ULUSAL SİBER GÜVENLİK STRATEJİSİ: FRANSA

Dr. Ahmet Emre KÖKER[1]

Öz: Siber uzaya yönelik risk ve tehditler çoğaldıkça, siber güvenlik ve savunma konuları Fransa için önemli bir politika alanı haline gelmiştir. Uluslararası ilişkilerde beşinci boyut alanı olarak kabul edilen siber ortamda, Fransa, rakiplerinin gerisinde kalmıştır. Aynı zamanda, Fransa, söz konusu rakiplerini yakalamak, tehditleri bertaraf etmek, gerekli reformları gerçekleştirmek, siber ortamda küresel liderliği sağlamak gibi amaçlar doğrultusunda ulusal güvenlik stratejilerini belirleyerek doktrin geliştirme çabasına girmiştir. Bu makale, Fransa'nın ulusal siber güvenlik ve savunma politikalarının kavramsal temeline, geliştirilen strateji ve doktrinlere, uluslararası ilişkilerde gerçekleştirilen ikili ilişkilere, kurumsal yapının en önemli unsurlarına, kritik noktalara yönelik gerçekleştirilen siber saldırılara, son olarak siber çabalara ve girişimlere genel bir bakış sunmaktadır. Makale, Fransa'nın siber güvenlik stratejini incelemeye yönelik gerçekleştirilecek araştırmalar için bir başlangıç sağlamayı amaçlamaktadır. Bu amaç doğrultusunda, makale, Ulusal Bilgi Sistemleri Güvenlik Ajansı (L'Agence nationale de la sécurité des systèmes d'information-ANSSI) ile Savunma ve İçişleri Bakanlıklarının (MOD ve MOI) çabalarına odaklanmaktadır. Söz konusu çalışma gerçekleştirilirken, Fransa'nın siber güvenlik ve savunma politikalarını belirleyen kurumlar ve kişiler özelindeki tüm aktörlerin birincil (resmi belgeler ve üst düzey devlet yetkilileri tarafından yapılan açıklamalar ile yasal mevzuat) ve ikincil kaynaklarına (kitaplar, tezler, akademik makaleler, haberler ve bu konuda yazılmış analizler) odaklanılarak analiz gerçekleştirilmiştir.

Anahtar Kelimeler: *Siber Güvenlik, Siber Savunma, Fransız Siber Savunma ve Güvenlik Politikaları, Ulusal Güvenlik ve Savunma Organizasyonu, ANSSI.*

Article Category: Political Science

Date of Submission: 15.10.2021

Date of Acceptance: 09.01.2022

[1] Dr. Siyaset Bilimi ve Uluslararası İlişkiler, PTT A.Ş. Genel Müdürlüğü, Ankara.
Email: a.emrekoker@hotmail.com / ahmetemrekoker@gmail.com.
ORCID: 0000-0002-8032-4237.

NATIONAL CYBER SECURITY STRATEGY: FRANCE

Abstract: Cybersecurity and defense issues have become an important policy area for France, with the rise of risks and threats to cyberspace. In the cyber environment, which is accepted as the fifth dimensional area in international relations, France has lagged behind its competitors. At the same time, France is in a struggle for development the doctrine by determining its national security strategies in line with the objectives such as catching its rivals, eliminating threats, carrying out necessary reforms, and providing global leadership in the cyber environment. This article provides a general overview of the conceptual basis of France's national cyber security and defense policies, developed strategies and doctrines, bilateral relations in international relations, the most important elements of the institutional structure, cyber-attacks against critical points, and finally, cyber efforts and initiatives. The article aims to provide a prelude to research to examine the cyber security strategy of France. For this purpose, the article focuses on the efforts of the National Information Systems Security Agency (L'Agence nationale de la sécurité des systèmes d'information-ANSSI) and the Ministry of Defense and the Ministry of the Interior (MOD and MOI). During the said study, the analysis was carried out by focusing on the primary (official documents and statements made by high-level state officials and legal legislation) and secondary (books, theses, academic articles, news and analyzes on the subject) sources of all actors, specific to the institutions and individuals that determine the cyber security and defense policies of France.

Keywords: *Cyber Security, Cyber Defence, French Cyber Defence and Security Policies, Organisation Of National Security and Defence, ANSSI.*

Giriş

İnternetin yaygın kullanımı, birbiriyle bağlantılı bilgi teknolojilerinin ve telekomünikasyonun hâkim olduğu bir siber çağı yaratmıştır. Özellikle dijitalleşmenin artmasıyla birlikte, siber çağın önemi, boyutu ve kapsamı da genişlemiştir. Siber uzaya yönelik son çeyrek yüzyıldaki bu genişleme, Fransa gibi modern ve teknolojik olarak gelişmiş ülkelerin yaşamında siber uzayın rolünü arttırmıştır. Gelinen bu süreci Fransa özelinde incelediğimizde, kurumların dönüştürüldüğü ve hukuksal düzenlemelerin güncellendiği görülmektedir.

Fransa'nın siber uzaya yönelik gerçekleştirdiği değişim ve dönüşümlerin en büyük sebepleri arasında bilginin serbest ve kesintisiz akışı ile bilgiyi elde etmeye veya kritik altyapı ve tesisleri bozmaya ya da engellemeye yönelik gerçekleştirilen siber saldırılardaki artışlar etkili olmuştur. Ayrıca siber saldırılardaki artış, ekonomik, siyasi, askeri, hukuki vb. tüm alanlarda siber uzayın etkili olmasına yol açmıştır. Bu doğrultuda, Fransa'da son 25 yıllık süreçte siber güvenlik ve savunma konusuna ciddi önem verilmiştir.

Fransa, vermiş olduğu bu önem çerçevesinde ulusal siber güvenlik stratejileri belirlemiş, siber uzaya yönelik doktrinler oluşturmuş ve ittifak ilişkileri geliştirmiştir. Böylece, uluslararası ilişkilerde yaşanan siber rekabete aktif olarak katılmıştır. Fransa'nın siber uzayda mücadeleye girmesiyle eş zamanlı olarak bazı temel adımlar atılmıştır. Bunlar arasında esnek bir yapının oluşturulması, yönetim ve komuta kademesinin belirlenmesi, siber yetenek ve kabiliyetlerin geliştirilmesi gibi adımlar bulunmaktadır. Fransa'da atılan bu adımlar sonucunda, siber uzay, milli güç unsurları arasına dâhil etmiştir. Bununla birlikte, Fransa'da siber uzaya yönelik artan risk ve tehditler ile siber uzayın sağladığı avantaj ve fırsatlar bir arada gelişmiştir.

Çalışmanın birinci bölümde, Fransa'nın ulusal siber güvenlik stratejisinin temelleri, bir doktrin haline gelmesi ve ikili ilişkiler ile ittifakları belirleyen dinamikler üzerinde durulmuştur. İkinci bölümde, Fransa'nın siber sürecini açıklamaya yönelik yasal ve düzenleyici hükümleri, yönetim, komuta ve kontrol sistemlerinin işleyişi, siber alanın diğer etki alanlarına etki etmesi ve siber kriz örnekleri incelenmiştir. Üçüncü bölümde ise, Fransa'da siber güvenliğin ve siber savunmanın sağlanması noktasında kurumsal süreçte önemli görevler üstlenen ANSSI, MOD ve MOI örnekleri üzerinden Fransa'nın içinde bulunduğu fırsatlar ve zorluklar ortaya konulmuştur.

1. Fransa'nın Ulusal Siber Güvenlik Stratejisi: Alanlar, Görevler, Öncelikler

Ulusal Dijital Güvenlik Stratejisi (SNSN), Fransa'nın mevcut siber güvenlik stratejisidir. SNSN, çok geniş bir yelpazeyi kapsamaktadır. Bu genişlik, siber güvenlik tanımı yerine "*dijital*" kelimesinin kullanılmasından kaynaklanmaktadır. Bu doğrultuda, belgenin başlığında bile "*siber*" kelimesi yerine "*dijital*" kelimesi kullanılmıştır.

Kavramsal olarak bu düşünsel genişliğin sonucunda Fransa'nın siber güvenlik sürecini incelediğimizde; gizlilik, internet kullanıcılarının hakları ve çevrimiçi propaganda gibi kavramlar ön plana çıkmaktadır. Bu bağlamda, SNSN, Fransız siber güvenliği için beş temel hedef belirlemiştir. Bu hedefler şunlardır:[2]

1. Ulusal ve uluslararası iş birliği yoluyla siber güvenliği ve dayanıklılığı geliştirmek,

2. Fransız kullanıcıların gizlilik haklarının iyileştirilmesi ve siber saldırıların ve "*siber kötü niyetliliğin*" kurbanlarına yardım etmek,

3. Siber sorunlar hakkında eğitim ve farkındalığı iyileştirmek,

4. Siber güvenlikte inovasyonu desteklemek,

5. Avrupa Birliği'nin siber özerkliği ve siber uzay istikrarı için AB kurumlarına lobi yapmaktır.

Fransa'nın ulusal siber güvenlik ve savunma politikaları, bu beş temel hedef çerçevesinde inşa edilmiştir.

1.1. Fransa'nın Ulusal Siber Güvenlik ve Savunma Politikalarının Temel Dinamikleri

Fransa'nın siber güvenliği ve siber savunmayı sağlamaya yönelik belirlemiş olduğu ulusal stratejisinin temeli 2008 yılına gitmektedir. 2008 yılında ilan edilen "*Ulusal Savunma Beyaz Kitabı*", siber savunma açısından bir dönüm noktasıdır. Bu kitap, Fransa'nın küresel bir siber devlet olma arzusunu ortaya çıkarmıştır. Bu bağlamda; *Beyaz Kitap* (*Défense et Sécuriténationale: Le Livre Blanc*) ile birlikte bilginin korunması sistemleri, Fransız ulusal

[2] Robert S. Dewar (2018), "CSS Cyber Defense Project, National Cybersecurity And Cyberdefense Policy Snapshots", Erişim Tarihi: 23.01.2022, Erişim Adresi: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports_National_Cybersecurity_and_Cyberdefense_Policy_Snapshots_Collection_1.pdf, ss. 7-24.

sisteminin savunma ve güvenlik politikalarının ayrılmaz bir parçası olarak tanımlanmıştır. Böylece, Fransa'nın askeri ve savunma teşkilatı yeniden yapılandırılmıştır. Ayrıca mevut doktrinler reforme edilerek, savunmanın dijital dönüşümü baştan tasarlanmıştır.

Fransa tarafından ilan edilen *Beyaz Kitap,* "*pasif savunma stratejisinden aktif savunmaya geçişi*" simgelemektedir. Fransa'nın bu dönüşümünü simgeleyen derin strateji, sistemlerin içsel korumasının zorunluluğunu, sürekli gözetimin kaçınılmazlığını, hızlı tepki alma ihtiyacının gerekliliğini, güçlü saldırı eylemi ve kuvvetli hükümet dürtüsünün zorunluluğunu göstermektedir.[3]

Aslına bakılırsa, "*Beyaz Kitap*", bilgisayar saldırıları ile siber uzayda ortaya çıkan tehdide önemli bir yer vermiştir. Böylece, Fransa tarafından günlük yaşamın istikrarsızlaştırılması, kritik öneme sahip ağların felç olması, belirli askeri yeteneklerin işleyişinin reddedilmesi gibi risklere karşı baştan önlem alınmıştır. Baştan bu önlemin alınmasının sebebi, pasif bir savunmanın gelişmiş bilgi teknolojilerine dayalı siber saldırılara karşı tam anlamıyla etkili olmamasıdır. Bu sonuç, 2009 yılında Ulusal Bilgi Sistemleri Güvenlik Ajansı'nı (*Agence nationale de la sécurité des systèmes d'information*/ANSSI) yaratmıştır.

ANSSI, 7 Temmuz 2009 tarihli kararname ile oluşturulmuştur.[4] Devletin sistem güvenliğini sağlama noktasında tavsiye verme görevinden sorumludur. Fransa'nın güvenliği için ulusal bir görev üstlenen kurum, Savunma ve Ulusal Güvenlik Genel Sekreteri'ne (SGDSN) bağlıdır. Sorumluluklarının yerine getirilmesinde Başbakan'a yardımcı olma görevine sahiptir. ANSSI'nin 2014 yılında bütçesi 83,4 milyon avro, personeli ise 350 kişi iken, 2015 sonunda 500 acente ve 2017 sonunda 567 acente olmuştur. İlerleyen süreçte, ANSSI, hizmet ağını ve bütçesini arttırarak büyümüş ve güç kazanmıştır.

ANSSI'ye ek olarak, 2010 yılında, Fransa Cumhurbaşkanlığı "*Siber Güvenlik Grubu Stratejik Eğitim ve Araştırma İçin*" (CSFRS) adı altında bir ulusal güvenlik stratejik konseyi oluşturdu. Oluşturulan bu konsey, sivil, askeri, endüstriyel ve hükümete ait geniş bir uzmanlık yelpazesi yarattı. Böylece, Fransa'nın strateji oluşturma işlevi daha kurumsal hale geldi.

[3] Philippe Baumard (2017), *Cybersecurity in France*, Springer, ss. 56-65.
[4] ANNSI (2021), "The National Cybersecurity Agency Of France", 2021, Erişim Tarihi: 07.11.2021, Erişim Adresi: https://www.ssi.gouv.fr/en/cybersecurity-in-france/the-national-cybersecurity-agency-of-france/.

Fransa, bu iki kurum tarafından gerçekleştirdiği kurumsal çalışmalar sonrasında siber güvenliği diğer gelişmiş ülkelerle bir "*güç eşitleyici*" mekanizma olarak benimsedi. Bu amaç doğrultusunda, Fransız hükümetinde siber güvenlik için merkezi koordinasyon otoritesi oluşturulması amacıyla ANSSI'nin yetki ve görevleri arttırıldı.[5]

2011 yılında Fransız hükümeti tarafından ilan edilen "*Ulusal Dijital Strateji*" çerçevesinde ulusal bir gözlemevi oluşturulmuştur. Ayrıca operasyonel düzeyde oluşturulan CERT ağı ve bir kamu-özel koordinasyon organı ile birlikte süreç hızlandırılmıştır. Sonrasında da, Fransız siber uzayının ulusal gelişiminin merkezinde olması amacıyla Fransız hükümeti Dijital Ulusal Konsey'i (*Conseil National du numerique*) kurdu.[6] Dijital Ulusal Konsey, 30 üyeli bağımsız bir danışma organıdır. Dijital alanda devletin rolünü güçlendirmeyi, yerel bir ağ tarafsızlığını korumayı, özgürlüğü savunmayı ve Fransa'nın kullandığı internet üzerindeki verilerin gizliliğini sağlamayı hedeflemektedir. Bu hedefler, 2012-2020 yıllarını içeren Bockel Raporu'nda da belirtilmiştir.

