sağlamakla yükümlü Siber Olaylar Mobil Yardım Ekibi (*Cyber Incident Mobile Assistant Team*) ve 2013 yılında Japonya Öz Savunma Kuvvetleri bünyesinde Siber Savunma Birimi kurulmuştur (Kallender & Hughes, 2017, ss. 122-128).

Gelişmiş Bilgi ve Telekomünikasyon Ağlarının Kurulmasına İlişkin Temel Yasa (Bilgi Teknolojileri Yasası) Ocak 2001'de yürürlüğe girmiştir. Söz konusu yasa çerçevesinde Bilgi Teknolojileri Stratejik Merkezi kurulmuş ve Japonya'yı beş yıl içinde bir bilgi teknolojisi devletine dönüştürme hedefiyle e-Japonya stratejisi ortaya konmuştur. Hızlı ve kapsamlı bilgi ve telekomünikasyon ağları aracılığıyla siber güvenliğe yönelik önlem alma sorumluluğunu haiz olan merkezin faaliyetleri ekseninde Haziran 2002'de "e-Japon Öncelikli Politika Programı" başlıklı ulusal bir proje kabul edilmiştir (Kaneko, 2001).

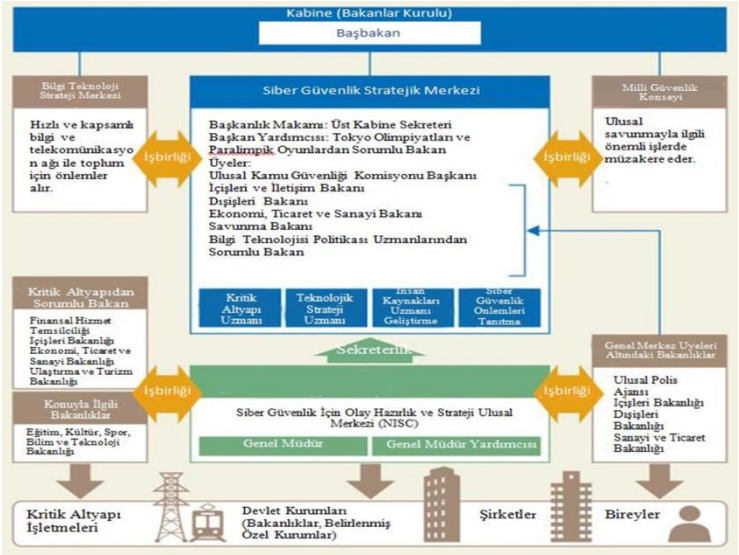
Bununla beraber, siber güvenlik politikalarında rol oynayan Milli Güvenlik Konseyi ulusal güvenlik konularında düzenli olarak ve gerektiğinde güçlü bir siyasi liderlikle Başbakan başkanlığında stratejik tartışmalar yürütecek bir forum sağlamak üzere 4 Aralık 2013 tarihinde ve 2014 yılında siber güvenlik politikalarının etkin ve kapsamlı bir şekilde yürütülmesi için Bakanlar Kurulu altında Siber Güvenlik Stratejik Merkezi kurulmuştur. Milli Güvenlik Konseyi, 2021 yılı itibariyle 9 üyeyi içermektedir: Başbakan, Maliye Bakanı, İçişleri ve Haberleşme Bakanı, Dışişleri Bakanı, Ekonomi-Ticaret ve Sanayi Bakanı, Altyapı-Ulaştırma Bakanı, Turizm Bakanı, Üst Kabine Sekreteri ve Kamu Güvenliği Komisyonu Başkanı. Siber Güvenlik Strateji Merkezi ise Başkan, Başkan Yardımcısı ve Merkez üyelerini içermektedir. Üst kabine sekreterinin başkanlığını ve Tokyo Olimpiyatları ve Paralimpik oyunlardan sorumlu bakanın başkan yardımcılığı yaptığı merkezde, Ulusal Kamu Güvenliği Komisyonu Başkanı, İçişleri ve İletişim Bakanı, Dışişleri Bakanı, Ekonomi, Ticaret ve Sanayi Bakanı, Savunma Bakanı ile Başbakan tarafından belirlenen siber güvenlik konusunda bilgi ve deneyime sahip uzmanlar siber güvenliğe yönelik faaliyetler üzerine çalışmaktadır (Ministry of Foreign Affairs of Japan, t.y.). Merkezin temel görevleri ise şu şekilde özetlenebilir:

- Siber güvenliğe yönelik stratejileri ve politikaları belirleyerek, uygulanmasını sağlamak
- Tüm kurumlar bağlamında siber güvenlik önlemlerini ortak hâle getirmek
- Siber saldırıların nedenlerini analiz etmek ve bunlara yönelik önlemleri belirlemek
- Siber güvenlik konusunda bütçe belirlemek ve genel koordinasyonu güçlendirmek (Global Regulation, 2016).

Öte yandan, bugün yaklaşık 200 çalışanı ile nispeten küçük bir kuruluş olmasına rağmen gün geçtikçe daha önemli hâle gelen Siber Güvenlik İçin Olay Hazırlık ve Strateji Merkezi (NISC), Japonya'nın siber güvenlik politikasında etkin bir rol oynamaktadır. 2005 yılında kurulan NISC, kurulduğu ilk yıllarda 22 personele sahipken aradan geçen yaklaşık 18 yılda kapasitesini neredeyse 10 katına çıkarmıştır. NISC; siber güvenliğe ilişkin ulusal strateji ve politika geliştirme, uluslararası stratejileri belirleme, bu alana ilişkin koordinasyonu sağlama, kritik altyapıların korunması ve acil durum analizlerinin yapılması gibi konulardan sorumludur (Ogawa & Tsuchiya, 2021, s. 18).

Bilgi Teknolojileri Stratejik Merkezi, Siber Güvenlik Stratejik Merkezi ve Milli Güvenlik Konseyi politika oluşturma ve koordinasyonun güçlendirilmesi konularında beraber çalışmaktadır. Söz konusu bu durum şekil 1'de görülmektedir. Mevzubahis kurumlara ek olarak siber güvenlik politikasında etkin bir rol oynayan Ulusal Polis Ajansı hem kolluk hem de istihbarat teşkilatı olarak görev yapmaktadır. Bu noktada soruşturma ve siber suç faillerinin tutuklanması gibi kolluk kuvvetleriyle ilgili ve bir istihbarat teşkilatı olarak, ciddi siber saldırılar gerçekleşmeden önce bunları önlemekle ilgili görevleri ifa etmektedir. Ayrıca, genel kamu güvenliği ve suçla mücadele önlemlerinin bir parçası olan ajansın altında bilgi, birikim ve deneyim paylaşımının sağlanması için 2014 yılında Siber Suçlar Kontrol Merkezi kurulmuştur (Ogawa & Tsuchiya, 2021, s. 18).

Diğer taraftan, 2001 yılında iki ayrı bakanlığın birleştirilmesi ekseninde kurulan İçişleri ve Haberleşme Bakanlığı; bilgi, iletişim ve posta hizmetleri sektörlerinin yanı sıra idari kuruluşlar, seçim sistemleri ve afet önleme gibi konuları düzenlemektedir. Ayrıca bilgi ve iletişim için yeni teknolojik sistemler geliştiren Bakanlık, operatörlere lisans verilmesi, ilgili düzenlemeler için tarife ve vergilerin belirlenmesinden sorumludur (Global Edge, t.y.). Bakanlığın siber güvenlikteki rolünün ise küresel kablosuz ağ altyapısının beşinci nesline (5G) geçilmesiyle beraber güçlendirildiği görülmektedir. Siber güvenlikten sorumlu bir diğer aktör Ekonomi, Ticaret ve Sanayi Bakanlığı'nın bünyesinde oluşturulan Siber Güvenlik Birimi'dir. Özellikle kritik altyapıların korunmasından sorumlu olan mevzubahis birimin, genel bazda siber güvenliğin sağlanması için yeterli deneyime ve kaynağa sahip olduğu vurgulanmaktadır. Ayrıca son dönemde tedarik zinciri güvenliği konusuna odaklanan birim, Siber Güvenlik Strateji Merkezi ve NISC ile iş birliğini güçlendirmektedir. Savunma Bakanlığı ise siber güvenliğe ulusal güvenlik açısından yaklaşmaktadır. Ancak bilindiği üzere siber saldırıların, geleneksel silahlarla yapılan saldırılardan doğası gereği farklı olması bilinciyle siber güvenliğin ulusal güvenlik içine dâhil edilmesi hususunda son derece ihtiyatlı bir yaklaşım benimsemektedir. Siber güvenlik alanında gerçekleştirilen diplomatik müzakerelerde rol oynayan Dışişleri Bakanlığı, 14 ülke ve bölge ile aktif ikili siber diyalog yürütmektedir (Ogawa & Tsuchiya, 2021, ss. 18-21).