2012 yılında yayınlanan siber savunma ile ilgili Bockel Raporu'nda, Fransa Cumhurbaşkanlığı bilgi sistemleri ve Maliye Bakanlığı genel merkezine yönelik birçok siber saldırı gerçekleştiği belirtildi. Aynı zamanda, raporda, rakip devletler tarafından da bu saldırıların gerçekleştirilebileceği açıklandı.[7]

Bockel Raporu'nun yayınlanmasından sonra 2013 yılında ilan edilen *Beyaz Kitap,* Fransa'nın siber dünyadaki değişiminin en önemli göstergesidir. Ayrıca, *Beyaz Kitap,* ulusal bir doktrinin oluşturulmasını zorunlu kılmıştır.[8] Daha da önemlisi, *Beyaz Kitap*, Fransa'nın siber uzayda resmi olarak tanınması gerektiğini belirtmiştir. 2014 yılında yayınlanan Siber Savunma Paktı (PCD), Fransız stratejisi veya "*Plan d'action cyberdéfense*"dır. Pakt, Fransa'nın niyetini ortaya koymuştur. 2013 tarihli *Beyaz Kitap*'ta belirtilen istihbarat yeteneklerini ilan etmiştir.

2015 yılında ilan edilen Ulusal Dijital Güvenlik Stratejisi (SNSN), Fransız siber güvenlik politikasını detaylandırmıştır. Aynı zamanda "*siber güvenlik*" yerine "*dijital güvenlik*"ten

[5] Governing National Law, Decree 2009-834 of 7 July 2009, establishment of a service with national competence called "National Agency for the Security of Information Systems", Erişim Tarihi: 01.11.2021, Erişim Adresi: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000020828212/.
[6] Digital National Council, Erişim Tarihi: 02.11.2021, Erişim Adresi: https://cnnumerique.fr/.
[7] Jean-Marie Bockel (2012), "Report on behalf of the Foreign Affairs", Defense and Armed Forces Committee, Erişim Tarihi: 02.11.2021, Erişim Adresi: https://www.senat.fr/rap/r11-681/r11-681.html.
[8] White Paper: Defense and National Security Report (2013), Ministry of the Armed Forces, Erişim Tarihi: 29.10.2021, Erişim Adresi: http://www.livreblancdefenseetsecurite.gouv.fr/index.html.

bahsetmiştir. Fransa'yı siber savunmada lider bir ülke haline getirmeyi hedeflemiştir. Odak noktası eğitim ve farkındalıktır. Faaliyetlerini sivil odaklı yürütmektedir.

2016 yılında dönemin Fransa Başbakanı Manuel Valls'ın önderliğinde Fransız Ulusal Dijital Güvenlik Stratejisi yenilenmiştir. Söz konusu yenilemede, belirleyici bazı değişiklikler gerçekleştirilmiştir. Bu temel değişiklikler arasında terminoloji değişimi bulunmaktadır. Örneğin; "*egemen çıkarları*" kavramı "*temel çıkarlar*" ile değiştirildi. Böylece, daha belirsiz ve esnek ama aynı zamanda önemli olan kritik altyapılar ve stratejik endüstriler (nükleer, enerji, su, gaz, ulaşım vb.) de kavrama dâhil edildi. Aynı zamanda, yeni doktrin, bölgeselliği teşvik etmek yerine siber uzaydaki temel çıkarların savunmasını teşvik etmiştir.

Fransız ulusal siber güvenliğinin tasarımındaki ve amacındaki bu kritik değişim siber saldırıların kapsamını da aynı oranda etkiledi. Bu etki, 2015 ve 2016 yıllarındaki Fransız yasalarında gerçekleştirilen yeni eklemeleri getirdi. Bu yasal değişiklikler arasında, IP bağlantıları, e-postalar, telefon dahil her Fransız dijital iletişimi, IP üzerinden ses ve anlık mesajlaşma gibi gerçek zamanlı bir dizi müdahale bulunmaktadır.[9] Aslına bakılırsa, gerçekleştirilen bu yeni kanunun temel amacı saldırgan bir Fransız siber güvenlik stratejisi yaratmaktır. Aynı zamanda, ülkenin diğer devletlerden gelen saldırılara karşı misilleme yapma hakkını vurgulayarak caydırıcılık oluşturmaktadır.

Ocak 2017'de, Fransa İçişleri Bakanlığı'nın Silahlı Kuvvetler (MdA) birimi siber savunma birimi kurdu. Söz konusu orduyu koordine etmek için ComCyber olarak bilinen komuta kademesini oluşturdu.[10] Başka bir ifadeyle, yeni bir siber doktrin belirlenerek Fransa siber ortamda pasif savunmadan aktif taarruza geçti.[11] Bunun sonucunda da, ComCyber, Fransa'da aktif ve manevra gerçekleştiren oyunculardan biri oldu. 2017 yılındaki bu manevra değişikliğine giden süreç "*Savunma ve Ulusal Güvenlik Üzerine Stratejik İnceleme*" belgesiyle güçlenmiştir.[12]

[9] National Assembly Session Service Division Of Laws, "Initial project of the Law", 16.04.2015, Erişim Tarihi: 30.10.2021, Erişim Adresi: http://www.assemblee-nationale.fr/14/ta-pdf/2697-p.pdf, ss.1-45.
[10] Ministry of the Armed Forces, "The Cyber Defense Command (COMCYBER)", Erişim Tarihi: 03.11.2021, Erişim Adresi: https://www.defense.gouv.fr/ema/organismesinterarmees/le-comcyber/le-comcyber/comcyber.
[11] Éléments Publics De Doctrine Militaire De Lutte İnformatique Offensive Report (2019), Ministry of the Armed Forces, Erişim Tarihi: 03.11.2021, Erişim Adresi: https://www.defense.gouv.fr/fre/content/download/551497/9393997/El%C3%A9ments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdf, s. 4.
[12] *A.g.e.*

Cumhurbaşkanı Emmanuel Macron tarafından verilen emirle 2017 yılında Fransa'nın savunma ve ulusal güvenlik stratejileri yeniden incelenmiştir. Gerçekleştirilen söz konusu stratejik inceleme sonrasında, siber tehditlere ve siber güvenliğe atıfta bulunan üçüncü Fransız Ulusal Güvenlik Stratejisi ilan edilmiştir. Stratejik incelemenin ana odak noktası, Fransa'nın stratejik özerkliğini korumak, yüksek derecede teknolojik gelişmelere dayanmak ve endüstriyel ve operasyonel bağımsızlığı sağlamak olmuştur.

2018 yılı Fransa'daki siber kuruluşlar ve entegrasyon açısından farklı bir dönüm noktası olmuştur. Çünkü İçişleri Bakanlığı'nın Silahlı Kuvvetleri dezenformasyona karşı mücadele başlatmıştır.[13] Başlatılan mücadele sonrasında istihbarat servisleri aracılığıyla sahadaki gerçeklere yönelik araştırma gerçekleştirilmiştir. Böylece, düşmanların saldırılarına karşı koymak amacıyla harekete geçilmesi için bir adım atılmıştır.

2019 ve 2020 yılında da siber uzayda izlenecek iki yeni politika belirlendi. Bunlar "*Savunma Amaçlı Siber Savaş için Bakanlık Politikası*"[14] ve "*Taarruz için Askeri Doktrin içeren Kamusal Unsurlar*"dır[15]. Oluşturulan bu politikalar çerçevesinde, 2021 yılı içerisinde Fransa'nın siber uzayda üstünlüğü sağlama stratejisi tekrarlanmıştır.[16] Sonuç olarak, Fransa, siber uzayda başarılı olmak için birçok yeni politika geliştirmiştir.

1.2. Fransa'nın Yeni Taarruz Stratejisi ve Siber Doktrini

Siber savunma doktrini, siber saldırıların önlenmesini, öngörülmesini, tespit edilmesini ve siber saldırılara karşı korunmayı gerektirir. Doktrinin kapsamı, siber saldırıya tepki vermek ve siber saldırıya atıfta bulunmakla sınırlıdır. Ayrıca savunma amaçlı ve askeri olmayan önlemlerle sınırlıdır.

[13] Florence Parly (2018), "Statement by Ms Florence Parly, Minister of the Armed Forces, on the manipulation of information", 04.10.2018, Erişim Tarihi: 03.11.2021, Erişim Adresi: https://www.vie-publique.fr/discours/206652-declaration-de-mme-florence-parly-ministre-des-armees-sur-la-manipulat.
[14] Ministry of the Armed Forces (2019), "Ministerial policy of defensive IT control", Erişim Tarihi: 04.11.2021, Erişim Adresi: https://www.defense.gouv.fr/salle-de-presse/communiques/communique_la-france-se-dote-d-une-doctrine-militaire-offensive-dans-le-cyberespace-et-renforce-sa-politique-de-lutte-informatique-defensive.
[15] Press center of the Ministry of the Armed Forces (2019), "Public Elements Of Military Doctrine For Offensive Computer Warfare", 21.01.2019, Erişim Tarihi: 04.11.2021, Erişim Adresi:https://www.defense.gouv.fr/salle-de-presse/dossiers-de-presse/dossier-de-presse_elements-publics-de-doctrine-militaire-de-lutte-informatique-offensive.
[16] Comcyber (2019), "GDA Tisseyre: On Est 3400 Cybercombattants et on Deviendra 4500 en 2025"', @ComcyberFR on Twitter, 12.10.2019, Erişim Tarihi: 04.11.2021, Erişim Adresi: https://twitter.com/ComcyberFR/status/1172186486134968322.

Fransa'nın siber savunma doktrini, askeri siber birimlerinin "*barış-kriz-savaş*" sürekliliğini benimsemesine dayanmaktadır. Bu süreklilik, her şeye her an hazırlıklı olmaya dayanmaktadır. Bu nedenle, başarısızlık durumu aslına bakılırsa çatışma durumu olarak nitelendirilmektedir.[17]

Fransa'nın ilan ettiği saldırı doktrini yeni bir şeydir. Çünkü siber faaliyetin konvansiyonel askeri operasyonlara entegre edilmesini hedeflemektedir. Saldırgan yaklaşım, olumsuz sistemlerin kullanılabilirliğini veya gizliliğini reddetmeyi amaçlayan gizli eylemler olarak tanımlanmaktadır. Bu bağlamda, Philippe Baumard, dünya çapında 35 ülkenin analitik verilerine dayanan ulusal siber doktrinlerin bir karşılaştırmasını gerçekleştirmiştir. Gerçekleştirilen incelemeler neticesinde, teknoloji ve politika arasında dengeli bir bakış açısı ortaya koymuştur. Fransa üzerine gerçekleştirilen incelemelerde, Fransa'nın önünde daha izlemesi gereken çalışmalar olduğu değerlendirilmektedir.[18]

2018 yılında gerçekleştirilen ve siber uzay için bir davranış kuralı olan Paris Çağrısı'ndan sonra, Fransız Silahlı Kuvvetler Bakanı Florence Parly, siber uzayda ilk saldırgan doktrini ilan etti. Doktrin, düşman sistemlerinin etkisiz hale getirilmesini hedeflemektedir. Ancak kavram belirsizdir. "*Taarruz harekâtı ne şekilde gerçekleşecektir?*", "*Asıl amaç geleneksel harekâtları hazırlamak ya da tanımlamak mıdır?*", "*Bir kuvvet çarpanı mıdır?*", "*Diğer çarpanların yerini alabilir mi?*" gibi sorular doktrinde net olarak belirtilmemiştir. Fakat doktrinin saldırgan niteliği siber uzayın operasyonlardaki etkinliğini arttırmaktadır. Bu doğrultuda, Fransa'nın siber saldırı doktrini, siyasi, hukuki ve askeri risklerin dikkate alınmasına ve azaltılmasına büyük önem vermektedir. Fakat doktrin, bilgi veya silah sistemlerinin bütünlüğüne karşı operasyonlara yönelik açıklama yapmamıştır.

Diğer yandan, 2011 yılında yayınladığı doktrinle birlikte, Fransa, uluslararası ilişkilerde bir siber savaş ve bilgi savaşı yaşandığını kabul etmiştir. Bu ön kabul çerçevesinde, Fransa, siber uzaya yönelik meselelerde güvenlik ve teknik konularını bir arada değerlendirmiştir. Ticari perspektiflerin artması ve askeri çıkarların oluşması da bu yaklaşımda etkili olmuştur. Bunun sonucunda, Fransa özelinde yeni bir modelleme ortaya çıkmıştır. Bu yeni model, siber uzayda birleşik bir ulusal güvenlik görüşüne dayanmaktadır.

[17]Arthur P.B. Laudrain (2019), "France's New Offensive Cyber Doctrine", Lawfare, 26.02.2019, Erişim Tarihi: 29.10.2021, Erişim Adresi: https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine.
[18] Philippe Baumard (2017), *Cybersecurity in France*, ss.67-96.

Aynı zamanda, Fransa tarafından ilan edilen Ulusal Güvenlik Stratejisi ile birlikte siber sınırların savunmasını gerçekleştirmek amacıyla dijital egemenlik sınırları belirlendi. Sınırların belirlenmesinin hemen ardından, söz konusu siber sınırları korumak amacıyla silahlı kuvvetler içinde Siber Savunma Komutanlığı kuruldu. Buna paralel olarak, Dışişleri Bakanlığı, daha önce ilan ettiği Paris Çağrısı'nı yineledi. Böylece, Fransa'nın Uluslararası Dijital Stratejisi resmi olarak açıklandı.

Son olarak, 2018 yazında yürürlüğe giren ve 2019-2025 arasındaki planları belirleyen Askeri Programlama Kanunu çerçevesinde siber uzayda taarruz amacıyla büyüme stratejileri belirlendi. Belirlenen plan çerçevesinde, Fransa'nın siber savaşçı sayısı ve siber savunma bütçesinde artış öngörüldü. Böylece, Fransa, 2025 yılına kadar askeri programlarla ilgili olarak 1.000 yeni siber güvenlik uzmanını işe alacağını ve 1,5 milyar avro (1,8 milyar ABD doları) tahsis edeceğini ilan etti.[19] Fransa'nın bu açıklamaları uluslararası ilişkilerde caydırıcı bir unsur olarak görülebilir. Ayrıca, bu açıklama, saldırgan bir politika izlendiğinin en temel göstergesidir.

1.3. Fransa'nın Siber Yetenekleri ve Milli Güç Sıralaması

Fransa, birçok açıdan Avrupa Birliği'nde lider ülkedir. Bu durum, siber güvenlik harcamalarında da kendini göstermiştir. Bu kapsamda, 2020 yılına ait siber güvenliğe yönelik harcama raporları incelendiğinde; Fransa'nın siber güvenlik önlemleri için birçok AB ülkesinden daha fazla harcama gerçekleştirdiği görülmektedir.[20]

Fransa'nın siber güvenliği sağlamaya yönelik devlet olarak verdiği bu önem, Fransız şirketlerinde de görülmektedir. Fransız şirketleri, siber güvenlik konusunda ciddi harcamalar gerçekleştirmektedir. Bu kapsamda, şirketlerin siber güvenlik konusunda gerçekleştirdikleri harcamaları temel alan bir araştırma dünyanın önde gelen altı borsa endeksinde yer aldı. Paris'in CAC 40 listesinde yer alan şirketlerin büyük çoğunluğunun siber güvenlik konusunda yüksek olgunluk seviyesine ulaştığı görülmüştür.[21]

[19] Ellen Tannam (2019), "Defence Secretary Says France Will Take An Offensive Cybersecurity Strategy", Silicon Republic, 23.01.2019, Erişim Tarihi: 03.11.2021, Erişim Adresi:https://www.siliconrepublic.com/enterprise/france-cybersecurity-parly.
[20] NIS Investments Report (2020), "European Union Agency for Cybersecurity", Erişim Tarihi: 28.10.2021, Erişim Adresi: https://www.enisa.europa.eu/publications/nis-investments/at_download/fullReport, s. 7.
[21] Top Companies Cybersecurity Index: 2020 Annual Reports (2020), Wavestone, Erişim Tarihi: 28.10.2021, Erişim Adresi: https://www.wavestone.com/app/uploads/2020/07/Wavestone-Cyberindex-top-companies-2020-EN.pdf, s. 1.

Bununla birlikte, bu harcamalar ve çabalar Fransa'nın siber uzayda kendini tamamen güvende hissetmesi için yeterli değildir. Çünkü 2020 boyunca yerel yönetim hizmetlerine yönelik siber saldırılarda artış yaşanmış ve bu artışlar arasında en büyük oranın fidye yazılımlara ait olduğu tespit edilmiştir. Bu bağlamda, siber güvenlik çabası dinamik bir mücadele gerektirmektedir. Fransız hükümeti de siber saldırılara engel olmak amacıyla tam anlamıyla bir destek verememektedir.

Fransa'nın siber yeteneğini oluşturan altyapısının güvenliği SGDSN'dir. SGDSN'nin sorumlulukları arasında hükümetin uygulamaları yer almaktadır. Bu uygulamaları, kritik ulusal altyapı politikalarını işletmekten sorumlu şirketler belirlemektedir. Ayrıca 2014-2019 yıllarını içeren "*Savunma Planlama Yasası*" ağların güvenliğini sağlama noktasında ciddi çalışmalar gerçekleştirmiştir.

Bu çalışmalara öncülük eden ve Fransız Devleti tarafından görevlendirilmiş ajanslar iç hukuka göre yetkilendirilmiştir. Örneğin, Fransa'nın savunma tedarik ajansı General Silahlanma Müdürlüğü (DGA), bilgi kontrolünün bir parçası olarak görev yapmaktadır.[22] DGA'nın görevleri arasında; siber saldırıların gerçekleşmesini sağlayan siber silahlara karşı ulusal yapılardaki bilgi ve silah sistemlerinin korunması bulunmaktadır. Bunu sağlamak için de, Silahlı Kuvvetler içerisinde teknik uzmanlık sağlamayı hedeflemektedir. Böylece, krizlerin çözümünde ve istihbarat faaliyetlerine yönelik oluşabilecek tehditlere destek sağlamaktadır.[23]

Bu sorumlulukların bir parçası olarak, Fransız Silahlı Kuvvetleri, siber sistemler üzerine araştırma ve geliştirme faaliyetlerini arttırmıştır.[24] Aynı zamanda, mücadeleyi dinamik tutmak, ani saldırılara karşı personelleri hazır bulundurmak ve personellerin tecrübesini arttırmak için 2015 yılından bu yana siber savaş oyunları düzenlemektedir. [25]

[22] Directorate General of Armaments, Erişim Tarihi: 29.10.2021, Erişim Adresi: https://www.defense.gouv.fr/dga.
[23] White Paper: Defense and National Security Report (2013), Ministry of the Armed Forces, Erişim Tarihi: 29.10.2021, Erişim Adresi: http://www.livreblancdefenseetsecurite.gouv.fr/index.html.
[24]Alexandra Valetta Ardisson & Bastien Lachaud (2018), "Filed In Application of Article 145 of the Rules, By the Commission for National Defense and the Armed Forces, In Conclusion of the Work of a Cyber Defense Information Mission", National Assembly, 04.07.2018, Erişim Tarihi: 29.10.2021, Erişim Adresi: http://www2.assemblee-nationale.fr/documents/notice/15/rap-info/i1141/#P439_94811.
[25] Intelligence Online (2018), "The DGA Develops Cyber Warfare Games In Bruz", 04.07.2018, Erişim Tarihi: 29.10.2021, Erişim Adresi: https://www.intelligenceonline.fr/renseignement-d-etat/2015/03/11/la-dgadeveloppe-les-jeux-de-cyberguerre-a-bruz,108065256-bre.

Fransız Devleti tarafından planlı olarak yürütülen siber savaş oyunları, milli imkânlarla siber yeteneklerin geliştirilmesi için çok önemlidir. Bu çerçevede, özellikle son 20 yılda siber yetenekler ulusal gücün yeni bir aracı haline geldi.

Siber yetenekleri belirterek ulusal karar alma süreçlerine yardımcı olmak amacıyla IISS tarafından bir rapor hazırlanmıştır. Hazırlanan bu rapor, ulusal güçler arasındaki farkları belirtmektedir. Ayrıca ülkelerin hükümetlerine ve şirketlerine yönelik risk hesaplamaları gerçekleştirilerek ülkelerin mevcut durumlarını görmeleri sağlanmaktadır. Bu kapsamda, rapora göre ülkelerin yetenekleri 7 bölümde değerlendirilmiştir. Değerlendirilen kategoriler şunlardır; [26]

• Strateji ve doktrin,

• Yönetim, komuta ve kontrol,

• Temel siber istihbarat yeteneği,

• Siber güçlendirme ve bağımlılık,

• Siber güvenlik ve esneklik,

• Siber uzay işlerinde küresel liderlik,

• Saldırgan siber yetenek.

Bu kategoriler çerçevesinde gerçekleştirilen inceleme sonrasında, saldırı ve savunma açısından Fransa'nın durumu çok iyi değildir. Özellikle BM'nin daimi üyeleri olan ABD, Çin, İngiltere ve Rusya'nın birçok konuda gerisindedir. Fakat Fransa'nın siber güvenlik konusunda güçlü ve geniş bir istihbarat erişimine sahip olduğu gözükmektedir.

Tüm bu süreçler karşısında uluslararası ilişkilerde Fransa'nın tutumu saldırgan bir görüntü sergilemektedir. Çünkü Fransa'nın 2019-2025 askeri program yasasında siber savunma için ayırdığı 1,6 milyar avronun (1,8 milyar dolar) 2025'e kadar "*1.000 siber savaşçı*" kiralamak için kullanılacağı Bakan Parly tarafından belirtilmiştir.[27]

[26] The International Institute for Strategic Studies (2019), "Cyber Capabilities And National Power: A Net Assessment", Erişim Tarihi: 29.10.2021, Erişim Adresi: https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power, ss. 57-69.

[27]Christina Mackenzie (2019), "French Defense Chief Touts Offensive Tack In New Cyber Strategy", Fifth Domain, 18.01.2019, Erişim Tarihi: 29.10.2021, Erişim Adresi: https://www.fifthdomain.com/global/europe/2019/01/18/french-defense-chief-touts-offensive-tack-in-new-cyber-strategy/.

Ayrıca, NCPI (2020), ITU (2018) ve Economist Intelligence Unit tarafından sağlanan veriler ışığında oluşturulan siber güç sıralamasında Fransa ilk 10 arasında yer almaktadır.[28] Fransa; NCPI (2020) sıralamasında 6. sırada, ITU (2018) sıralamasında 3. sırada ve Economist Intelligence Unit sıralamasında yine 6. sırada yer almaktadır.[29]

Aynı zamanda, Fransız hükümeti, küresel bir güç olma çabasıyla ulusal siber savunmasındaki 2017 yılı verilerine göre 2 milyar avroluk bir bütçeye sahiptir. Sahip olduğu bütçeyi geliştirmeye yönelik planları çerçevesinde 2014-2019 arası 1 milyar avro yatırım yapmayı taahhüt etmiştir. Bunun en önemli sebebi, Fransız siber güvenlik sektörünün önemli bir dinamizmden gelmesidir. Bu dinamizm içinde Fransız siber güvenlik pazarındaki ilk 5 şirket (Morpho, Thales, Orange, Cassidian ve Atos) toplam satışların yüzde 75'inden fazlasını temsil etmektedir. Yaklaşık 40.000 kişinin çalıştığı Fransız siber güvenlik endüstrisi, her yıl yaklaşık yüzde 10 oranında büyümektedir. Çünkü genel olarak siber suçların Fransız şirketlerine maliyeti 2015 yılında 3,3 milyar avroyu aşmıştır. Bu oran ilerleyen süreçte daha da artacaktır. Bunun en önemli sebebi, 2020 sonu itibariyle Fransa'da tüm nesnelerin yüzde 15'inin internet bağlantısında olmasıdır. Bu orandaki artış, siber saldırıları da arttıracak ve bu artış siber güvenlik sektörünün büyüklüğünü pekiştirecektir.[30]

Sonuç olarak, Fransa'nın siber güvenliğe verdiği önem her geçen gün artmaktadır. 2020 yılında Fransa siber güvenlik pazarı 7,42 milyar ABD doları değerindeydi. 2026 yılına kadar yaklaşık yüzde 6'lık büyüme beklenmektedir. [31] Artan kullanım oranı ile birlikte pazarın da büyümesiyle doğru orantılı olarak Fransa'da son yıllarda siber saldırılar ve siber suçlar önemli ölçüde artmıştır. Fransa'da artan siber saldırılara yönelik verileri 2019 Hiscox Siber Hazırlık Raporu'nda görebiliriz. Rapora göre, 2019'da Fransa'daki firmaların yüzde 67'sinden fazlası siber saldırıya uğradı.[32]

---

[28] NCSI, Erişim Tarihi: 29.10.2021, Erişim Adresi: https://ncsi.ega.ee/country/fr/.

[29]Julia Voo & Irfan Hemani (2020), "National Cyber Power Index 2020 Methodology and Analytical Considerations Report", Harvard Kennedy School Belfer Center for Science and International Affairs, Erişim Tarihi: 29.10.2021, Erişim Adresi: https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf, ss. 7-8.

[30] Charles DeFranchi & Christophe Joly (2016), "Cyber Security Opportunities in France", International Trade Administration, Erişim Tarihi: 29.10.2021, Erişim Adresi: https://2016.export.gov/france/build/groups/public/@eg_fr/documents/webcontent/eg_fr_110164.pdf.

[31] Mordorintelligence, "Fransa Siber Güvenlik Pazari - Büyüme, Eğilimler, Covid-19 Etkisi ve Tahminler (2022 - 2027)", Erişim Tarihi: 29.10.2021, Erişim Adresi:https://www.mordorintelligence.com/industry-reports/france-cybersecurity-market.

[32] Hiscox (2020), "Hiscox Cyber Readiness Report 2020", ss. 1-16.

1.4. Fransa'nın İkili İlişkileri ve İttifakları

İkili ilişkilerin karşılıklı güvene dayanması gerekmektedir. Fransa'nın üyesi olduğu ve ittifak ilişkilerini sürdürdüğü NATO ve AB ilişkileri koşulsuz güvene dayanmaktadır. Fakat konu siber uzay olduğunda, koşulsuz güvenden bahsedilmemektedir. Özellikle NATO'nun Siber Savunma Taahhüdü ve Avrupa Birliği'nin siber ortamda birlik girişimleri Fransa için güçlü bir ortaklık durumu olarak gözükebilir. Fakat tam anlamıyla resmi bir güvenlik şemsiyesi sağlamamaktadır.