Şekil 1. Siber Güvenlik Yapılanması
Kaynak: (National Information Security Policy Council, t.y.; Demir, 2020, s. 238).

Öte yandan üzerinde durulması gereken bir başka husus, kamusal kurumlarla beraber özel sektörün de siber güvenlik alanında ifa ettiği roldür. Bu noktada siber saldırılara müdahale etmek ve siber saldırılardan kaynaklanan zararı en aza indirmek ve kurumlar arasında koordinasyonun sağlanması noktasında JPCERT/CC'nin sorumlu olduğu görülmektedir. Dünyanın dört bir yanındaki siber güvenlik uzmanları, giderek çeşitlenen siber tehditlerden kaynaklanan olayları uygun şekilde ele alabilmek için Bilgisayar Güvenliği Olay Müdahale Ekipleri'nin (CSIRT'ler) kurulmasını savunmaktadır. Japonya'daki birçok şirket ve kuruluş bu hususu dikkate alarak, kendi CSIRT'lerini tesis etmiştir. CSIRT'ler, bilgi ve teknolojiyi

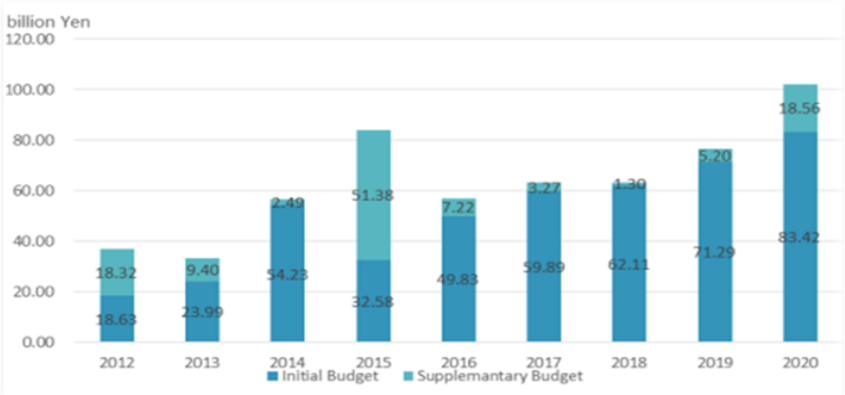
paylaşarak siber tehditlere karşı yanıt verme yeteneklerini geliştirmektedir. Herhangi bir devlet kurumundan veya şirketinden bağımsız bir kuruluş olan JPCERT/CC, siber güvenlik açısından koordinasyonun sağlanması için Japonya'nın irtibat noktası olarak yurtiçinde ve yurtdışındaki CSIRT'lerle eş güdümlü bir şekilde çalışmaktadır. Ayrıca yurt dışındaki CSIRT'lerin kurulmasını destekleyerek, dünya çapında temas noktaları geliştirmekte ve onları birbirine bağlayan bir köprü görevi görmektedir (JPCERT/CC, t.y.). Bununla beraber, 2021 yılı itibariyle 254 çalışana sahip olan Japonya Ağ Güvenliği şirketi ve Japonya İş Federasyonu siber güvenlik konusundaki diğer aktörlerdir. Japonya hükûmetiyle birlikte çalışan mevzubahis bu aktörler, toplum 5.0 hedefine ulaşılması ve kamuoyunun bu alandaki bilinçlilik düzeyinin artırılması noktasında çeşitli faaliyetlerde bulunmaktadır (Ogawa & Tsuchiya, 2021, ss. 21-22).

Ayrıca altı çizilmesi gereken bir başka konu, siber uzay politikası oluşturmanın organizasyonel yapısının siber güvenliğinkiyle benzerlik taşımasıdır. Bu noktada 2008 yılında, Japonya'daki uzay faaliyetleri için yasal bir çerçeve sağlamak üzere "Temel Uzay Yasası" çıkarılmıştır. Başbakan başkanlığındaki Ulusal Uzay Politikası Stratejik Merkezi'ne ek olarak, ulusal uzay politikası için bakanlıklar arası koordinasyon organı olarak hareket etmek üzere Kabine Ofisinde bulunan Ulusal Uzay Politikası Sekreterliği (NSPS) kurulmuştur. Bununla beraber, Uzay Politikasına İlişkin Temel Plan, ana ulusal uzay planlama belgesini teşkil etmekte ve çoğu akademi ve endüstriden gelen uzay uzmanlarından oluşan Ulusal Uzay Politikası Komitesi'nin tavsiyeleri üzerine NSPS tarafından sıklıkla revize edilmektedir. Ayrıca NSPS, hükûmetin uzay işlerinde yetki alanına sahip çok sayıda bakanlık ve kurumunun farklı rollerini ve katkılarını belirleyerek, ulusal uzay gelişimine ilişkin politikaların formüle edilmesine ve tutarlı bir şekilde kullanılmasına hizmet etmektedir. Savunma tarafında ise öz savunma kuvvetleri, Mayıs 2020'de ana görevi 5.800 km'nin üzerindeki yörüngeleri kapsayan bir uzay durumsal farkındalık radarını işletmek olan ve 2023 mali yılında faaliyete geçmesi beklenen Uzay Operasyonları Filosu'nu hayata geçirmiştir. Japon uydularına yönelik elektronik müdahaleleri izlemeye odaklanan ikinci bir filo ve iki filoyu birleştiren "Uzay Operasyonları Grubu" olarak nitelendirilen kapsayıcı bir yapı kurulmuştur (Iwamoto &Verspieren, 2023).

Bununla beraber Japonya hükûmeti, uzayın sürdürülebilirliği ile ilgili çeşitli önlemler almış olmasına rağmen uzay operasyonlarının güvenliğine ve uzay varlıklarının hem sivil hem de savunma amaçlı kullanımına yönelik olası risklere ilişkin herhangi bir değerlendirme yapmamış veya yayımlamamıştır. Öte yandan, Japonya'nın genel olarak uzay güvenliğinin ve sürdürülebilirliğin teşvik edilmesinde son derece olumlu bir rol oynadığı, hem politika hem de onu destekleyen teknolojiler açısından gündemi teşvik eden önde gelen devletlerden biri olduğu görülmektedir. Ancak Japonya için sorun, küresel bir uzay trafiği koordinasyonu çerçevesi oluşturma çağrısı yapmak veya uzay güvenliği ve sürdürülebilirliği konusunda daha önemli küresel taahhütlerle uğraşmaya istekli olup olmamasından kaynaklanmaktadır (Iwamoto & Verspieren, 2023).

Tüm bunlara ek olarak, Covid-19 pandemi döneminden itibaren çalışma koşullarının ofisten çevrimiçi ortama kaymış olması doğrultusunda kimlik avı, kötü amaçlı yazılım, kimlik hırsızlığı ve şirket sistemlerine yönelik ihlaller gibi siber güvenlik tehditlerinin ülke genelinde keskin bir şekilde arttığı görülmektedir. Ayrıca fidye yazılımı saldırıları ve gizli bilgi hırsızlığı bağlamında tedarik zinciri güvenlik açıklarında önemli bir artış yaşanmaktadır. Bu noktada siber güvenliğin sağlanması konusunda 2012 yılında 36,95 milyar Japon Yeni bir bütçe söz konusuyken bu oran 2020 yılında 101,98 milyar Japon Yeni'ne yükselmiştir ki bu durum Japonya hükûmetinin NISC'in etkinlik kapasitesini güçlendirerek siber güvenliğe öncelik vermesi hususunu göstermektedir (Ogawa & Tsuchiya, 2021, ss. 13-14). Şekil 2'den görüldüğü üzere Japonya hükûmeti siber güvenliğe yönelik bütçesini her yıl artırmaktadır. Bununla beraber, Mayıs 2022'de IDC tarafından yayımlanan istatistikî rapor ekseninde dünyanın en kalabalık nüfusunu haiz 11. ülkesi olan ve üçüncü en büyük ekonomisine sahip Japonya'nın siber güvenliğe yönelik harcamalarının bir önceki yıla göre %16 artışla 3,6 milyar dolara yükseldiği ortaya konmaktadır (International Trade Administration, 2023). Öte yandan, onaylanan 114,3 trilyon yenlik (865 milyar dolar) 2023 mali yılı bütçe taslağı çerçevesinde ulusal savunma harcamalarına – ki uzun zamandır 5 trilyon yen ile (36 milyar dolar) sınırlandırılıyordu- 6,8 trilyon yen ayırırken (Euronews, 2022) siber saldırılara karşı savunmanın güçlendirilmesi için 34 milyar yen (312 milyon dolar ve uzay projeleri için ise 79 milyar yen (765 milyon

dolar) harcanması planlanmaktadır (Savunma Sanayi, 2021). Diğer taraftan, 2023'ten başlayarak beş yılda 43 trilyon yen siber savunma harcaması yapılması hedeflenmektedir (Defence of Japan, 2023).



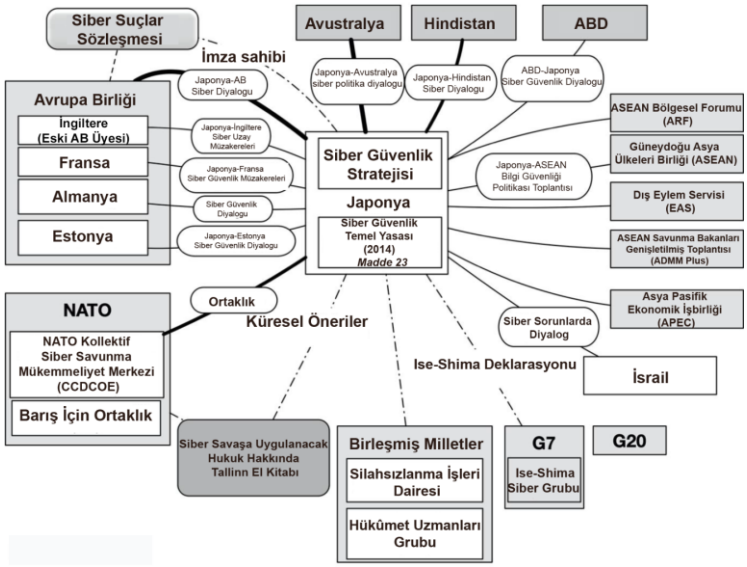
Şekil 2. Japonya Hükûmet Bütçesinde Siber Güvenliğe Ayrılan Pay
Kaynak: (Ogawa ve Tsuchiya, 2021, s. 14).

5. Japonya'nın Siber Güvenlik Politikası Çerçevesinde İş Birliği

Ulusal ve uluslararası güvenlikle beraber topyekûn barış ortamının sağlanması konusuyla yakın ilişkili olan siber güvenlik bağlamında Japonya uluslararası iş birliklerine önem vermektedir. Bu noktada Uluslararası Siber Güvenlik İşbirliği Stratejisi çerçevesinde endüstriyel ve akademik kurumlar da dâhil olmak üzere tüm yerel paydaşlar tarafından siber güvenlik alanında uluslararası iş birliği ve karşılıklı yardımlaşma için ortak bir anlayış paylaşıldığı görülmektedir (Information Security Policy Council, 2013). Son derece iyi dizayn edilmeye çalışılan Japonya'nın siber diplomasisi bağlamında Dışişleri Bakanlığı önem teşkil etmekte; özgür, adil ve güvenli bir siber uzayın nasıl sağlanacağına ve diğer ülkelerle koordinasyonun nasıl güçlendirileceğine ilişkin konularda etkin bir rol oynamaktadır (MOFA, t.y.). Bu noktada Japonya çok paydaşlı ve hükûmetler arası bir yaklaşımla özgür ve güvenli bir siber uzay ortamının şekillenmesine aktif olarak katkıda bulunmaya yönelik politikalar takip etmektedir. İkili ve çok taraflı diyaloglar ve Güneydoğu Asya Ülkeleri Birliği (ASEAN) gibi bölgesel oluşumlar çerçevesinde siber uzaya ve siber güvenliğe yönelik kapasitenin geliştirilmesine ilişkin uluslararası normlar koyma konusunda aktif olmaya çalışmaktadır. Örneğin 2004 yılında Japonya, bilgi güvenliğinin sağlanması konusunda hayata geçirilecek bir proje için Kore ve Çin ile çalışmaya başlamış ve bu doğrultuda bir çalışma grubu oluşturulmuştur. Uluslararası güvenlik sorunlarına da yol açan siber alanda, güvenlik önlemleri alınması yönündeki çalışma grubunun faaliyetleri bölgesel iş birliğini güçlendirmiştir (Austin, 2018, ss. 186-187).

Öte yandan 2006 yılında Japonya, ABD, Çin, Rusya, Kuzey Kore ve Güney Kore'nin Devlet Başkanları, Dışişleri ve Savunma Bakanlarının da yer aldığı ASEAN Bölgesel Forumu'nda, bölgesel ekonomi ve insan refahı için siber güvenliğin yasal olarak ve iş birliği ekseninde sağlanabileceğinin altı çizilmiştir (Austin, 2018, s. 189). Ayrıca 2017 yılında Vietnam Ordusundaki personele siber güvenlik semineri verilerek, uluslararası ve bölgesel iş birliği kapsamının güçlendirildiği görülmektedir (Japan Ministry of Defence, 2020). Diğer taraftan Japonya, sadece bölge ülkeleriyle iş birliğini geliştirmeye çalışmamaktadır. Bu noktada Tokyo; İsrail, Hindistan, Avustralya, İngiltere, Fransa, Almanya, Estonya ile de siber alandaki iş birliğine yönelmiştir (Şekil 3). Ayrıca bu alanda NATO ile iş birliğini geliştiren Japonya, 2019 yılında NATO'nun ev sahipliğinde gerçekleşen siber savunma tatbikatına gözlemci statüsünde katılım sağlamıştır (Japan Ministry of Defence, 2020).

Japonya'nın bu alanda önemli bir hedefi olan kapasite güçlendirme ekseninde özellikle kritik altyapıların korunmasına odaklandığı görülmektedir. Bu noktada "Uluslararası İzleme ve Uyarı Ağı" önem teşkil etmektedir (Schuetze, 2020). Diğer yandan Japonya'nın amacı, uluslararası toplum nazarında hiçbir bölgeyi siber tehditlere karşı savunmasız bırakmamaktır. Öyle ki söz konusu amaç ekseninde insan kaynakları geliştirmeye, olay müdahalesi ve bilgi paylaşımı oluşturmak için etkin mekanizmalar kurarak küresel düzeyde kapasite güçlendirme faaliyetlerine aktif olarak katkıda bulunmaya çalışılmaktadır (OECD, 2019).



Şekil 3. Japonya'nın Siber Güvenlik Alanındaki İş Birlikleri
Kaynak: (Vosse, 2019, s. 7'den alınan verilerle yazar tarafından oluşturulmuştur).

Japonya'nın siber güvenlik politikasının yürütülmesi çerçevesinde ana ortağının ABD olduğu bilinmektedir. ABD ve Japonya arasında siber güvenlik konusunda iş birliğinin güçlendirilmesi önem teşkil etmektedir. Bu noktada iki aktör arasında en son Ocak 2023'de bir iş birliği anlaşması imzalandığı görülmektedir (Reuters, 2023). Siber güvenliğe yönelik iki devlet arasında oluşturulan mekanizmaların genel çerçevesi ise şu şekildedir:

- Japonya-ABD siber diyalogu
- İnternet ekonomisinde Japonya-ABD politika iş birliği diyalogu
- Tehditlerle ilgili bilgi paylaşım süreçleri
- Japonya-ABD arasında güvenlik düzenlemeleri aracılığıyla siber olay müdahale mekanizmaları
- ABD–Japonya siber savunma politikası çalışma grubu
- ABD-Japonya ortak siber savunma tatbikatı (Schuetze, 2020).

Öte yandan, Güneydoğu Asya coğrafyasında kapasite geliştirme ve teknik uzmanlık açısından önemli bir rol üstlenmeye çalışan Japonya'nın bölgedeki bilgi paylaşımına katkıda bulunmak için şu faaliyetleri hayata geçirdiği görülmektedir:

- ASEAN–Japonya bilgi güvenliği politikası toplantısının yapılması
- ASEAN–Japonya Siber Güvenlik Kapasite Merkezi'nin Tayland'da kurulması
- JASPER - Japonya–ASEAN güvenlik ortaklığının oluşturulması
- Asya bölgesindeki bilgisayar güvenliği olayı müdahale ekipleriyle iş birliği yapılmasını merkez noktasına alan TSUBAME projesinin hayata geçirilmesi (Schuetze, 2020).