Fransa, AB ile olan iş birliği çerçevesinde Rusya'yı siber uzayda ortak tehdit olarak görmektedir. Örneğin, Ekim 2018'de, Fransa Dışişleri Bakanlığı, diğer üye ülkelerin Rusya'ya atfettiği Kimyasal Silahların Yasaklanması Örgütü'nün hacklenmesi olayında Fransa'nın müttefiklerinin yanında olduğunu söyleyerek tepki göstermiştir.[33]

Diğer yandan, Hindistan ve Fransa arasında siber uzaya yönelik bir dizi görüşme gerçekleştirilmiştir. Üçüncü Hint-Fransız Siber Diyaloğu 20 Haziran 2019 Perşembe günü Paris'te gerçekleştirildi. Gerçekleştirilen bu toplantıya Fransa'nın Dijital İşlerden Sorumlu Büyükelçisi Henri Verdier ve Hindistan Dışişleri Bakanlığı'nda E-Yönetişim, Bilgi Teknolojisi ve Siber Diplomasiden sorumlu Ortak Sekreter Shri Upender Singh Rawat katıldı. Toplantı sonrasında gerçekleştirilen açıklamada, her iki tarafın da tehdit analizlerini paylaştığı ve kendi siber politikalarındaki son gelişmeler ile kritik ulusal altyapılarının korunması için attıkları adımların konuşulduğu belirtilmiştir. Ayrıca, siber uzayda barış, güvenlik, dijital egemenlik ve internet yönetişimi konuları hakkında görüş alışverişinde bulunulmuştur. İlave olarak, iş birliğini derinleştirecek alanlar belirlenmiştir. Böylece, Fransa ve Hindistan, açık, güvenilir, güvenli, istikrarlı ve barışçıl bir siber uzaya olan bağlılıklarını yeniden teyit etmiştir.[34]

Aynı zamanda, Fransa, 2010 tarihli SOG-IS Avrupa karşılıklı tanıma anlaşmasının imzacıları arasındadır. 8 Eylül 2014 tarihinden itibaren geçerli olan bu anlaşmayı Fransa adına imzalayan kurum ANSSI'dir. Özellikle "*Akıllı kartlar ve benzeri cihazlar*" konusunda Avrupa'da birlik sağlamaya yönelik teknik alan çalışmaları özelinde kalifiye bir sertifikasyon sürecini sağlamayı

[33]François Delerue & Alix Desforges & Aude Géry (2019), "A Close Look at France's New Military Cyber Strategy", 23.04.2019, Erişim Tarihi: 31.10.2021, Erişim Adresi: https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/.

[34] Ministry of Europe And Foreign Affairs (2019), "France Diplomacy", Erişim Tarihi: 31.10.2021, Erişim Adresi: https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/fight-against-organized-criminality/cyber-security/.

hedeflemektedir.[35] Bu doğrultuda Avrupa Birliği'nde liderlik konusunda faaliyetler yürüten Fransa, ABD'nin AB verilerine erişimini engellemek istemektedir. Bunu gerçekleştirmek için de AB tarafından bir dizi siber kural getirilmesini istemiştir. Yeni siber güvenlik sertifikası da bunlardan biridir. Böylece, Amerikan kolluk kuvvetlerinin Avrupa'daki kritik verilere doğrudan erişimini engellemeyi planlamaktadır.[36]

Sonuç olarak, siber uzayda stratejik istikrarı ve uluslararası güvenliği artırmak Fransa'nın önceliğidir. Bu öncelik özelinde Avrupa ve Dışişleri Bakanlığı, Fransa'nın "*siber diplomasi*" konusundaki çalışmalarını koordine etmektedir. Bu doğrultuda gerçekleştirilen dijital diplomasi faaliyetleri Fransa'nın ilgisini ortaya koymaktadır.[37]

1.5. Fransa'nın Siber Uzay'daki Küresel Liderlik Hedefi

Fransa, önemli bir uluslararası ve Avrupalı aktördür. Fransa, Avrupa'nın tek nükleer gücü ve BM Güvenlik Konseyi'ndeki beş daimi üyeden biridir. AB ve NATO'da lider konumdadır. Birçok konuda kapsayıcı ve etkileyici bir rol almaktadır. Bu sebeple, uluslararası sahnede rol alan en önemli ülkelerden biri Fransa'dır. Bu özelliklerini kullanmak isteyen Fransa, uluslararası ilişkilerde beşinci bir boyut olarak görülen siber uzaydaki anarşik yapı içerisinde kendini sorumluluk almak zorunda hissetmektedir. Yaptığı düzenlemeler sonucunda da siber uzayda önemli bir oyuncu olmak istemektedir.[38]

Bu istekleri doğrultusunda, Fransa, siber uzayda gerçekleşen mevcut bilgisayar korsanlığını sınırlamak için kurumsal mekanizmaların geliştirilmesini önermektedir. Bu öneri kapsamında, Paris, 2018 yılında siber uzayda istikrarsızlaştırıcı faaliyetlerin uluslararası bir girişim aracılığıyla çözülmesi amacıyla "*Siber Uzayda Güven ve Güvenlik için Paris Çağrısı*"nı ilan

[35] "French National Digital Security Strategy", French Republic Prime Minister, Erişim Tarihi: 04.11.2021, Erişim Adresi:https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf, ss.1-44.
[36]Laurens Cerulus (2021), "France Wants Cyber Rule To Curb US Access To EU Data", *Politico*, 13.10.2021, Erişim Tarihi: 31.10.2021, Erişim Adresi: https://www.politico.eu/article/france-wants-cyber-rules-to-stop-us-data-access-in-europe/.
[37] French Ministry for Europe and Foreign Affairs (2019), "France Diplomacy Digital Diplomacy", 18.09.2019, Erişim Tarihi: 30.10.2021, Erişim Adresi: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/.
[38] Ministry of Europe and Foreign Affairs (2017), "France's International Digital Strategy", 15.12.2017, Erişim Tarihi: 03.11.2021, Erişim Adresi: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-s-international-digital-strategy/#:~:text=France's%20international%20digital%20strategy%2C%20presented,governance%2C%20the%20economy%20and%20security.

etti.[39] Böylece, Fransa, BM Hükümet Uzmanları Grubu[40] ve AB siber güvenliğinin çerçevelenmesinde aktif olarak yer almıştır.

Diğer yandan, Fransa, uluslararası alandaki gücünü kullanarak siber diplomasi alanında da güçlü olmak istemektedir. Bu doğrultuda, 2019'da üçüncü Hindistan-Fransa Siber Diyaloğu gerçekleştirildi.[41] 2020 yılında AB içerisinde birlikteliği sağlama amacıyla Fransa ve Almanya'yı kapsayacak şekilde üçüncü yıllık BİT güvenlik değerlendirmesini yayınladı.[42] Ayrıca, Fransa'nın G7 Başkanlığı sürecinde de siber uzay için gönüllü normların uygulanması konusunda faaliyetlerde bulunuldu.[43]

Son yıllarda siber uzaya yönelik Fransa tarafından gerçekleştirilen bu stratejiler, Fransa'nın lider olma hedefiyle doğrudan bağlantılıdır. Çünkü Fransa, siber sınırlarının güvenliğini sağlamada ve istikrarını oluşturmada aktif rol oynamak istemektedir. Bu amaç çerçevesinde, Fransa, AB'ye karşı gerçekleştirilen siber saldırılara karşı faillere karşı yaptırım uygulanması konusunda AB'nin harekete geçirilmesinde öncü rol oynadı.[44] Örneğin, 2020'de gerçekleşen siber saldırılardan sonra Rusya ve Çin'e karşı ilk AB yaptırımı gerçekleşti.[45] AB tarafından

[39]Arthur Laudrain (2018), "Avoiding A World War Web: The Paris Call for Trust and Security in Cyberspace", Lawfare, 04.12.2018, Erişim Tarihi: 03.11.2021, Erişim Adresi: https://www.lawfareblog.com/avoiding-world-war-webparis-call-trust-and-security-cyberspace.

[40] UN Office for Disarmament Affairs, "Developments In The Field Of Information And Telecommunications In The Context Of International Security", Erişim Tarihi: 03.11.2021, Erişim Adresi: https://www.un.org/disarmament/ict-security.

[41] Ministry of Europe and Foreign Affairs (2019), "Indo-French Bilateral Cyber Dialogue", 20.06.2019, Erişim Tarihi: 03.11.2021, Erişim Adresi: https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/fight-against-organized-criminality/cyber-security/article/indo-french-bilateral-cyber-dialogue-20-06-19.

[42] Federal Office for Information Security (Germany) ve National Information Systems Security Agency (2020), "Third edition of the Franco-German common situational picture", Erişim Tarihi: 03.11.2021, Erişim Adresi: https://www.ssi.gouv.fr/uploads/2020/12/anssi-bsi-common_situational_picture_2020.pdf, ss.1-20.

[43] Ministry of Europe and Foreign Affairs (2019), "G7 French presidency – Cyber Norm Initiative: Synthesis of Lessons Learned and Best Practices", 26.11.2019, Erişim Tarihi: 03.11.2021, Erişim Adresi: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/g7-french-presidency-cyber-norm-initiative-synthesis-of-lessons-learned-and.

[44] Ministry of Europe and Foreign Affairs, "Guaranteeing Cybersecurity", Erişim Tarihi: 03.11.2021, Erişim Adresi: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-s-international-digital-strategy/article/guaranteeing-cybersecurity.

[45] Ministry of Europe and Foreign Affairs (2020), "EU – Cyberattacks – Q&A from the press briefing", 30.07.2020, Erişim Tarihi: 03.11.2021, Erişim Adresi: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/eu-cyberattacks-q-a-from-the-press-briefing-30-jul-20.

gerçekleştirilen bu yaptırımda, Rusya'nın askeri istihbarat müdürlüğündeki (GRU) dört üyesine ve iki Çinli vatandaşa seyahat yasağı getirilmiş ve mal varlıkları dondurulmuştur.[46]

2. Fransa'nın Siber Sürecine Yakından Bir Bakış

2.1. Siber Konuları Ele Alan Temel Yasal ve Düzenleyici Hükümler

Fransa'nın siber güvenliği sağlamaya yönelik geliştirdiği yasal süreç 2009 yılından sonra hızlanmıştır. Yasal sürecin güçlenmesinde ANSSI en önemli kurumdur. ANSSI'nin kurulmasının sebebi, siber uzayda tüm süreçlerden sorumlu milli bir otorite kurulmak istenmesidir. Bu doğrultuda, Avrupa Birliği'nde Genel Veri Koruma Yönetmeliği'nin (GDPR) yürürlüğe girmesiyle birlikte, Fransa, siber güvenlik politikalarıyla ilgili büyük reformlar başlattı.

Fransa'da siber güvenlikle alakalı sıklıkla kullanılan 4 temel yasa bulunmaktadır. Bu yasalar; Godfrain Yasası (*The Godfrain law*), *The FDPA, The Law for a Digital Republic* ve *The network and Information System* (*NIS Rules*) şeklindedir. Bu temel yasalar etrafında zaman içerisinde bazı temel reformlar gerçekleştirilmiştir.

Bu bağlamda, Fransa'nın siber güvenlik rejimi, 1978 Veri Koruma Yasası'na kadar uzanmaktadır. BT dolandırıcılığına ilişkin 1988 Godfrain Yasası, Veri Koruma Yasası'nı izleyen ve bilgisayar suçları ve bilgisayar korsanlığı konusunda ilk eylem olan bir başka öncü BT yasasıdır. 21 Haziran 2004 tarihli Dijital Ekonomiye Güven Yasası (2004-575) ("*LCEN*" olarak da bilinir) 8 Haziran 2000 tarihli AB E-Ticaret Direktifi'ni ve 12 Temmuz 2002 tarihli Gizlilik ve Elektronik İletişim Direktifi'ni ulusal mevzuata aktarmıştır. Bir sisteme izinsiz giriş eylemleri gerçekleştirmek veya bir sistemin işleyişini engellemek için tasarlanmış teçhizatın bulundurulması ve sağlanması ile ilgili olarak Ceza Kanunu'na Bölüm 323-3-1'i ekledi. Aynı zamanda, ANSSI tarafından oluşturulan Genel Güvenlik Referansı, uyguladıkları elektronik değişimlerin güvenliğini sağlamada idari makamlara yardımcı oldu. 13 Temmuz 2018 tarihli

[46] Lorie Maglana & Sunny Man (2020), "Europe: EU Imposes The First Ever Sanctions Against Cyber-Attacks", Global Compliance News, 21.08.2020, Erişim Tarihi: 03.11.2021, Erişim Adresi: https://www.globalcompliancenews.com/2020/08/21/eu-imposes-the-first-ever-sanctions-against-cyber-attacks-20200810/.

2019-2025 (2018-607) Askeri Programlama Yasası'nın 34. bölümü, ulusal güvenliği artırmak için bilgisayar saldırılarını tespit etme kapasitesini güçlendirmeye yönelik hükümler eklendi.[47]

İlerleyen süreçte, 18 Aralık 2013 tarihli Askeri Programlama 2014-2019 (2013-1168) Yasası ilan edildi. Böylece, "*hayati öneme sahip operatörlerin*" (OIV'ler) -yani güvenlik veya operasyon ihlalinin Fransa'nın güvenliğini önemli ölçüde azaltabileceği sistem operatörlerinin- BT güvenliğini güçlendirdi. Daha sonrasında da 26 Şubat 2018 tarihinde Ağların ve Bilgi Sistemlerinin Güvenliği Yasası (2018-133) gerçekleştirildi. Söz konusu yasa ile birlikte yükümlülüklerin OIV'ler dışındaki operatör kategorilerine genişletilmesine olanak sağlandı. Bu durum, iki yeni aktör kategorisi yarattı. Bu kategoriler; "*temel hizmet operatörleri*" (OSE'ler) ve "*dijital hizmet sağlayıcılar*"dır (FSN'ler). Ayrıca, 17 Nisan 2019 tarihli son AB Yönetmeliği olan ve doğrudan bağlayıcı bir genel uygulama kanunu olan bilgi ve iletişim teknolojisi siber güvenlik sertifikasına (Siber Güvenlik Yasası) tabi olduğunu kabul etmiştir.

Yukarıda bahsedilen ulusal yasalara ek olarak oluşturulan uluslararası yasaların da iç hukuka etkileri olmuştur. Bu çerçevede, Fransa, 1 Mayıs 2006'da yürürlüğe giren Budapeşte Siber Suç Sözleşmesi'ni imzalamıştır. İmza altına alınan bu sözleşme kapsamında yükümlülüklerini yerine getirmek isteyen Fransa, ITU-IMPACT koalisyonunun bir parçası olmuştur. Ayrıca EUROJUST, EUROPOL ve AB Siber Güvenlik Ajansı (ENISA) gibi birçok Avrupa kuruluşuna üye olmuştur.