Tüm bunlara ek olarak siber güvenlik alanında Japonya, Avrupa Birliği (AB) üye devletleriyle de yakın temas hâlindedir. Son dönemlerde iş birliği ve ortak değerler odağı çerçevesinde ikili ilişkilerin daha ileri boyuta taşınması için AB-Japonya Siber Diyalogu tesis edilmiştir ki bu ortaklığın 2018 yılında serbest veri akışı anlaşmasıyla kendini gösteren başarılı bir ticaret ortaklığı üzerine kurulduğu görülmektedir. Bu noktada AB ve Japonya arasındaki ilk Siber Diyalog ekseninde özgür ve açık bir siber alan üzerinde anlaşmaya varılmış, çok paydaşlı bir model ve alana yönelik normları tartışmak için bölgesel forumları kullanmanın önemi kabul edilmiş ve şeffaflık yoluyla güven oluşturmayı teşvik edici adımların atılması üzerine anlaşmaya varılmıştır. Yine 2018 yılında iş birliği yapılmasını ve siber suçlarla zamanında ve etkili bir şekilde mücadele edilmesini sağlamak amacıyla Europol ve Japonya Ulusal Polis Ajansı arasında siber alana ilişkin bir çalışma anlaşması imzalanmıştır. 2019 yılında Japonya ile AB arasındaki güvenlik ortaklığı

için siber diplomasi konularını da içeren Stratejik Ortaklık Anlaşması'nın imzalanması ise ikili ilişkilerdeki bir diğer kilometre taşını teşkil etmiştir. Nitekim genel güvenlik ortaklığını güçlendirmek için yeni kanallar sağlayan söz konusu anlaşma, 40'dan fazla ortak alanda siyasi ve sektörel iş birliğini ve ortak eylem geliştirilmesini teşvik etmiştir (Schuetze, 2020). Ayrıca Japonya'nın uluslararası güvenlik çerçevesinde bilgi ve telekomünikasyon alanındaki gelişmelere ilişkin birbirini izleyen altı BM Hükûmet Uzmanları Grubu (2004–2021) çalışmalarına, bilgi ve iletişim teknolojilerinin kullanımında güvenliğin sağlanmasına yönelik "Açık Uçlu Çalışma Grubu" gibi çok taraflı çerçevelere aktif olarak katıldığı görülmektedir (2021–2025) (Iwamoto & Verspieren, 2023).

6. Teorik Analiz

Japonya'nın siber güvenlik politikalarını analiz eden bu çalışma çerçevesinde elde edilen veriler teorik bir düzleme yansıtılarak, bu verilerle teorinin sunduğu çıktıların ne ölçüde uyum gösterdiği analiz edilmektedir. Bu noktada devreye tarihsel kurumsalcılık kuramı ve iş birliği modeli girmektedir.

Tarihsel kurumsalcılık teorisi, merkez noktasına kurumları koymaktadır. Teori ekseninde kurumlar hem fiziki yapıları hem de fiziki olmayan (sözleşmeler, prosedürler, normlar ve rutinler gibi) yapıları kapsamaktadır (Hall & Taylor, 1996: 938). Kurumlar zaman içinde nasıl bir gelişim göstermektedir? Kurumlar, aktörlerin davranışlarını, kararlarını, politikalarını, tutumlarını ne yönde etkilemektedir? gibi soruları önceliklendiren teori bağlamında zaman unsuru önem teşkil etmektedir (Pierson & Skocpol, 2002, s. 695; Pollack, 2009, s. 127). Bununla beraber sorunları tanımlamaya yardımcı olan kurumların, kararları ve tercihleri netleştirdiği ifade edilmektedir (March & Olsen, 1984, s. 739; Skocpol & Finepol, 1982, s. 262; Wildavsky, 1987, s. 12).

Diğer yandan teori, kurumlar ve aktörler arasındaki ilişkiyi yol/izlek bağımlılığı çerçevesinde ele alırken elde edilen sonuçlar kesintiye uğramış/ noktalanmış denge mekanizması çerçevesinde analiz edilmektedir. Yol bağımlılığı ekseninde "kritik eşiklerle karşı karşıya kalınana kadar başlangıçta alınan kararlar, daha sonrakiler üzerinde belirgin bir etki yaratmaktadır" şeklinde bir varsayım ortaya konmaktadır (Hall & Taylor, 1996, s. 941; Pollack, 2009, s. 127). Bu noktada başlangıçta alınan kararların, tercihlerin önem arz ettiği ve alınan karar/tercih sonrasında bu karardan veya tercihten dönmelerinin zor olduğu belirtilmektedir (Pierson, 2000, s. 251; Pollack, 1996, ss. 437-438). Bu zorluğun altında ise mevcut yapıya uygun şekilde kararların alınması ve tercihlerin belirlenmesi ekseninde "kenetlenme" etkisi bulunmaktadır (Thelen, 1999, ss. 369-404). "Değişime karşı direnç gösterme" olarak betimlenen bu önermeye rağmen teori; kararların, politikaların ve tercihlerin değişebileceğini de belirtmektedir ki bu noktada devreye kesintiye uğramış/noktalanmış denge mekanizması girmektedir (Pierson, 2000, s. 259; Krasner, 1984, s. 240). Mevzubahis mekanizma, kritik olayların ve eşiklerin yaşandığı durumlarda yeni kararlara/tercihlere yönelinmesi hususunu ortaya koymaktadır. Bir diğer ifadeyle dışsal faktörler tarafından kararların bozulabileceği, tercihlerin ve politikaların değişebileceği ve yeni çözümlere gidilmesini gerektiren süreçler yaşanabileceği vurgulanmaktadır (Collier & Collier, 1991). Tüm bunlara ek olarak, ilgili karar doğrultusunda yeni kurumlar tesis edilmesi ve/veya mevcut kurumların yetkilerinin artırılması hususlarına "olumlu geri bildirim döngüsü" çerçevesinde atıf yapıldığı görülmektedir (Pierson, 2004, ss. 20-21; Lockwood vd., 2016).

Öte yandan, iş birliğinin birçok tanımı ve anlamı bulunmaktadır. Bağlam, zaman, kültür ve koşullar, hem terimin tanımlanmasında hem de fiili olarak uygulanmasında önemli bir rol oynamaktadır. İş birliği kalıcı, geçici veya durumsal olabilmekte; hem resmi düzenlemelere hem de gayri resmi anlaşmalara dayandırılabilmektedir. Siber güvenlik bağlamında iş birliği modeli ise bir siber saldırının yol açtığı zararı önlemek ve/veya en aza indirmek için kurumsallaşmış mekanizmalar sunmaktadır. Bir siber saldırının sonuçlarını ve etkisini en aza indirmek için gereken kaynaklar göz önüne alındığında, iş birliği modelinin amacı, mevzubahis saldırıların hem doğrudan hem de dolaylı maliyetlerini en aza indirmektir. Bu noktada model, "bir siber saldırıyı önlemek konusunda ortak bir çaba göstermenin, başarılı bir saldırının maliyetlerini karşılamaya tercih edildiği" varsayımına dayanmaktadır. Bir diğer ifadeyle iş birliği modelinin kabul edilmesinden elde edilen bir fayda olmalıdır. Bu fayda, herhangi bir ilgili maliyetten daha ağır basmalıdır, aksi takdirde söz konusu iş birliği devreye alınmamaktadır. Nitekim ortaya konan bu varsayım önem teşkil etmektedir çünkü siber tehditlerin etkisi, iş birlikçi bir model benimsemenin avantajlarının fark

edilememesi nedeniyle artmaktadır. Bu bağlamda siber saldırılar nedeniyle hayata geçirilen bir iş birliği anlaşmasının şu hususları içermesi gerekliliğine dikkat çekilmektedir:

- Ortak hedefler konusunda fikir birliğinin sağlanması
- Maliyet-fayda değerlendirmesi yapılması
- Anlaşmadan çekilme mekanizmalarının oluşturulması
- Anlaşmanın belirlenmiş parametreleri içermesi
- Anlaşmaya varılan uygulama mekanizmalarının tesis edilmesi (Guiora, t.y.).

Bununla birlikte, siber saldırıların oluşturduğu riskler ve tehditler, iş birliğini zorunlu kılan mekanizmaların kullanılmasını ön plana çıkarmaktadır. Bu noktada öncelikle gönüllü iş birliğinin kurulması odak noktası olmasına rağmen eğer bu mümkün değilse zorunlu iş birliği ihtimali üzerinde durulması gerekliliği ortaya konmaktadır. Öte yandan kişi, devlet, kurum ve kritik altyapıları hedef alan siber saldırılar bilindiği üzere risk unsurunu artırmaktadır. Risk kavramı ise iş birliğine alan açmaktadır. Diğer taraftan, potansiyel bir riskin olmaması, bir anlaşmaya girme dürtüsünü tamamen ortadan kaldırılmasa bile önemli ölçüde minimum düzeye indirmektedir. Diğer taraftan iş birliği veya karşılıklı güven, tüm konularda anlaşma anlamına gelmediği gibi çıkarların, değerlerin ve hedeflerin mükemmel bir birleşimini de yansıtmamaktadır. Ancak bir iş birliği modeli; siber tehditlerin olası sonuçları göz önüne alındığında, tarafların çatışan çıkarları olsa bile ortak bir noktada buluşmanın kabul edildiğini ortaya koymaktadır. Nitekim iş birliği ekseninde güçleri birleştirmenin siber tehditlere karşı daha etkili önlemlerin geliştirilmesini önemli ölçüde artıracağı vurgulanmaktadır. Bu noktada geliştirilen iş birliği modeli doğrultusunda şu hususlara dikkat edilmesi gerekliliğinin altı çizilmektedir:

- Tehdit tanımlaması
- Güvenlik açığının en aza indirilmesi
- Maliyet fayda analizi
- Uzmanlarla birlikte karmaşık simülasyon çalışmaları yapılması doğrultusunda savunmasızlık noktalarının daha iyi belirlenmesi
- Gelecekteki saldırıların etkisini en aza indirme (Guiora, t.y.).

Tarihsel Kurumsalcılık teorisi ve iş birliği modeli çerçevesinde Japonya'nın siber güvenlik politikaları analiz edildiğinde mevzubahis politikaların hem teorinin hem de modelin ortaya koyduğu çıktılarla büyük ölçüde örtüştüğü görülmektedir. Japonya siber güvenlik alanında sahip olduğu fiziki ve fiziki olmayan kurumlarıyla tarihsel kurumsalcılık teorisinin sunduğu varsayımların analiz edilmesine olanak sağlamaktadır. Nitekim teorinin kurumlara verdiği "öncelik" durumunun Japonya'nın siber güvenlik politikaları bağlamında hayata geçirildiği görülmektedir. Öyle ki siber güvenlik alanında hem fiziki hem de fiziki olmayan (kanunlar, stratejiler vb.) kurumlar bazında 2000'li yıllarla beraber kurumsallaşmaya gidilmekte, ama özellikle 2011'den günümüze peyderpey ve istikrarlı bir biçimde ilerleme kaydedilmektedir. Japonya'nın siber güvenlik politikasına yönelik 2000'li yılların başından günümüze kadar yapılan tarihsel okumadan elde edilen çıktılar şu hususları ortaya koymaktadır: 1) Japonya, bilgi ve ulusal güvenliği birbiriyle ilişkili olarak tanımlamakta ve bu doğrultuda siber güvenliğe yönelik kurumsal yapıyı güçlendirme eğiliminde hareket etmektedir. 2) Kritik altyapıların korunması ve buna yönelik mekanizmalar geliştirilmesi önem arz etmektedir. 3) Özgür, adil ve güvenli bir siber alanın tesis edilmesi üzerinde durulmaktadır. 4) Siber güvenlik önlemlerinin yüksek yoğunluklu bir düzeyde alınmasına odaklanılmaktadır. 5) Kamu-özel sektör, bölge dışı devletler, bölgesel ve küresel örgütlerle iş birliğinin ve koordinasyonun geliştirilmesi önem teşkil etmektedir. Altı çizilen tüm bu hususlar, Japonya'nın ortaya koyduğu yasalar ve strateji belgelerinde yer almaktadır. Bu minvalden hareketle başta alınan kararların ve izlenen politikaların daha sonraki karar/politikalar üzerinde etki ederek, devamlılığı betimleyen tarihsel kurumsalcılığın yol/izlek bağımlılığı mekanizmasıyla Japonya'nın siber güvenlik politikasının örtüştüğü, başta uygulamaya alınan politikaların daha sonraki süreçlerde daha da güçlenerek devam ettiği görülmektedir. Öte yandan, teorinin vurguladığı kritik olaylarla/eşiklerle karşılaşıldığı zaman, karar/politikaların değişebileceğini betimleyen kesintiye uğramış/noktalanmış denge mekanizmasının işlerliğine yönelik örnekler söz konusudur. Öyle ki bahsedildiği üzere 2011 yılında Mitsubishi Heavy Industries şiketine, Temsilciler Meclisine, hükûmet ağlarına yönelik gerçekleştirilen siber saldırılar ve topyekûn siber saldırıların niceliksel olarak büyük oranda

artması doğrultusunda 2013 yılında yeni bir siber güvenlik strateji belgesi yayımlanmıştır. Öz savunma kuvvetlerinin savunma kapasitesinin güçlendirilmesinden ilk kez söz eden belge çerçevesinde sivil mekanizmadan askeri bir yapıya doğru gidilmesi hedefi ortaya konmuştur. Diğer yandan bahsi geçen bu durumun 2022 yılında kabul edilen yeni güvenlik stratejisi bağlamında çok daha somut bir zemine oturduğu görülmektedir. Nitekim Rusya, Çin, Kuzey Kore faaliyetlerinden algılanan tehdit, Rusya'nın uluslararası hukuku göz ardı ederek Ukrayna'ya gerçekleştirdiği saldırı ve bunun Çin ve Tayvan arasında yaşanma olasılığı, Çin'in askeri gücünü artırması, Senkaku/Diaoyu adaları konusunda Çinle yaşanan gerilim ve Kuzey Kore'nin nükleer silah denemelerine devam etmesi çerçevesinde Japonya; savunma yeteneklerini, kapasitesini ve bu doğrultuda savunma harcamalarını artıracağını, karşı müdahale yeteneklerini Batı ülkeleriyle eş bir seviyeye hatta onları aşacak şekilde güçlendireceğini net bir şekilde ortaya koymakta ve bunun siber güvenlik alanına da yansıyacağını ifade etmektedir. Bu noktada mevzubahis örnekler doğrultusunda Japonya'nın pasifist politikadan militarist bir duruşa kayması, tarihsel kurumsalcılığın kesintiye uğramış/noktalanmış denge mekanizmasını yansıtmaktadır. Son olarak, Ulusal Öz Savunma Kuvvetlerinin siber birimlerini koordine edecek yeni bir birimin tesis edilmesi üzerinde durulması ve Siber Güvenlik Stratejik Merkezi, NISC gibi mevcut kurumların yetkilerinin artırılması ise teorinin olumlu geri bildirim döngüsünü göstermektedir.

Siber saldırıların neden olduğu zararı önlemek veya minimum düzeye getirmek için kurumsallaşmış iş birliğini ve koordinasyonu yansıtan iş birliği modeli çerçevesinde Japonya'nın siber güvenlik alanında başta ABD olmak üzere İsrail, Hindistan, Avustralya, İngiltere, Almanya, Fransa, Estonya ile iş birliğini güçlendirdiği görülmektedir. Bir diğer ifadeyle siber güvenlik bağlamında iş birliğine önem veren Tokyo, ortaklarla karşılıklı yardımlaşma üzerine kurulu, çok paydaşlı ve ikili diyalog ve anlaşmalar çerçevesinde hem devletler hem de bölgesel ve küresel örgütlerle uluslararası ve bölgesel iş birliğini geliştirmeye yönelik bir politika takip etmektedir. Bu noktada Japonya'nın tek ulusal güvenlik garantörü olan ABD ile siber diyalogları çerçevesinde söz konusu ittifakın daha da güçlendirilmesi, ulusal siber politikaların karşılaştırılması, planlama ve kritik altyapıyı koruma çabalarında iş birliği yapılması gibi hususlar üzerinde yoğunlaştıkları görülmektedir. Öte yandan Japonya ve AB, bir taraftan iş birliklerini siber güvenlik alanında yoğunlaştırma, diğer taraftan siber uzayı; hukukun üstünlüğü, özgürlük ve liberal dünya düzeninin istikrarı gibi liberal normları ve değerleri yaymak için etkin bir platforma dönüştürme konusunda anlaşmaya varmıştır. Diğer yandan, Japonya'nın Avrupa'daki en yakın güvenlik ortağı hâline gelen İngiltere ve Tokyo arasında özgür, barışçıl ve güvenli bir siber alanın tesis edilmesi için çeşitli toplantılar gerçekleşmekte, ASEAN'ında içinde bulunduğu çalıştaylar organize edilmektedir. Bununla beraber, Fransa ve Japonya Dışişleri ve Savunma Bakanları arasında gerçekleştirilen toplantılarda insan hakları ve hukukun üstünlüğü ile yönetilen güvenli bir siber alan inşa etmenin her iki ülkenin de çıkarına olduğunun her defasında yinelenmesi dikkati çekmektedir. Ayrıca başlangıçta geleneksel konularda iş birliği yapan Japonya ve NATO, son dönemlerde siber güvenlik konusunda yakın iş birliği içerisindedir. Yapılan istişarelerde ortak zorluklarla yüzleşmek için birlikte çalışmanın önemi vurgulanmakta, güçlü ortaklıkların siber tehdit ve risklerin bertaraf edilmesinde kilit rol oynadığı vurgulanmaktadır. Hint-Pasifik coğrafyasında Japonya'nın en önemli güvenlik ortağı olan Hindistan ile gerçekleşen siber diyaloglar ekseninde ise siber politikalar konusunda karşılıklı anlayış geliştirilmesine odaklanılmaktadır. Aynı zamanda, son 10 yıldır daha yakın güvenlik bağları kuran Japonya ve Avustralya, siber güvenlik politika diyalogları çerçevesinde bölgesel kapasite geliştirme çabaları, nesnelerin interneti, tedarik zinciri, güçlendirilmiş iş birliği gibi konulara odaklanmaktadır. Ek olarak, İsrail'in güçlü siber savunma ve saldırı yeteneklerine sahip olması akabinde Japonya ve İsrail başbakanlarının siber güvenlik alanında iş birliklerini derinleştirme konusunda anlaşmaya varmaları ve her yıl düzenli olarak gerçekleştirilen siber diyaloglar ekseninde "Siber Güvenlik Alanında İş Birliği Mutabakat Zaptı'nın" imzalanması önem teşkil etmektedir (Vosse, 2019, ss. 7-16). Son olarak tarafların çatışan çıkarlarına rağmen ortak bir noktada buluşmalarına atıf yapan iş birliği modeli çerçevesinde Japonya'nın Çin ve Kuzey Kore ile yaşadığı sorunlar ve bu devletlerden algıladığı tehdide rağmen altı çizildiği üzere siber güvenlik alanında iş birliği geliştirdiği görülmektedir.