Bu üyeliklerine ek olarak, Fransa, Veri Koruma Yasası uyarınca Veri Koruma Denetleme Kurumu'nu (CNIL) kurmuştur. Böylece üye kuruluşlarca bilgi sistemi güvenliği konusuyla Genel Veri Koruma Yönetmeliği'ne uyumu sağlamaktadır. Çünkü kurallara uymayan şirketlere siber suç bağlamında CNIL veya ANSSI tarafından yaptırım uygulanabilmektedir. CNIL ve ANSSI'nin yaptırım gücü ikisinin de bağımsız idari makam olmasından gelmektedir. Şirketler, bu organların kararlarına karşı doğrudan Fransız en yüksek idari mahkemesine (*Conseil d'Etat*) itiraz edebilmektedirler.

2.2. Yönetim, Komuta ve Kontrol Yapısı

Fransa'da siber tüzük ve yönetmeliklerin uygulanmasından sorumlu devlet kurumu ANSSI'dir. ANSSI, bilgi sistemlerini ve dijital kullanıcıları siber saldırılara karşı savunmak ve korumak için

[47]Jean Philippe Souyris (2021), "France: Cybersecurity Comparative Guide", Montaq, 16.04.2021, Erişim Tarihi: 03.11.2021, Erişim Adresi: https://www.mondaq.com/france/technology/963020/cybersecurity-comparative-guide.

2009 yılında kuruldu. ANSSI'nin birçok görevi bulunmaktadır. Bu görevlerden bazıları şunlardır;

- Hayati öneme sahip operatörlere yardımcı olur,
- Nitelikli ürünlerin ve güvenilir hizmet sağlayıcıların kullanılmasını önerir,
- Güvenlik önlemlerinin sağlamlığını kontrol etmek için denetimler yapar,
- Önerilerde bulunur,
- Etiketlerin ve niteliklerin yayınlanmasından ve standartların belirlenmesinden sorumludur.

Bu görevlere ek olarak, 18 Aralık 2013 tarihli Askeri Programlama Yasası'na (2013-1168) göre, ANSSI, ulusal politikayı tanımlayan ve bilgi sistemlerinin güvenliği ve savunması açısından hükümet eylemlerini koordine eden Başbakan adına hareket eder.

Fransa'nın siber konularda aldığı rota, Cumhurbaşkanı tarafından belirlenmektedir. 2018 yılında kurulan iki kurum rotanın belirlenmesinde önemli bir görev üstlenmektedir. ANSSI'nin içinde yer aldığı Ulusal Güvenlik Konseyi CDSN, SGDSN ve ComCyber Başkanı siber uzaya yönelik süreçlerde Fransa Genelkurmay Başkanı tarafından temsil edilir.

Bir diğer önemli organ Siber Savunma İcra Komitesi'dir. Bu komitedeki Başkan'ın yetkisi, üst düzey yetkililer tarafından alınan kararların uygulanmasında belirleyicidir. Ayrıca siber savunma yönlendirmesinin sorumluluğunu üstlenen SGDSN kapsamındaki komite, yılda bir kez rapor vermektedir.

Askeri bir varlık olan ComCyber, taarruzda en önemli kurumdur. Diğer önde gelen siber güçlerde olduğu gibi siber saldırılara karşı önemli görev üstlenmektedir. ComCyber'ın 2019'un sonlarında 3.400 personeli bulunmaktadır. Fakat 2025 yılına kadar 4.500'e ulaşması planlanmaktadır.

Fransa tarafından ilgili kurumlar arasında güçlü bir fikir birliği sağlanmaya çalışılmaktadır. Bu doğrultuda, yüksek kaliteli teknik sistemler tedarik edilmekte ve siber operasyonlara göre komuta düzenlemeleri planlanmaktadır.[48]

Son olarak, Fransa'da siber istihbarat üretiminin odak noktası Dış İlişkiler Genel Müdürlüğü'dür (DGSE).[49] Ancak, diğer ülkelerdeki gibi Fransa'da da istihbarat teşkilatlarının siber yetenekleri kendi özel yetkinlik alanına yöneliktir. Çünkü kurumlar da istihbarat faaliyetlerini yürütmektedir. Böylelikle siber uzaydaki taarruz ve savunma birbirinden ayrılmıştır. Bu kurumlar arasında Savunma İstihbarat ve Güvenlik Müdürlüğü[50], Askeri İstihbarat Müdürlüğü[51] ve İç Güvenlik Genel Müdürlüğü[52] bulunmaktadır.

2.3. Siber Alanın Konvansiyonel ve Etki Operasyonlarına Entegre Edilmesi

Fransa'nın yeni askeri siber stratejisine yakından baktığımızda, üzerinde durulması gereken bazı önemli noktalar bulunmaktadır. Bu kapsamda, Fransa'da "*siber savunma*" kavramı, Savunma Bakanlığı'nın ağları dâhil, devletin tüm ağlarının korunmasını sağlamayı amaçlayan ulusal çerçeveyi ifade eder. Bu nedenle, genel olarak Fransa'da siber savunma Ulusal Siber Güvenlik Ajansı'nın sorumluluğundayken, siber savunma komutanı (ComCyber) münhasıran Savunma Bakanlığı'nın siber savunmasından sorumludur.[53]

2018 yılında Fransa Silahlı Kuvvetler Bakanı Florence Parly tarafından ilan edilen siber savunma stratejisi ile birlikte Fransa'nın Silahlı Kuvvetler yapısına siber uzay entegre edilmiştir. Böylece Fransa'nın askeri siber stratejisinin unsurları belirlenmiş, stratejinin saldırgan yönleri belirtilmiş ve Fransız ordusunu 21. yüzyıl tehditlerine uyarlama çabası sergilenmiştir. Bu durum, Fransa'nın askeri üstünlük için siber uzayda üstün olma gereğini göstermiştir. Fransa tarafından

[48] Comcyber (2019), "GDA Tisseyre: On Est 3400 Cybercombattants et on Deviendra 4500 en 2025"', @ComcyberFR on Twitter, 12.10.2019, Erişim Tarihi: 04.11.2021, Erişim Adresi: https://twitter.com/ComcyberFR/status/1172186486134968322.
[49] Defense Intelligence and Security Directorate, Erişim Tarihi: 04.11.2021, Erişim Adresi: https://www.dgse.gouv.fr/en.
[50] Direction du Renseignement et de la Sécurité de la Défense, Erişim Tarihi: 04.11.2021, Erişim Adresi: https://www.drsd.defense.gouv.fr/.
[51] Directorate of Military Intelligence, Erişim Tarihi: 04.11.2021, Erişim Adresi: https://www.defense.gouv.fr/drm.
[52] General Directorate of Internal Security, Erişim Tarihi: 04.11.2021, Erişim Adresi: https://www.interieur.gouv.fr/Le-ministere/DGSI.
[53] François Delerue & Alix Desforges & Aude Géry (2019), "A Close Look at France's New Military Cyber Strategy", War On the Rocks, 23.04.2019, Erişim Tarihi: 30.10.2021, Erişim Adresi: https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/.

kabul edilen bu durum, siber silahların artık konvansiyonel ve nükleer silahların yanında Fransa'nın askeri yeteneklerinin bir parçası olduğunu simgelemiştir.

Diğer yandan, Fransa'nın siber savunma stratejisine yönelik açıkladığı doktrin, Fransa'nın siber gücünün duruşunu göstermektedir. Böylece, Paris, müttefiklerine ve ortaklarına olduğu kadar potansiyel saldırganlara da bir mesaj göndermiştir. Parly'nin sözleri ile gönderilen mesaj, Fransa'nın siber yeteneklerini kullanmaktan çekinmeyeceği ve gerekirse misilleme yapma gücüne sahip olduğunu göstermektedir. Bu durum, Fransa'ya karşı siber saldırı gerçekleştirmeyi düşünenlere karşı ciddi bir caydırıcılık yaratmıştır.

Bununla birlikte, Fransa'nın alenen ilan ettiği saldırgan doktrini, kendisine yönelik gerçekleştirilebilecek siber saldırıları affetmeyeceğini belirten güç göstermenin başka bir yoludur. İzlenen bu yeni yolun resmi bir nitelik kazandığının göstergesi ise Fransa yetkilileri tarafından siber uzaya yönelik gerçekleştirilen hukuksal ve kamusal atıflardaki artışlardır.

Son olarak, Fransız hükümeti, ister saldırı, ister savunma amaçlı olsun, siber operasyonlar hakkında kamuoyu önünde nadiren konuşmaktadır. Bu gerçek, Fransa'nın siber savaş doktrininin konvansiyonel süreçlere entegre olan eylem halindeki belirli örneklerine işaret etmeyi zorlaştırmaktadır. Ancak Parly ile birlikte, Fransa, saldırgan bir siber savaş doktrini yayınlayarak, siber saldırılara yönelik gelecekteki tepkisini ortaya koymuştur. Böylece, siber alanın konvansiyonel ve etki operasyonlarına entegre edilmiştir.

2.4. Fransa'ya Karşı Gerçekleştirilen Siber Operasyonlar

Sistemlerini güvence altına almak ve savunmak isteyen Fransa, bir dizi siber güvenlik önlemi uygulamaktadır. Bu uygulamaları gerçekleştirirken de herhangi bir siber saldırıya yanıt verme hakkını saklı tutmaktadır. Çünkü Fransa, kendi siber sınırlarındaki bilgi sistemleri üzerinde egemenliğini kullanmaktadır.

Fransa'nın elinde tuttuğu siber saldırılara karşı yanıt verme kararı uluslararası hukuka uygun olarak alınan siyasi bir karardır. Siyasi bir karar çerçevesinde gerçekleştirilecek bir yanıtta, siber saldırının ağırlığına bağlı olarak güç kullanımı oranı değişebilir. Çünkü Fransız Devleti, siber uzay sistemlerindeki alanlarına herhangi bir yetkisiz sızmanın gerçekleşmesini engellemek istemektedir. Bunun için de Fransız yasalarına göre dijital bir vektör aracılığıyla Fransız sınırlarındaki herhangi bir etkinin üretilmesi bir egemenlik ihlali olarak tanımlanmıştır. Bu

kapsamda, bir siber saldırının kuvvet kullanımını oluşturan etkilerin gerçekleşmesi halinde, Fransa, Birleşmiş Milletler Şartı'nın 4. maddesine göre karşı önlemler alabileceğini veya konuyu Birleşmiş Milletler Güvenlik Konseyi'ne (BMGK) getirebileceğini ilan etmiştir.[54] Fakat şu ana kadar böyle bir süreç yaşanmamıştır.

Siber uzayda genellikle Çin, Rusya ve Kuzey Kore'den siber saldırıların geldiği iddia edilmektedir. Bu kapsamda, söz konusu siber saldırıları gerçekleştiren ülkelere yönelik AB yaptırım uygulamıştır. Uygulanan bu yaptırım süreci Fransa'nın da desteğiyle gerçekleşmiştir. Alınan bu yaptırım kararları çerçevesinde, Avrupa çıkarlarını hedef alan ve AB'nin güvenliğini baltalayan siber saldırıların faillerine karşı oybirliğiyle yaptırım uygulanması kararı kabul edildi.[55]

Diğer yandan, Fransa'ya yönelik gerçekleşen siber saldırılar devletler dışında da gerçekleşmektedir. Özellikle terör örgütleri ve bireysel gruplar tarafından Fransa'ya yönelik siber saldırılar gerçekleşmektedir. Bu saldırıların odak noktasında hükümet ve Bakanlıklar bulunmaktadır.[56] Örneğin, 2015 yılında Fransız *Le Parisien* gazetesi, internet güvenlik şirketlerine dayandırdığı bir haberde, *Charlie Hébdo* dergisine ve Fransa merkezli binden fazla internet sitesine yönelik saldırıların arkasında "*siber-cihatçı*" grupların olduğunu yazdı.[57] 2017 yılında Fransa'da sadece Pazar günleri yayınlanan *Le Journal du Dimanche* gazetesine konuşan Savunma Bakanı Jean-Yves Le Drian, Cumhurbaşkanlığı seçimlerine 4 ay kala ABD'de olduğu gibi Fransa'daki seçimlerde de siber saldırı yapılması ihtimalinden bahsetmiştir.[58] Bir diğer örnekte ise Fransa'da beş Bakan'ın cep telefonlarında *"Pegasus*" adlı casus yazılım tespit edilmiştir. Ayrıca Cumhurbaşkanı Macron'un da aralarında bulunduğu eski Başbakan Edouard Philippe ile hükûmetin üst düzey isimlerini ve gazetecileri de içeren yaklaşık 100'den fazla

[54] International Law Applied To Operations In Cyberspace (2019), The French Ministry Of The Armies, ss. 1-20.
[55] The French Ministry for Europe and Foreign Affairs (2020), "EU Cyberattacks-Q&A From The Press Briefing", 30.07.2020, Erişim Tarihi: 04.11.2021, Erişim Adresi: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/eu-cyberattacks-q-a-from-the-press-briefing-30-jul-20.
[56] Defense And Security Of Information Systems: France's Strategy (2011), National Information Systems Security Agency, Erişim Tarihi: 04.11.2021, Erişim Adresi:https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf.
[57] Kayhan Karaca (2015), "Fransa Siber-Cihatçıların Da Hedefinde", *Deutsche Welle Türkçe*, 15.01.2015, Erişim Tarihi: 04.11.2021, Erişim Adresi: https://p.dw.com/p/1EKx5.
[58] *Diriliş Postası* (2017), "Fransa'da Cumhurbaşkanlığı Seçimlerinde 'Siber Saldırı' Uyarısı", 08.01.2017, Erişim Tarihi: 04.11.2021, Erişim Adresi:https://www.dirilispostasi.com/haber/6292216/fransada-cumhurbaskanligi-secimlerinde-siber-saldiri-uyarisi.

kişinin telefonuna sızma girişiminde bulunulduğu tespit edilmiştir.[59] Eylül 2019'da, ülkenin önde gelen havacılık şirketlerinden biri olan Airbus, ticari sırlar ve güvenlik arayışı içinde tedarikçilerini hedef alan bir dizi siber saldırıya uğramıştır.