7. Sonuç

Devletlerin siber uzay gibi geleneksel olmayan alanlarda ortaya çıkan tehditleri önlemeye çalıştıkları ve bu noktada siber güvenliği sağlama konusunun son derece önem arz ettiği bilinen bir gerçektir. İç ve dış politika hedeflerine ulaşmanın bir aracı, günümüzün modern silahı ve en önemli özelliği kaynağının belirsiz olması olan siber saldırılar, bireyler ve şirketlerden devletlere ve uluslararası kuruluşlara kadar çeşitli aktörleri hedef almaktadır. Asya Pasifik devletlerinden biri olan ve her yıl milyonlarca siber saldırı yaşayan Japonya, siber tehditleri ulusal güvenliğine yönelik bir tehdit olarak nitelendirmekte ve bu tehditlerle başa çıkma mekanizmaları oluşturmaya, siber güvenlik ve savunma stratejileri formüle etmeye çalışmaktadır. Öte yandan Japonya, siber güç kategorisi altında tanımlanmamaktadır. Ancak Japonya'nın siber güvenliğin sağlanması konusunda harcadığı yoğun çabalar ve her geçen gün bu alana yönelik etkin politikalar geliştirmeye devam etmesi noktasında önem teşkil ettiği görülmektedir. Öyle ki Japonya'nın siber güvenlik politikası ve siber güvenlik konusundaki uluslararası taahhütleri tarihsel bir perspektiften analiz edildiğinde söz konusu politika ve taahhütler hızlı bir şekilde gelişim göstermektedir. Bir diğer ifadeyle 2000'lerin başından günümüze Japonya hükûmeti, siber güvenliğe ilişkin stratejik vizyonunu istikrarlı bir şekilde geliştirmeye ve güçlendirmeye devam etmektedir. Bu noktada belirtilmesi gereken bir husus ise 2000'lerden günümüze peyderpey bir biçimde güçlendirilmeye çalışılan siber güvenlik politikalarına özellikle son 10 yılda görünür biçimde ilgi gösterilmesidir.

2000'li yılların başından günümüze ulusal güvenliği odak noktasına koyarak siber güvenlik alanında fiziki ve fiziki olmayan kurumlar çerçevesinde kurumsal kapasitesini güçlendiren Japonya'nın, bu alanda ortaya koyduğu politikalarını aynı kararlılıkla sürdürme eğiliminde olduğu görülmektedir. Bu noktada çalışmada tarihsel kurumsalcılık teorisi ekseninde analiz edilen Japonya'nın siber güvenlik politikalarının teorinin yol/izlek bağımlılığı mekanizmasıyla örtüştüğü sonucuna ulaşılmaktadır. Diğer taraftan Japonya, siber güvenlik politikalarına etki edecek kritik eşiklerden geçmiştir. 2011 yılında Mitsubishi Heavy Industries şirketine yapılan siber saldırılar, Çin'in askeri olarak her geçen yıl yükselişe geçmesi, Rusya'nın Ukrayna saldırısı ve bu durumun Çin tarafından Tayvan'a yapılma olasılığı, Kuzey Kore'nin yaptırım kararlarına rağmen nükleer faaliyetlerine hız kesmeden devam etmesi gibi kritik eşikler çerçevesinde genel olarak ulusal güvenlik özel de ise siber güvenlik politikasında değişime gideceğinin ilk sinyali 2013 yılında yayımlanan Siber Güvenlik Strateji Belgesi ekseninde verilmiş olup, pasifist politikadan militarizme kaymanın somut adımı ise 2022 yılında kabul edilen yeni Ulusal Güvenlik Stratejisiyle atılmıştır. Bu ise teorinin ortaya koyduğu kritik dönemeçlerde politika değişikliğine gidilebileceğini yansıtan kesintiye uğramış/noktalanmış denge mekanizmasını yansıtmaktadır. Öyle ki 2015, 2018 ve 2021 yılında güncellenen 2013'te Japonya hükûmeti tarafından yayımlanan strateji belgesi, siber güvenliğin ulusal güvenlik için ciddi etkileri olduğunu kabul eden ve siber uzayı hem Savunma Bakanlığı hem de Öz Savunma Kuvvetleri için yeni bir operasyonel alan olarak tanıyan ilk strateji olma özelliğini haizdir. Öte yandan, Yeni Ulusal Güvenlik Stratejisi, ciddi bir siber saldırı olasılığını önceden ortadan kaldırmak için aktif siber savunmanın uygulamaya konduğunu ve ulusal siber güvenlik çabalarının koordinatörü rolünü güçlendirmek için NISC'nin yeniden yapılandırıldığını duyurarak büyük bir doktrin değişikliğine neden olmaktadır. Bu noktada siber güvenlik alanında yeni bir birimin inşa edilmesine yönelik karar alınması ve mevcut kurumların (NISC, İçişleri ve Haberleşme Bakanlığı gibi) yetkilerinin artırılması ise teorinin olumlu geri bildirim döngüsünü ortaya koymaktadır.

Öte yandan, siber güvenlik politikaların güçlendirilmesine yönelik takip edilen mevcut yaklaşım, doğru yönde ilerlemekle birlikte çeşitli boyutlarda daha fazla derinlik gerektirdiğini göstermektedir. Nitekim kritik uzay altyapılarına karşı hem siber hem de uzay güvenliği risklerinin değerlendirilmesi, bu konularda sivil ve askeri yetenek ve bilgilerin daha derin entegrasyonunun sağlanması ve ilgili sektörden gelen uzmanlığa daha fazla güvenilmesi gibi konular üzerinde durulması gerekliliği rahatlıkla ifade edilebilir. Bununla beraber, Japonya'nın potansiyel siber güvenlik açıklarını gözden geçirmesi kritik öneme sahiptir. Ek olarak, kritik altyapıların siber dayanıklılığını desteklemek ve daha güçlü hâle getirmek için Japonya'nın yasalarını, politikalarını ve uygulamalarını geliştirmeye yönelik çabaları devam etmektedir. Ancak, uzay varlıklarının siber güvenliği konusunda özel değerlendirmeler yapılmasını gerektiren yeni şartlar ortaya çıksa da uzay varlıklarına henüz odaklanılmamaktadır.

Bununla beraber, siber güvenlik alanında sürdürülebilir gelişmenin sağlanması ve devamlılığı için tüm aktörlerin, siber güvenlik konusunda üstlerine düşen görevleri özgür şekilde yerine getirmeleri önem teşkil etmektedir. Bir diğer ifadeyle tüm paydaşların siber güvenlik konusundaki rollerinin farkında olması ve gerekli önlemleri uygulaması gerekmektedir. Bu bağlamda Japonya hükûmeti de siber güvenlik alanındaki girişimleri destekleme yönünde hareket etmektedir. Ayrıca, özgür, adil ve güvenli bir siber alan sağlamanın yalnızca ulusal çabalarla sağlanamayacağı kabulünden yola çıkılarak, uluslararası ve bölgesel iş birliğinin, Japonya'nın siber güvenlik politikasının önemli bir parçası olduğu görülmektedir. İş birliği modeli ekseninde fayda unsuruna atıfta bulunulmaktadır. Nitekim fayda unsuru söz konusu olmadığında iş birliğine gidilmediğinin altı çizilmektedir. Bu bağlamda genel olarak, siber saldırılar tüm devletleri etkilediğinden söz konusu saldırıları bertaraf etmek, ilgili taraflar açısından fayda unsuruna yol açmaktadır. Faydanın maksimizasyonu noktasında taraflar iş birliğini ve koordinasyonu geliştirmeye ve güçlendirmeye çalışmaktadır ki Japonya'nın başta ABD olmak üzere, Avustralya, Hindistan, İsrail, İngiltere, Fransa, Almanya, Estonya ile siber güvenlik alanında iş birliği geliştirdiği görülmektedir. Mevzubahis devletlere ek olarak, BM gibi küresel NATO ve ASEAN gibi bölgesel örgütlerle de söz konusu alanda iş birliği yapılmaktadır. Ancak modelin sunduğu fayda unsuruna özel olarak yaklaşıldığı takdirde modern dünyanın en etkili silahı olarak kullanılan siber saldırılara, aktörlerin hedeflerine ve çıkarlarına ulaşılması ekseninde başvurulması doğrultusunda siber güvenlik için iş birliği ve karşılıklı fayda üzerine kurulu somut anlamda evrensel bir mekanizmanın söz konusu olmadığı ve yakın gelecekte de oluşturulması olasılığının düşük olduğu rahatlıkla ifade edilebilir. Etkili siber karşı güvenliğin geliştirilmesi ve uygulanmasında iş birliği modeli son derece önemlidir. Paydaşlar arasında iş birliğini kurumsallaştırmak ise zaman, özveri ve kaynak gerektirmektedir. Farklı kültürleri, normları ve adetleri temsil eden aktörlerin, iş birliğini kolaylaştıran protokolleri, anlaşmaları biranda uygulamaya koymaları kolay değildir. Bu durumun hayata geçirilmesi hususu, ortak bir çabaya işaret etmektedir.

Son kertede, Japonya'nın siber güvenlik politikası tarihsel kurumsalcılık teorisi ve iş birliği modelinin ortaya koyduğu çıktılarla büyük oranda uyuşmaktadır. Ayrıca, Japonya hükûmeti siber alan risklerinin her geçen gün ele alınması gerekliliğine yönelik geliştirdiği güçlü farkındalığı sayesinde, siber güvenlik açıklarının belirlenmesi ve siber güvenlik yeteneklerinin geliştirilmesi konusunda şüphesiz büyük bir ilerleme kaydetmektedir. Öte yandan tüm bu çabalara rağmen altı çizilmesi gereken bir diğer husus ise yayımlanan strateji belgelerinde belirtilen hedeflere tam olarak ulaşılamamasıdır. Ancak bu hususun altında hız kesmeden ilerleyen teknolojisi karşısında güncelliği korumanın zorluğu, siber güvenlik ile ilgili yatırımların maliyetli olması ve yeterli bütçe ayrılmaması ve siber alanda nitelikli uzman yetiştirmek için çok fazla çaba gösterilmemesi gibi başlıklar bulunmaktadır. Yine de siber güvenlik alanında daha militarist bir yapıya evrilmekle beraber, kurumsallaşma ve iş birliği odaklı bir Japonya gerçeği, bu alanda çok daha fazla ilerleme kaydedileceği sinyallerini vermektedir.

8. Extended Abstract

Cyberspace makes up one of the most popular concepts in the modern world. The high-intensity change and transformation of information and communication technologies both have many advantages and cause security vulnerabilities arising from cyber threats. It is a known reality that the advantages and disadvantages of cyberspace are experienced within the framework of the changing and transforming world composition and the ever-growing technological globalization.

Being one of today's primary risk factors, cyber threats affect states, international organizations, and individuals, and thus, they make it a necessity for the said actors to take precautions against them. It leads to the formulation of policies and/or strategies to eliminate cyber attacks, the most important specific feature of which is the uncertainty of their source, and to ensure security in the digital environment. At this point, the information and technology society in Japan, one of the Asia-Pacific states, which is in constant cyber conflict with China and North Korea and is exposed to millions of cyber attacks every year, is trying to put its cyber security on more solid ground. Although Japan is not defined under the category of cyber power, its intensive efforts to ensure cyber security and its continuing to develop effective policies in this area are important. From this point of view, in this study, it is analyzed what policies Japan follows in the face of threats originating from cyberspace. When the Turkish literature is examined, it is seen that there is no study on this subject. In this study, which was written in order to close

the gap in question and created with the descriptive analysis method, first of all, the institutionalization process of Japan in the field of cyber security from the beginning of the 2000s to the present is examined. Subsequently, by considering the New National Security Strategy Document published in 2022, cyber security is approached within the framework of the said document. On the other hand, the subject in question is carried to the dimension of the actors playing a role in the context of cyber security and the expenditures made. In addition, collaborations with Japan in the cyber field are discussed. Finally, by transferring all this data to the theoretical level (historical institutionalism and cooperation model), an answer is sought to the question of how much Japan's cyber security policies overlap with the outputs of historical institutionalism and cooperation model.

On the basis of the data obtained during the study, it is concluded that Japan, which has strengthened its institutional capacity within the framework of physical and non-physical institutions in the field of cyber security by putting national security in the spotlight from the beginning of the 2000s to the present, tends to maintain its policies in this area with the same determination. In addition, mechanisms for establishing new institutions in the field of cyber security and strengthening the powers of existing institutions are presented. On the other hand, it is seen that a policy change has been made in this area with the new national security strategy adopted in 2022 for the first time and, more concretely, with the cyber security strategy document published in 2013. As a matter of fact, Japan, which has shifted from a pacifist structure to a militarist structure, also follows policies to strengthen cooperation and coordination in the field of cyber security. It is seen that Japan has developed cooperation in the field of cyber security with Australia, India, Israel, England, France, Germany, and Estonia, especially the USA. In addition to the aforementioned states, cooperation is also made with global organizations such as the UN and regional organizations such as NATO and ASEAN. In this context, Japan's cyber security policy largely coincides with the outputs of historical institutionalism theory and the cooperation model. However, the cooperation model used in the development and implementation of cybersecurity is not always effective. As a matter of fact, institutionalizing cooperation among stakeholders requires time, dedication, and resources. It is not easy for actors representing different cultures, norms, and customs to put into practice protocols and agreements that facilitate cooperation. Achieving this situation requires a joint effort.

On the other hand, despite Japan's efforts to provide cyber security, it is clear that the objectives specified in the published strategy documents have not been fully achieved. However, under this issue, there are topics such as the difficulty of keeping up-to-date in the face of rapidly advancing technology, the cost of investments in cyber security, the lack of a sufficient budget, and the lack of effort to train qualified experts in the cyber field. Nevertheless, although it is evolving into a more militaristic structure in the field of cyber security, the fact that Japan is focused on institutionalization and cooperation signals that much more progress will be made in this field.

Keywords: Cyber Security, Japan, Historical Insitutionalism, Cooperation Model.

Çıkar Çatışması Beyanı / Conflict of Interest

Çalışmada herhangi bir kurum veya kişi ile çıkar çatışması bulunmamaktadır.
There is no conflict of interest with any institution or person in the study.

İntihal Politikası Beyanı / Plagiarism Policy

Bu makale İntihal programlarında taranmış ve İntihal tespit edilmemiştir.
This article was scanned in Plagiarism programs and Plagiarism was not detected.

Bilimsel Araştırma ve Yayın Etiği Beyanı / Scientific Research and Publication Ethics Statement

Bu çalışmada Yükseköğretim Kurumları Bilimsel Araştırma ve Yayın Etiği Yönergesi kapsamında belirtilen kurallara uyulmuştur.
In this study, the rules specified within the scope of the Higher Education Institutions Scientific Research and Publication Ethics Directive were followed.

Kaynakça

Austin, G. (2018). International Legal Norms in Cyberspace: Evolution of China's National Security Motivations. In A. Osula, & H. Roigas (Ed.), *International Cyber Norms Legal, Policy & Industry Perspectives*, https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_full_book.pdf.

Barlett, B. (2019). *How Japanese Cyber Security Policy Changes*. https://programs.wcfia.harvard.edu/files/us-japan/files/19-01_bartlett.pdf.

Basic Act on Information and Telecommunications Network Society. (2000). https://japan.kantei.go.jp/it/it_basiclaw/summary.html.

Collier, R. B., & Collier, D. (1991). *Framework: Critical Junctures and Historical Legacies*. https://polisci.berkeley.edu/sites/default/files/people/u3827/Collier-Collier%20SPA%20Chap%201.pdf.

Cybersecurity Insiders. (2020). *Cyber Attack on Mitsubishi Electric and China Held as a Suspect*. https://www.cybersecurity-insiders.com/cyber-attack-on-mitsubishi-electric-and-china-held-as-a-suspect/.

Cybersecurity Strategic Headquarters. (2017). *The Cybersecurity Policy for Critical Infrastructure Protection*. http://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4_r1.pdf.