Yukarıda bahsedilen tüm bu örneklerden de anlaşıldığı üzere, Fransa'da son yıllarda birçok siber saldırı örneği yaşanmıştır. Fransa'da yaşanan tüm bu siber saldırı örnekleri çerçevesinde Fransa'nın AB içerisindeki durumuna baktığımızda, Eurostat verileri ön plana çıkmaktadır. Eurostat'a göre, güvenlikle ilgili sorunlar yaşayan ülkelerden en yüksek orana sahip olan ülkeler Danimarka (% 50), ardından Fransa (% 46), İsveç (% 45), Malta (% 42), Hollanda (% 42), Bulgaristan (% 13) ve Yunanistan'dır (% 13).[60]

Fransa'nın siber saldırılarda başı çekmesine paralel olarak, 2019 yılı Ocak ayında, Florence Parly, son yıllarda gerçekleşen siber vakalara atıfta bulunarak, Fransa'ya yönelik gerçekleşen siber saldırılardan Rusça konuşan bir siber casus grubu olan Turla'yı sorumlu tutmuştur. Turla'nın sorumlu tutulduğu bu vakalar arasında 2017 ve 2018 yıllarında Fransız Donanması'nın petrol tedarik zincirinin ayrıntılarını ortaya çıkaran saldırılar, Fransa seçimleri arifesinde Macron'un kampanyasına ait belgelerin koordineli bir şekilde sızması ve üst düzey Fransız yetkililerin hedef alınması gibi iç politikasına dışarıdan müdahaleler bulunmaktadır.[61]

Bu doğrultuda gerçekleşen siber saldırı örnekleri karşısında, Fransa, önlem alıp savunma yapabilmek amacıyla siber politikalar geliştirmeyi hızlandırmıştır. Çünkü ağ güvenliği ve veri kaybını önlemek Fransa için çok önemlidir. Özellikle siber saldırılar yoluyla kaybedilen verileri kurtarmaya çalışırken önemli miktarda para ve zaman harcanmaktadır. Bu yüzden, bu tür saldırılara karşı savunma yapma ve siber güvenliği sağlama amacıyla BT altyapısına yatırım yapmaktadır. Bu yatırımlara yönelik gerçekleştirilen harcamaların ilerleyen dönemde daha da artması beklenmektedir. Bu durum da Fransa'da siber güvenlik çözümlerine olan talebi artıracaktır.

---

[59] *Anadolu Ajansı* (2021), "5 Fransız Bakanın Telefonunda Casus Yazılım Pegasus'un İzi Bulundu", 24.09.2021, Erişim Tarihi: 04.11.2021, Erişim Adresi: https://www.gazeteduvar.com.tr/5-fransiz-bakanin-telefonunda-casus-yazilim-pegasusun-izi-bulundu-haber-1536117.

[60] Mordorintelligence, "Fransa Siber Güvenlik Pazari - Büyüme, Eğilimler, Covid-19 Etkisi ve Tahminler (2022 - 2027)", Erişim Tarihi: 29.10.2021, Erişim Adresi: https://www.mordorintelligence.com/industry-reports/france-cybersecurity-market.

[61] Ergün Varlık (2019), "Fransa Savunma ve Saldırı İçin Siber Politika Geliştiriyor", *Siber Bülten*, 11.05.2019, Erişim Tarihi: 04.11.2021, Erişim Adresi: https://siberbulten.com/uluslararasi-iliskiler/fransa-savunma-ve-saldiri-icin-siber-politika-gelistiriyor/.

3. Siber Güvenlik ve Savunma için Organizasyon

Siber güvenliği sağlamaya yönelik oluşturulan siber savunma faaliyetleri için temel parametreler incelendiğinde, Fransız organizasyon yapısı oldukça merkezi ve tutarlıdır. Çünkü Fransa'nın siber uzaya yönelik oluşturduğu siyasi yapısı sivil bir kuruluş olan ANSSI'ye odaklanmaktadır. ANSSI, Fransa Başbakanı tarafından denetlenmektedir. ANSSI, siber sorunların ekonomik, sosyal ve hükümetsel yönlerine odaklanmaktadır. Ayrıca internet ile ilgili işletmeler ve rekabetçi bir Fransız ekonomisini korumak için güvenli bir siber alanı teşvik etmektedir.

ANSSI'nin sivil odağına paralel olarak, Fransız Savunma Bakanlığı (MoD) ve İçişleri Bakanlığı (MOI) siber savunmadan sorumludur. Bu organizasyon yapıları kendi sistemlerini korumakta ve ağlarının bakımını sağlamaktadır. Bunu yaparken de, özellikle Savunma Bakanlığı analiz düzeyinde ANSSI ile iş birliği yapmaktadır.

Bu doğrultuda, Fransız siber güvenliğinin organizasyon yapısı, ANSSI etrafında merkezileştirilmiştir. Bu ajans, sorumlu devlet kurumlarına siber güvenlik konularında yardımcı olmaktadır. Ayrıca, endüstriler için siber güvenlik standartlarını düzenlemektedir. Buna ilave olarak, kritik altyapılar ve siviller için bilinçlendirme kampanyaları gerçekleştirmekte ve eğitimler düzenlemektedir.

3.1. Ulusal Bilgi Sistemleri Güvenlik Ajansı (ANSSI)

Bilgi, her zaman güvenlik ve savunma stratejilerinde önemli bir unsur olmuştur.[62] Fransa'nın bilgi güvenliği konusundaki çalışmaları, İkinci Dünya Savaşı'na kadar uzanmaktadır. 1943'te kurulan *Direction Technique du Chiffre* (DTC), savaş sırasında Fransız ulusal direnişi altındaki Fransız topraklarının kurtulması amacıyla Almanların şifreli iletişimini önlemeye çalışarak iletişiminin gizliliğini sağlamıştır. 1953 yılında, DTC, *Service Central Technique du Chiffre*-STC-CH'ye dönüşmüştür. Sonrasında 1977 yılında kurulan İletişim Güvenliği ve Parola Hizmetleri Merkezi (*Service Central du Chiffre et Sécuritédes Télécommunications*), 1986 yılında Bilgi Sistemleri Güvenliği Merkezi'ne (*Service Central de la Sécurité des Systèmes D'information*-SCSSI) dönüştürülmüştür. Merkez, daha sonra *Direction Centrale de la Sécurité des Systèmes* yani Bilgi Sistemleri Güvenlik Merkezi'ne (DCSSI) dönüştürülmüştür. Fransa'da

[62] Philippe Vitel & Henrik Bliddal (2015), "French Cyber Security and Defence: An Overvıew, Vitel and Bliddal", *Information and Security: An International Journal***,** Cilt 32, ss. 1-13, Erişim Tarihi: 29.10.2021, Erişim Adresi: https://connections-qj.org/system/files/3209_france.pdf.

bilgi güvenliği politikalarının uygulanmasını koordine etmek amacıyla, DCSSI, 2008'de ANSSI olmuştur.[63]

Bu tarihten sonraki süreçte Fransa'nın Ulusal Güvenlik ve Savunması hakkında "*Beyaz Kitap*" tarafından öneriler geliştirilmiştir. Böylece Fransa'nın siber ortamdaki savunma kapasitesinin arttırılmasına yönelik koordinasyon yapısı ANSSI olarak adlandırılmıştır. ANSSI'nin görevlerinden bazıları şunlardır:[64]

- Devlete yönelik gerçekleştirilecek siber saldırılara karşı Siber Güvenlik Operasyon Merkezi ile iş birliği içinde hareket etmek,
- Siber saldırılara karşı kamu kurumlarının ve elektronik kamu hizmetlerinin sunulduğu ağları hazır tutmak,
- Fransa'daki özel veya kamu tüm sektör kuruluşlarının bilgi güvenliği risklerini önlemek,
- Hükümetin bilgi güvenliği politikalarının askeri kurumlarla iş birliği ve uyum içinde uygulanmasını sağlamak
- Ağ ve ürün güvenliği alanına yönelik kamu kurumlarının ihtiyaç duyduğu güvenlik malzemelerini tedarik etmek veya geliştirmek.

Sonuç olarak, Fransa'nın siber alandaki ulusal stratejisi; siber güvenliği sağlamak ve bu alanda kararlı politikalar çizmek üzerine kurgulanmıştır. Ayrıca Fransa'nın siber güvenlik ve savunma yaklaşımında ANSSI aktif bir politika izlemektedir. ANSSI, Fransız siber savunmasının altı görevinin tamamında aktiftir. Bu görevler arasında siber tehditleri tespit, tahmin, önleme, tepki, koruma ve ilişkilendirme bulunmaktadır. Gerçekleştirilen bu aktif uygulamalar sırasında görevli aktörler arasında bazı çakışmalar yaşanmaktadır. Bu sebeple, istihbarat, adli soruşturmalar, koruma ve askeri harekat zincirleri olarak tanımlanan dört başlık altında sahadaki kamu eylemini merkezileştirmek ve düzene koymak için "*operasyonel zincir*" oluşturulmuştur. Oluşturulan bu düzen içerisinde biri Başbakan'a, diğeri Cumhurbaşkanı'na bağlı iki komite devlet politikalarını koordine etmektedir. Ayrıca, bir merkez, kriz zamanlarındaki eylemlerinin koordinasyonuna adanmıştır. Bu çerçevede, Fransa'nın önde gelen siber güvenlik ajansı siber ortamda istihbarat

[63] Özge Güleç & Zülfükar Aytaç Kişman (2021), "Uluslararası İlişkiler Açısından Siber Güvenlik ve NATO'nun Siber Güvenlik Stratejileri", *Akademik Açı*, Cilt 1, Sayı: 1, ss. 148-149.
[64] Murat Güngör (2015), "Ulusal Bilgi Güvenliği Strateji ve Kurumsal Yapılanma", Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı Uzmanlık Tezi, Ankara, ss. 85-87.

topluluğunun bir parçası değildir. Bu, siber strateji incelemesinin tanımlayıcı bir unsurudur ve Fransız siber savunmasının tüm yapısını beslemektedir. Bu durum, Fransız siber modelinin özelliğinin hem yerel siber sorunları, hem de uluslararası siber sorunları kapsamasına yol açmaktadır. [65]

3.2. Bilgi Sistemleri Güvenliği Operasyonel Merkezi (COSSI)

Bilgi Sistemleri Güvenliği Operasyonel Merkezi (COSSI), ANSSI'nin sorumlu birimidir. COSSI tarafından 7/24 siber tehditler izlenmekte, analiz edilmekte ve bu tehditlere yanıt verilmektedir. Ayrıca, mevcut sistemlerdeki güvenlik açıkları belirlenmekte ve devam eden saldırılar araştırılmaktadır.

COSSI, yetkilileri uyarmaktan sorumlu bir merkezdir. COSSI'nin merkezi Paris'tedir. COSSI, CERT International'ın bir parçası olan Bilgisayar Acil Müdahale Ekibi-Fransa'ya (CERT-FR) ev sahipliği yapmaktadır. Aynı zamanda, CERT-FR, siber tehditler ve güvenlik açıkları hakkında uluslararası bilgi alışverişine katkı sağlamaktadır. Görev alanı ve uzmanlığı nedeniyle, COSSI, Savunma Bakanlığı'ndaki muadili Savunma Analiz Merkezi ile yakın iş birliği içindedir.

3.3. Savunma Bakanlığı (MOD) ve İçişleri Bakanlığı (MOI ve MdA)

Fransız Siber Savunma Stratejisi, esas olarak sağlamlığı ve esnekliği geliştirerek savunma önlemlerine odaklanmaktadır. Savunma Bakanlığı (MoD) lider kuruluştur ve kendi bilgilerinin siber güvenliğinden sorumludur.

Fransız Savunma Bakanlığı, ANSSI ile paralel olarak çalışmakta ve sivil muadilleri ile iş birliği yapmaktadır. MoD, ayrıca siber saldırı için kendi altyapılarının korunmasından da sorumludur. Bu doğrultuda, MoD, Silahlı Kuvvetlerin savunma yetenekleri ve siber güvenlik ürünlerinin (hem donanım, hem de yazılım) gelişmesinde görevlidir.

İçişleri Bakanlığı İç Güvenlik Genel Müdürlüğü (*Ministre de l'Intérieur*-MOI) 30 Nisan 2014 kararnamesi ile oluşturulmuştur. Temeli 1907 yılında kurulan Genel İstihbarat Merkez Müdürlüğü ile 1944'te kurulan Toprak Gözetleme Müdürlüğü'nün 1 Temmuz 2008'deki

[65]Agence Nationale de la Sécurité des Systèmes D'information (ANSSI) (2021), "International Agreements", Erişim Tarihi: 04.11.2021, Erişim Adresi: https://www.ssi.gouv.fr/en/certification/common-criteria-certification/international-agreements/.

birleşmesine dayanmaktadır. Özellikle terörle mücadele alanında adli polis (SDAT ve SAT) ile siber suçlar alanında uzman polis ve jandarma teşkilatları ile birlikte hareket etmektedir.[66]

Bir diğer önemli kurum olan İçişleri Bakanlığı'nın Silahlı Kuvvetler (MdA) biriminin temeli siber savunmayı sağlamaktır. Bu amacı gerçekleştirmek için ComCyber olarak bilinen kendi komuta kademesini oluşturmuştur. Böylece, Fransa özelinde yeni bir doktrin ortaya konarak pasif savunmadan aktif taarruza geçilmiştir.

ComCyber, siber savunmanın stratejik bir konu ve öncelik olduğunu göstermiştir. Ayrıca ComCyber ile birlikte MdA ulusal egemenliğin garantörü konumuna gelmiştir. Bu amaç doğrultusunda, Silahlı Kuvvetler Bakanlığı, birçok aktörle birlikte siber uzayda bilgi sistemlerinin korunması ve savunulmasına aktif olarak katılmaktadır.

Son olarak, rekabet ve çatışmanın artık yalnızca geleneksel ortamlar, kara, deniz, hava ve uzay ile sınırlı olmadığını resmileştiren bu kurum, Fransa'nın ulusal güvenliğinin sağlanmasında önemli bir görev üstlenmektedir. Üstlenilen bu görevler çerçevesinde, Fransız siber savunmasının günlük eylemi birkaç alanda ifade edilmektedir. Bunlar; bilgi sistemleri güvenliği (ISS), güvenli durumda bakım (MCS), savunma bilgisayar savaşı (LID), saldırgan bilgisayar savaşıdır (LIO).[67]

3.4. Siber Komutanlık (ComCyber)

Savunma Bakanlığı bünyesindeki Savunma Kurmay Başkanı, Fransa'nın Siber Komutanlığı'nı (ComCyber) denetlemektedir. ComCyber'ın görevi; siber istihbarat, siber savunma ve siber suç operasyonlarını yasal çerçevede yürütmektir. Uluslararası silahlı çatışma yasaları ve Fransız ceza ve savunma yasalarına göre faaliyetlerini yürütmektedir. ComCyber, yaklaşık 2.600 askeri personelden oluşmaktadır. Oluşabilecek siber krizlere karşı personel sayısını arttırmayı hedeflemektedir. Fransız siber savunma birimleri Tuğgeneral tarafından kontrol edilmektedir.

ComCyber, siber savunmadaki sorumluluklarını ve hedeflerini gerçekleştirmek için 4 belirli kuruma görev vermiştir. Bu kurumlar:

[66] *A.g.e.*
[67] *A.g.e.*

- *Savunma Siber Operasyonları Analiz Merkezi* (CALID), Savunma Bakanlığı'nın operasyon merkezidir. COSSI ile yakın iş birliği içindedir. CALID'in rolü siber tehditleri tahmin etmek ve sürekli olarak izlemektir.

- *Silahlanma Genel Müdürlüğü'nün Bilgi İşlem Bölümü* (DGA MI), DGA'nın uzmanlık merkezidir. Elektronik harp, bilgi sistemleri, telekomünikasyon ve bilgi güvenliği konularında uzmandır. Ayrıca, DGA MI, bilgi teknolojilerinde tedarik, araştırma ve geliştirmeden sorumludur. Bruz'da yer almaktadır. DGA MI'nın bir dizi görevi vardır. Bunlar:[68]

1. Siber tehditler hakkında uzmanlık sağlamak ve bunları öngörmek,

2. Siber savunma için tavsiye ve destek sağlamak,

3. Siber güvenlik ürünleri geliştirmek ve değerlendirmek,

4. Her silahlanma programında siber güvenlik konularını değerlendirmek,

5. Devletin haberleşmesi için kriptolojik çözümler geliştirmek,

6. Siber konulardaki araştırma ve geliştirmeyi diğer Bakanlıklar, endüstriler ve akademi ile koordine etmektir.

- *807. İletim Şirketi*, denizaşırı operasyonlarda konuşlandırılabilen bir siber savunma birimidir. Şirketin rolü, siber tehditleri tespit etmek, bilgi sistemlerini korumak ve siber savunma müdahalesini gerçekleştirmektir.

- *Operasyonel Siber Savunma Rezervi* (OCR), siber savunma askeri uzmanlarına ve DGA MI'a yardımcı olmaktır. Temel görevi, büyük siber krizden sonra ağları ve bilgi sistemi altyapılarını yeniden inşa etmektir.

Tüm bu yardımcı kurumlar özelinde 2017'de Fransa tarafından ilan edilen "*Savunma ve Ulusal Güvenlik Revizyonu"* siber uzayı tanımlamış ve Siber Savunma Komutanlığı'nın kurulmasına önderlik etmiştir. Böylece, Kasım 2018'deki Paris Çağrısı'nda ofansif siber operasyonlara karşı Fransa'nın siber savaşla ilgili doktrini ortaya konulmuştur. Doktrinin ortaya konmasıyla birlikte, 2019 yılında Lille'de küresel ölçekte düzenlenen konferansta Fransa Savunma Bakanı Florence Parly, Fransa'ya yönelik gerçekleşen siber saldırılara karşılık vermek ve saldırıda bulunmak için

[68] Robert S. Dewar (2018), "CSS Cyber Defense Project, National Cybersecurity And Cyberdefense Policy Snapshots", ss. 7-24.

ülkesinin siber ordularını bütün diğer geleneksel silahlarla birlikte kullanacağını belirtti. Ayrıca, Parly, siber güvenlik tehditlerine ilişkin olarak Pan-Avrupa iş birliği çağrısında bulundu.

3.5. Fransız Siber Stratejisinin Fırsat ve Tehditlerini Anlamanın Anahtarları

21. yüzyılın uluslararası ilişkiler sahnesinde yaşanan güç mücadelesinde siber silahlar önemli bir konuma yükselmiştir. Siber silahların kullanımının artması, siber saldırıların ve dolayısıyla da siber savaşların artmasına sebep olmuştur. Bu kapsamda, siber ortamda ortaya çıkan siber savaş, mücadelenin ve rekabetin yaşandığı yeni bir satranç tahtası haline geldi. Bu sebeple, devletler giderek daha fazla siber savaşa hazırlanmakta ve siber silahlar geliştirmek için yatırım yapmaktadır. Fransa da askeri operasyonlarda yaygın olarak kullanılan siber yeteneklere en çok yatırım yapan Avrupa ülkelerinden biridir. Çünkü Fransa, uluslararası ilişkilerde aktif bir rol almak istemektedir. Bu amaç doğrultusunda da, Fransız Ordusu, ulusal güvenliği korumak için siber saldırı yeteneklerini kullanmanın önemini kabul etmiştir.[69]

Fransa Savunma Bakanı Florence Parly tarafından siber savunma ve siber saldırı operasyonlarına rehberlik edilmesi için strateji ve doktrin ilan edilmiştir. İlan edilen bu doktrin, Fransa'nın askeri alanda siber savunma ve siber saldırı yeteneklerini nasıl kullanacağına dair ilk açık yönergedir. Fakat "*Askeri Siber Savaş Doktrini için Kamu Unsurları*" başlıklı stratejik belgenin başarılı olarak uygulanabilmesi için bazı riskler ve zorluklar bulunmaktadır.

Siber saldırı yeteneklerinin kullanımına ilişkin doktrinel zorluklardan ilki, barış zamanlarında ve savaş zamanlarında saldırı araçlarının kullanımı arasındaki farktır. İkincisi, uluslararası kamu hukuku kapsamında ciddi hasara neden olan siber saldırı eyleminin saldırıya uğrayan ülkeye meşru müdafaa hakkı vermesidir. Fakat barış ve savaş zamanlarında kullanılan siber saldırıların orantılı ve ölçülü olması için uluslararası çaba gösterilmelidir. Son olarak, özellikle düşmandan bilgi elde etmeyi amaçlayan saldırgan siber saldırılara karşı Fransız hükümeti stratejik özerkliği korurken özel şirketlerin gelişimine güvenmelidir.

Bu bağlamda, Fransa'nın ilan ettiği saldırgan doktrin, siber silahların doğası düşünüldüğünde fırsat ve tehditleri bir arada sunmaktadır. Değişen ve dönüşen teknoloji sayesinde, geçmişte veya

[69] Beatriz de León Cobo (2020), "The Keys To Understanding French Cyber-Strategy And İts Risks", Atalayar, 22.10.2020, Erişim Tarihi: 30.10.2021, Erişim Adresi: https://atalayar.com/en/content/keys-understanding-french-cyber-strategy-and-its-risks.

günümüzde tasarlanmış ve tedarik edilmiş programlar, cihazlar ve uygulamalar sıfırdan güvenlik açıkları oluşturmaktadır.

Siber saldırılar ve uluslararası siber savaş kavramlarına yönelik Fransa'da gerçekleştirilen kurumsal düzeydeki gelişmeler siber güvenlik tehditlerine karşı farkındalığı arttırmaktadır. Bu bağlamda, Fransız siber güvenlik pazarı risk ve tehditleri içinde barındırmaktadır. Bu yüzden konu hakkında uzman kapasitesi oldukça ileri düzeydedir. Ayrıca, Fransa'da kritik noktalarda risk ve tehditlerin artmasıyla birlikte siber güvenlik ürünlerine olan talep her geçen gün artmaktadır. Artan bu talep, Fransa'nın milli güvenlik çözümlerine duyduğu ihtiyacı göstermektedir.

Özellikle bulut bilişim, nesnelerin interneti, mobil bilgisayar, sosyal medya ve yapay zekâ gibi alanlar siber saldırılar için bir tehdit unsuru olmuştur. Bu tehditlere yönelik önlem almak için Fransa'da siber silahların araştırılması ve geliştirilmesi süreci siber komutanlık tarafından ifade edilen operasyonel ihtiyaçlarla yakın iş birliği içindeki Savunma Tedarik Ajansı'nın (DGA) sorumluluğuna verilmiştir. Bu sorumluluk sayesinde, siber komutanlık, Fransa'nın güvenliğini sağlayabilmek için yetenekli bireyleri çekmeye çalışmakta ve bu alanda eğitimli bireyler yetiştirmeye çabalamaktadır. Ayrıca, geleceğin fabrikaları, endüstriyel sistemler, e-ödeme sektörü, nükleer yapılar, internetin kamu ve özel sektörde temel bir iletişim aracı kullanımı ve bağlı cihazların (akıllı telefonlar ve aynı zamanda otomobiller gibi çok sayıda başka nesne dahil) hızla artan kullanımı bu hedeflere yönelik siber saldırıları arttırdı. Bu doğrultuda dijitalleşen Fransa'da kayda değer oranda potansiyel tehdit olabilecek hedefler arttı.

Son olarak, asimetrik bir ortamda saldırı operasyonlarının hazırlanmasında ve yürütülmesinde risk dengeleme ilkesi belirlenmelidir. Özellikle sivil altyapılar üzerindeki ikincil hasar veya öngörülemeyen dolaylı etki riskine karşı dengeleme önemlidir. Bu doğrultuda liberalleşmiş siber uzaya sahip ABD ve İngiltere gibi ülkelerin aksine, Fransa'nın halka açık bir güvenlik açığı süreci yoktur.

Sonuç

ANSSI, Fransa'nın endüstriyel altyapısının siber güvenliğini güçlendirmek için pratik bir yaklaşım tanımlamakta ve bir dizi belge hazırlamaktadır. Böylece kısmen ANSSI'nin liderliğinin bir sonucu olarak, Fransa'da yaşanan siber saldırıların sayısı azalmaktadır.

Sayısı sürekli artan siber saldırılardan sonra, Fransa, siber güvenlik ve siber savunma söz konusu olduğunda kendisinin küresel rakiplerinin gerisinde kaldığını fark etti. Bu doğrultuda ulusal siber güvenlik ve siber savunma yeteneklerini artırmaya başladı. Avrupa Birliği ve NATO ile siber ortamda daha etkili uluslararası iş birliği ve koordinasyon sağlamaya yönelik çabaları da bu noktada arttı.

Fransa, siber politikaları, organizasyonu ve bütçesi açısından uzun bir yol kat etmiş olsa da, teşebbüs edilen ve başarılı olan siber saldırılarda artış devam etmektedir. Fransa'da kamu ve özel sektör genelinde yapılması gereken başta bütçenin arttırılması, kurumların yapılandırılması ve hukuki düzenlemelerin güncellenmesi gibi çok fazla şey bulunmaktadır.

Fransa, ilk olarak siber uzaya yönelik gerekli mali kaynakları tahsis etmezse, ulusal egemenliğinin onarılamaz biçimde sarsılacağını anladı. Bu sebeple, Fransa'nın siber savunmaya ayırdığı bütçe önemli derecede arttı. Fransa, son yıllarda taarruz odaklı siber güvenlik ve siber savunma modelini kavramsallaştırdı ve benimsedi. Yakın zamanda yayınlanan saldırgan doktrin, başta Silahlı Kuvvetler olmak üzere bu derin dönüşümün doruk noktasını oluşturdu. Fransa'nın saldırgan strateji belgesi ve Bakan Parly'nin açıklamaları, siber savaşta Rusya'nın bir düşman olarak görüldüğünün somut göstergesi oldu. Ayrıca geçmiş yıllarda Fransa'nın siber konularda Rusya'ya yönelik katı ifadeleri yoktu. Bu açıklamayla birlikte, Fransa, başta AB olmak üzere ABD'nin de içinde olduğu Batı blokunda olduğunu siber uzayda da gösterdi.

Sonuç olarak, Fransa, siber krizlerin tırmanmasını önlemek için siber alanda uluslararası kuralları ve istikrarı teşvik etmeyi amaçlamaktadır. Aynı zamanda Fransa'nın siber uzaydaki ulusal güvenliğini sağlamak için geleneksel operasyonları, caydırıcılığı ve geri dönüşü desteklemeye yönelik kendine manevra alanı oluşturmaya çalıştığı görülmektedir. Bu çerçevede, siber uzaydaki anarşik yapı içerisinde Fransa kendine güvenli bir hassas denge yaratmak istemektedir. Bu dengeyi oluştururken de birçok fırsat yakalarken, aynı zamanda da bir o kadar risk ve tehditle karşı karşıya kalmaktadır.