Cyber Security Strategy. (2015). https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf.

Cyber Security Strategy. (2018). https://www.nisc.go.jp/eng/pdf/cssenryaku2018-en.pdf.

Cyber Security Strategy. (2021). www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-en.pdf.

Defence of Japan. (2023). https://www.mod.go.jp/en/publ/w_paper/wp2023/DOJ2023_Digest_EN.pdf.

Demir, Y. (2020). Japonya'nın Siber Güvenlik Politikası. İçinde F. Köksoy (Ed.), *Yeni Küresel Tehdit Siber Saldırılar* (ss. 227-224). Ankara: Nobel Yayınevi.

Euronews. (2022). *Japonya 2023'te Askeri Harcamaları Artırmak İçin Rekor Bütçe Açıkladı*. https://tr.euronews.com/2022/12/23/japonya-2023te-askeri-harcamalari-artirmak-icin-rekor-butce-acikladi.

Gady, F. S. (2017). *Japan: The Reluctant Cyberpower*. https://www.ifri.org/sites/default/files/atoms/files/gady_japan_reluctant_cyberpower_2017.pdf.

Global Edge. (t.y.). *Japan: Ministry of Internal Affairs and Communications*. https://globaledge.msu.edu/global-resources/resource/10557.

Global Regulation. (2016). *The Basic Act on Cybersecurity*. https://www.global-regulation.com/law/japan/3009836/the-basic-act-on-cybersecurity.html.

Guiora, A. N. (t.y.). *Cybersecurity: A Cooperation Model*. https://www.bbvaopenmind.com/en/articles/cybersecurity-a-cooperation-model/.

Hall, P., & Taylor, C. (1996). Political Science and The Three New Institutionalisms. *Political Studies,* 44 (2), 936-957.

Information Security Policy Council. (2006). *The First National Strategy on Information Security*. https://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf.

Information Security Policy Council. *(2009). The Second National Strategy on Information Security. https://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf.*

Information Security Policy Council. (2013). *International Strategy on Cybersecurity Cooperation – J-Initiative for Cybersecurity*. http://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf.

International Trade Administration. (2023). *Japan Cybersecurity*. https://www.trade.gov/market-intelligence/japan-cybersecurity.

Iwamoto, A., & Verspieren, Q. (2023). *Cybersecurity of Space Infrastructure and Space Sustainability: Japan's View*. https://www.cigionline.org/articles/cybersecurity-of-space-infrastructure-and-space-sustainability-japans-view/.

Japan Ministry of Defense. (2020). https://www.mod.go.jp/e/publ/w_paper/pdf/2020/DOJ2020_Digest_EN.pdf.

Japan Times. (2023). *Cyberattacks Increasing in Japan Ahead of G7 Summit*. https://www.japantimes.co.jp/news/2023/04/30/national/crime-legal/cyberattacks-japan-g7/.

JPCERT/CC. (t.y.). *Coordination Center for Cyber Incidents Towards a Safer Cyber Space Without Incident*. https://www.jpcert.or.jp/english/about/01.html.

Kallendera, P., & Hughes, C. W. (2017). Japan's Emerging Trajectory as a Cyber Power: From Securitization to Militarization of Cyberspace. *The Journal of Strategic Studies*, 40(1), 118-145.

Kaneko, Y. (2001). *Promoting Electronic Government: With a Focus on Statistical Activities*. https://www.stat.go.jp/english/info/meetings/iaos/pdf/kaneko.pdf.

Kingston, J. (2016). *Japan's Cybersecurity Upgrade: Too Little, Too Late?*. https://www.japantimes.co.jp/opinion/2016/05/21/commentary/japans-cybersecurity-upgrade-little-late/.

Köksoy, F., & Ceyhan, N. (2023). Japonya'nın Yeni Güvenlik Stratejisi: Geleneksel Güvenlik Yaklaşımına Geri Dönüş Mü?. *Manas Sosyal Araştırmalar Dergisi*, 12(2), 775-785.

Krasner, D. S. (1984). Approaches to the State: Alternative Conceptions and Historical Dynamics. *Comparative Politics*, 16(2), 223–246.

Lockwood, M. vd. (2016). *Historical Institutionalism and the Politics of Sustainable Energy Transitions: A Research Agenda.* https://core.ac.uk/download/pdf/43098859.pdf.

March , J. G., & Olsen, J. P. (1984). The New Institutionalism: Organizational Factors in Political Life. *The American Political Science Review,* 78(3) 734–749.

Matsubara, M., & Mochinaga, D. (2021). *Japan's Cyber Security Strategy from the Olmpics to the Indo-Pacific*. https://www.ifri.org/sites/default/files/atoms/files/matsubara_mochinaga_japan_cybersecurity_strategy_2021.pdf.

Ministry of Defence. (2018). http://www.mod.go.jp/e/publ/w_paper/2018.html.

Ministry of Foreign Affairs of Japan. (t.y.). *National Security Council*. https://www.mofa.go.jp/fp/nsp/page1we_000080.html.

Ministry of Foreign Affairs of Japan. (2021). *Diplomatic Bluebook 2021*. www.mofa.go.jp/policy/other/bluebook/2021/pdf/pdfs/4-2.pdf.

MOFA. (t.y). *Japan's Cyber Diplomacy*. https://www.mofa.go.jp/files/000412327.pdf.

National Information Security Policy Council. (t.y.). https://www.nisc.go.jp/eng/index.html.

Nikkei Asia. (2021). *Cyberattacks on Japan Aerospace Industry Exploited Zero-Day Flaw*. https://asia.nikkei.com/Business/Technology/Cyberattacks-on-Japan-aerospace-industry-exploited-zero-day-flaw.

Nitta, Y. (t.y.). *Japan's Approach Towards International Strategy on Cyber Security Cooperation*. https://cybersummit.info/sites/cybersummit.info/files/Japan_edited%20v2.pdf-FINAL.pdf.

OECD. (2019). *Japan's Information Security Initiatives*. http://www.oecd.org/japan/japansinformationsecurityinitiatives.htm.

Ogawa, H., & Tsuchiya, M. (2021). Cyber Security Governance in Japan. *Internatinal Journal of Cyber Diplomacy,* 7-30.

Osowa, J. (2023). *How Japan is Modernizing Its Cybersecurity Policy*. https://www.stimson.org/2023/japan-cybersecurity-policy/.

Pierson, P. (2000). Increasing Returns, Path Dependence and The Study of Politics. *American Political Science Association,* 94(2), 251-267.

Pierson, P. (2004). *Politics in Time: History, Institutions, and Social Analysis*. Princeton University Press.

Pierson, P., & Skocpol, T. (2002). Historical Institutionalism in Contemporary Political Science. In I. Katznelson, H. Milner, & A. Finifter (Ed.), *Political Science: The State of the Discipline (pp. 693-721)*. NewYork: Norton Press.

Phys. (2011). *New Cyber Attack on Japan Parliament*. https://phys.org/news/2011-11-cyber-japan-parliament.html.

Pollack, M. (1996). The New Institutionalism and EU Governance: The Promise and Limits of Institutionalist Analysis. *Governance*, 9(4), 429-458.

Pollack, M. (2009). The New Institutionalism and European Integration. In A. Wiener, & T. Diez (Ed.), *European Integration Theory* (pp. 125-143). Newyork: Oxford University Press.

Reuters. (2023). *US and Japan Agree to Step up Cyber Security Cooperation*. https://www.reuters.com/technology/us-japan-agree-step-up-cybersecurity-cooperation-2023-01-07/.

Savunma Sanayi. (2021). *Japonya'nın Savunma Bütçesi Bir Kez Daha Rekor Kırdı*. https://www.savunmasanayist.com/japonyanin-savunma-butcesi-bir-kez-daha-rekor-kirdi/.

Schuetze, J. (2020). *Japan's Cybersecurity Policy: An Introduction.* https://www.stiftung-nv.de/sites/default/files/rif-japan-schuetze-final.pdf.

Skocpol, T., & Finegold, K. (1982). State Capacity and Economic Intervention in The Early New Deal. *Political Science Quarterly* , 97(2), 255–278.

Thelen, K. (1999). Historical Institutionalism in Comparative Politics. *Annual Review of Political Science*, 2, 369–404.

Ukhanova, E. (2022). *Cybersecurity and Cyber Defence Strategies of Japan*. https://www.shs-conferences.org/articles/shsconf/pdf/2022/04/shsconf_eac-law2021_00159.pdf.

Vosse, W. M. (2019). *Japan's Cyber Diplomacy*. https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/eapFPDHU/vosse_rif_topublish.pdf.

Wildavsky, A. (1987). Choosing Preferences by Constructing Institutions: A Cultural Theory of Preference Formation. *The American Political Science Review*, 81(1), 4–21.