KAYNAKÇA

- Agence Nationale De La Sécurité Des Systèmes D'information (2021), "The National Cybersecurity Agency Of France", Erişim Tarihi: 07.11.2021, Erişim Adresi: https://www.ssi.gouv.fr/en/cybersecurity-in-france/the-national-cybersecurity-agency-of-france/.
- Agence Nationale De La Sécurité Des Systèmes D'information (2021), "International Agreements", Erişim Tarihi: 04.11.2021, Erişim Adresi: https://www.ssi.gouv.fr/en/certification/common-criteria-certification/international-agreements/.
- *Anadolu Ajansı* (2021), "5 Fransız Bakanın Telefonunda Casus Yazılım Pegasus'un İzi Bulundu", 24.09.2021, Erişim Tarihi: 04.11.2021, Erişim Adresi: https://www.gazeteduvar.com.tr/5-fransiz-bakanin-telefonunda-casus-yazilim-pegasusun-izi-bulundu-haber-1536117.
- Ardisson, Alexandra Valetta & Lachaud, Bastien (2018), "Filed In Application of Article 145 of the Rules, By the Commission for National Defense and the Armed Forces, In Conclusion of the Work of a Cyber Defense Information Mission", National Assembly, 04.07.2018, Erişim Tarihi: 29.10.2021, Erişim Adresi: http://www2.assemblee-nationale.fr/documents/notice/15/rap-info/i1141/#P439_94811.
- Baumard, Philippe (2017), *Cybersecurity in France*, Springer, ss. 56-65.
- Bliddal, Henrik & Vitel, Philippe (2015), "French Cyber Security and Defence: An Overview, Vitel and Bliddal", *Information and Security: An International Journal*, Cilt 32, ss.1-13, Erişim Tarihi: 29.10.2021, Erişim Adresi: https://connections-qj.org/system/files/3209_france.pdf.
- Bockel, Jean-Marie (2012), "Report on behalf of the Foreign Affairs, Defense and Armed Forces Committee", Erişim Tarihi: 02.11.2021, Erişim Adresi: https://www.senat.fr/rap/r11-681/r11-681.html.
- Cerulus, Laurens (2021), "France Wants Cyber Rule To Curb US Access To EU Data", *Politico*, 13.10.2021, Erişim Tarihi: 31.10.2021, Erişim Adresi: https://www.politico.eu/article/france-wants-cyber-rules-to-stop-us-data-access-in-europe/.
- ComCyber (2021), "GDA Tisseyre: On Est 3400 Cybercombattants et on Deviendra 4500 en 2025"', @ComcyberFR on Twitter, 12.10.2019, Erişim Tarihi: 04.11.2021, Erişim Adresi: https://twitter.com/ComcyberFR/status/1172186486134968322.
- De León Cobo, Beatriz (2020), "The Keys To Understanding French Cyber-Strategy And Its Risks", Atalayar, 22.10.2020, Erişim Tarihi: 30.10.2021, Erişim Adresi: https://atalayar.com/en/content/keys-understanding-french-cyber-strategy-and-its-risks.
- Delerue, François & Desforges, Alix & Géry, Aude (2019), "A Close Look at France's New Military Cyber Strategy", War On The Rocks, 23.04.2019, Erişim

Tarihi: 31.10.2021, Erişim Adresi: https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/.

- Dewar, Robert S. (2018), "CSS Cyber Defense Project, National Cybersecurity And Cyberdefense Policy Snapshots", Erişim Tarihi: 23.01.2022, Erişim Adresi: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports_National_Cybersecurity_and_Cyberdefense_Policy_Snapshots_Collection_1.pdf, ss. 7-24.
- Defense Intelligence and Security Directorate, Erişim Tarihi: 04.11.2021, Erişim Adresi: https://www.dgse.gouv.fr/en.
- Defense And Security Of Information Systems: France's Strategy (2011), National Information Systems Security Agency, Erişim Tarihi: 04.11.2021, Erişim Adresi: https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf.
- Digital National Council, Erişim Tarihi: 02.11.2021, Erişim Adresi: https://cnnumerique.fr/.
- Directorate General of Armaments, Erişim Tarihi: 29.10.2021, Erişim Adresi: https://www.defense.gouv.fr/dga.
- Direction du Renseignement et de la Sécurité de la Défense Erişim Tarihi: 04.11.2021, Erişim Adresi: https://www.drsd.defense.gouv.fr/.
- Directorate of Military Intelligence, Erişim Tarihi: 04.11.2021, Erişim Adresi: https://www.defense.gouv.fr/drm.
- *Diriliş Postası* (2017), "Fransa'da Cumhurbaşkanlığı Seçimlerinde 'Siber Saldırı' Uyarısı", 08.01.2017, Erişim Tarihi: 04.11.2021, Erişim Adresi: https://www.dirilispostasi.com/haber/6292216/fransada-cumhurbaskanligi-secimlerinde-siber-saldiri-uyarisi.
- Éléments Publics De Doctrine Militaire De Lutte İnformatique Offensive Report (2019), Ministry of the Armed Forces, Erişim Tarihi: 03.11.2021, Erişim Adresi: https://www.defense.gouv.fr/fre/content/download/551497/9393997/El%C3%A9ments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdf.
- Federal Office for Information Security (Germany) ve National Information Systems Security Agency (2020), "Third edition of the Franco-German common situational picture", Erişim Tarihi: 03.11.2021, ErişimAdresi: https://www.ssi.gouv.fr/uploads/2020/12/anssi-bsi-common_situational_picture_2020.pdf, ss. 1-20.
- Franchi, Charles De & Joly, Christophe (2016), "Cyber Security Opportunities in France", International Trade Administration, Erişim Tarihi: 29.10.2021, Erişim Adresi: https://2016.export.gov/france/build/groups/public/@eg_fr/documents/webcontent/eg_fr_110164.pdf.

- French Republic Prime Minister, "French National Digital Security Strategy", Erişim Tarihi: 04.11.2021, Erişim Adresi: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf, ss. 1-44.
- French Ministry for Europe and Foreign Affairs (2019), "France Diplomacy Digital Diplomacy", 18.09.2019, Erişim Tarihi: 30.10.2021, Erişim Adresi: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/.
- General Directorate of Internal Security, Erişim Tarihi: 04.11.2021, Erişim Adresi: https://www.interieur.gouv.fr/Le-ministere/DGSI.
- Governing National Law, Decree 2009-834 of 7 July 2009, establishment of a service with national competence called "National Agency for the Security of Information Systems", Erişim Tarihi: 01.11.2021, Erişim Adresi: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000020828212/.
- Güleç, Özge & Kişman, Zülfükar Aytaç (2021), "Uluslararası İlişkiler Açısından Siber Güvenlik ve NATO'nun Siber Güvenlik Stratejileri", *Akademik Açı,* Cilt 1, Sayı: 1, ss. 127-154.
- Güngör, Murat (2015), "Ulusal Bilgi Güvenliği Strateji ve Kurumsal Yapılanma", Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı Uzmanlık Tezi, Ankara.
- Hiscox (2020), "Hiscox Cyber Readiness Report 2020", ss.1-16.
- Intelligence Online (2018), "The DGA Develops Cyber Warfare Games In Bruz", 04.07.2018, Erişim Tarihi: 29.10.2021, Erişim Adresi: https://www.intelligenceonline.fr/renseignement-d-etat/2015/03/11/la-dgadeveloppe-les-jeux-de-cyberguerre-a-bruz,108065256-bre.
- Karaca, Kayhan (2015), "Fransa Siber-Cihatçıların Da Hedefinde", *Deutsche Welle Türkçe*, 15.01.2015, Erişim Tarihi: 04.11.2021, Erişim Adresi: https://p.dw.com/p/1EKx5.
- Laudrain, Arthur (2018), "Avoiding A World War Web: The Paris Call for Trust and Security in Cyberspace", Lawfare, 04.12.2018, Erişim Tarihi: 03.11.2021, Erişim Adresi: https://www.lawfareblog.com/avoiding-world-war-webparis-call-trust-and-security-cyberspace.
- Laudrain, Arthur P.B. (2019),"France's New Offensive Cyber Doctrine", Lawfare, 26.02.2019, Erişim Tarihi: 29.10.2021, Erişim Adresi: https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine.
- Maglana, Lorie & Man, Sunny (2020), "Europe: EU Imposes The First Ever Sanctions Against Cyber-Attacks", *Global Compliance News*, 21.08.2020, Erişim Tarihi: 03.11.2021, Erişim Adresi: https://www.globalcompliancenews.com/2020/08/21/eu-imposes-the-first-ever-sanctions-against-cyber-attacks-20200810/.
- Mackenzie, Christina (2019), "French Defense Chief Touts Offensive Tack In New Cyber Strategy", Fifth Domain, 18.01.2019, Erişim Tarihi: 29.10.2021, Erişim

Adresi: https://www.fifthdomain.com/global/europe/2019/01/18/french-defense-chief-touts-offensive-tack-in-new-cyber-strategy/.

- Ministry of the Armed Forces, "The Cyber Defense Command (COMCYBER)", Erişim Tarihi: 03.11.2021, Erişim Adresi: https://www.defense.gouv.fr/ema/organismesinterarmees/le-comcyber/le-comcyber/comcyber.
- Ministry of the Armed Forces (2019), "Ministerial policy of defensive IT control", Erişim Tarihi: 04.11.2021, Erişim Adresi: https://www.defense.gouv.fr/salle-de-presse/communiques/communique_la-france-se-dote-d-une-doctrine-militaire-offensive-dans-le-cyberespace-et-renforce-sa-politique-de-lutte-informatique-defensive.
- Ministry of Europe And Foreign Affairs (2019), "France Diplomacy", Erişim Tarihi: 31.10.2021, Erişim Adresi: https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/fight-against-organized-criminality/cyber-security/.
- Ministry of the Armed Forces (2013), "White Paper: Defense and National Security Report", Erişim Tarihi: 29.10.2021, Erişim Adresi: http://www.livreblancdefenseetsecurite.gouv.fr/index.html.
- Ministry of Europe and Foreign Affairs (2017), "France's International Digital Strategy", 15.12.2017, Erişim Tarihi: 03.11.2021, Erişim Adresi: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-s-international-digital-strategy/#:~:text=France's%20international%20digital%20strategy%2C%20presented,governance%2C%20the%20economy%20and%20security.
- Ministry of Europe and Foreign Affairs (2019) "Indo-French Bilateral Cyber Dialogue", 20.06.2019, Erişim Tarihi: 03.11.2021, Erişim Adresi: https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/fight-against-organized-criminality/cyber-security/article/indo-french-bilateral-cyber-dialogue-20-06-19.
- Ministry of Europe and Foreign Affairs (2019), "G7 French presidency – Cyber Norm Initiative: Synthesis of Lessons Learned and Best Practices", 26.11.2019, Erişim Tarihi: 03.11.2021, Erişim Adresi: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/g7-french-presidency-cyber-norm-initiative-synthesis-of-lessons-learned-and.
- Ministry of Europe and Foreign Affairs, "Guaranteeing Cybersecurity", Erişim Tarihi: 03.11.2021, Erişim Adresi: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-s-international-digital-strategy/article/guaranteeing-cybersecurity.
- Ministry of Europe and Foreign Affairs (2020), "EU – Cyberattacks – Q&A from the press briefing", 30.07.2020, Erişim Tarihi: 03.11.2021, Erişim Adresi: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/eu-cyberattacks-q-a-from-the-press-briefing-30-jul-20.

- Mordorintelligence, "Fransa Siber Güvenlik Pazari - Büyüme, Eğilimler, Covid-19 Etkisi ve Tahminler (2022 - 2027)" Erişim Tarihi: 29.10.2021, Erişim Adresi: https://www.mordorintelligence.com/industry-reports/france-cybersecurity-market.
- National Assembly Session Service Division Of Laws (2015), "Initial project of the Law", 16.04.2015, Erişim Tarihi: 30.10.2021, Erişim Adresi: http://www.assemblee-nationale.fr/14/ta-pdf/2697-p.pdf, ss. 1-45.
- NCSI, Erişim Tarihi: 29.10.2021, Erişim Adresi: https://ncsi.ega.ee/country/fr/.
- NIS Investments Report (2020), "European Union Agency for Cybersecurity", Erişim Tarihi: 28.10.2021, Erişim Adresi: https://www.enisa.europa.eu/publications/nis-investments/at_download/fullReport.
- Parly, Florence (2018), "Statement by Ms Florence Parly, Minister of the Armed Forces, on the manipulation of information", 04.10.2018, Erişim Tarihi: 03.11.2021, Erişim Adresi: https://www.vie-publique.fr/discours/206652-declaration-de-mme-florence-parly-ministre-des-armees-sur-la-manipulat.
- Press center of the Ministry of the Armed Forces (2019), "Public Elements Of Military Doctrine For Offensive Computer Warfare", 21.01.2019, Erişim Tarihi: 04.11.2021, Erişim Adresi: https://www.defense.gouv.fr/salle-de-presse/dossiers-de-presse/dossier-de-presse_elements-publics-de-doctrine-militaire-de-lutte-informatique-offensive.
- Souyris, Jean Philippe (2021), "France: Cybersecurity Comparative Guide", Montaq, 16.04.2021, Erişim Tarihi: 03.11.2021, ErişimAdresi: https://www.mondaq.com/france/technology/963020/cybersecurity-comparative-guide.
- Tannam, Ellen (2019), "Defence Secretary Says France Will Take An Offensive Cybersecurity Strategy", Silicon Republic, 23.01.2019, Erişim Tarihi: 03.11.2021, Erişim Adresi: https://www.siliconrepublic.com/enterprise/france-cybersecurity-parly.
- The French Ministry of the Armies (2019), "International Law Applied To Operations In Cyberspace", ss. 1-20.
- The French Ministry for Europe and Foreign Affairs (2020), "EU Cyberattacks-Q&A From The Press Briefing", 30.07.2020, Erişim Tarihi: 04.11.2021, Erişim Adresi: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/eu-cyberattacks-q-a-from-the-press-briefing-30-jul-20.
- The International Institute for Strategic Studies (2019), "Cyber Capabilities and National Power: A Net Assessment", Erişim Tarihi: 29.10.2021, Erişim Adresi: https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power, ss. 57-69.
- Wavestone (2020), "Top Companies Cybersecurity Index: 2020 Annual Reports", Erişim Tarihi: 28.10.2021, Erişim Adresi: https://www.wavestone.com/app/uploads/2020/07/Wavestone-Cyberindex-top-companies-2020-EN.pdf.

- UN Office for Disarmament Affairs, "Developments In The Field Of Information And Telecommunications In The Context Of International Security", Erişim Tarihi: 03.11.2021, Erişim Adresi: https://www.un.org/disarmament/ict-security.
- Varlık, Ergün (2019), "Fransa Savunma ve Saldırı İçin Siber Politika Geliştiriyor", Siber Bülten, 11.05.2019, Erişim Tarihi: 04.11.2021, Erişim Adresi: https://siberbulten.com/uluslararasi-iliskiler/fransa-savunma-ve-saldiri-icin-siber-politika-gelistiriyor/.
- Voo, Julia & Hemani, Irfan (2020), "National Cyber Power Index 2020 Methodology and Analytical Considerations Report", Harvard Kennedy School Belfer Center for Science and International Affairs, Erişim Tarihi: 29.10.2021, Erişim Adresi: https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf.