Üçüncü Sektör Sosyal Ekonomi Dergisi
Third Sector Social Economic Review
61(2) 2026, 2200-2216
doi: 10.63556/tisej.2026.1799

Derleme Makale

Dijital Yönetimlerin Siber Güvenlik Stratejileri: AB ve Finlandiya İncelemesi

Cybersecurity Strategies of Digital Administrations: A Review of The EU and Finland

Elif EKİNCİ ÖZYARDIMCI
Dr. Öğr. Üyesi, Erzincan Binali Yıldırım Üniversitesi
İktisadi ve İdari Bilimler Fakültesi
eekinci@erzincan.edu.tr
https://orcid.org/0000-0002-5067-5685

Makale Geliş Tarihi	Makale Kabul Tarihi
12.01.2026	**24.05.2026**

Öz

Bu çalışma, dijital dönüşüm süreciyle birlikte karmaşıklaşan siber tehditlerin kamu yönetimi ve politika yapım süreçleri üzerindeki etkilerini Avrupa Birliği (AB) ve Finlandiya örnekleri üzerinden incelemektedir. AB, siber güvenlik alanında normatif bir liderlik hedefiyle hareket etmekte; yasal düzenlemeler, kurumsal koordinasyon ve dayanıklılık politikalarıyla, bütünleşik bir güvenlik kültürü oluşturmaya çalışmaktadır. NIS2 Direktifi, Siber Dayanıklılık Yasası, Dijital Hizmetler Yasası, Genel Veri Koruma Tüzüğü (GDPR) ve Yapay Zekâ Yasası, birliğin dijital güvenliği kapsamlı bir normatif çerçeveye oturtma girişimlerinin temelini oluşturmaktadır. Ancak üye devletler arasındaki uygulama farklılıkları, AB düzeyinde siber güvenlik stratejilerinin etkinliğini ve sürdürülebilirliğini sınırlandırmaktadır. Finlandiya ise 2024–2035 Ulusal Siber Güvenlik Stratejisi kapsamında katılımcı yönetişim, kamu–özel iş birliği, kriptografi, yapay zekâ uygulamaları ve ulusal izleme mekanizmalarını bütünleştirerek operasyonel düzeyde güçlü bir model ortaya koymuştur. Ülkenin stratejisi, siber güvenliği yalnızca teknik bir savunma aracı olarak değil, ekonomik kalkınma, demokratik yönetişim ve ulusal egemenliğin dijital boyutu olarak ele almaktadır. Çalışma sonucunda, sürdürülebilir siber güvenliğin sadece teknolojik kapasiteyle değil, aynı zamanda kurumsal dayanıklılık, uluslararası iş birliği, insan kaynağının niteliği ve toplumsal farkındalık düzeyine bağlı olduğu kanısına varılmıştır. AB'nin normatif düzenleme kapasitesi ile Finlandiya'nın uygulama disiplini birlikte değerlendirildiğinde, Avrupa'nın bütüncül ve dirençli bir dijital güvenlik ekosistemi oluşturma potansiyeli giderek güçlenmektedir.

Anahtar Kelimeler: Siber güvenlik stratejisi, avrupa birliği, finlandiya, kamu yönetimi, dijital yönetim.

Abstract

This study examines the impact of increasingly complex cyber threats on public administration and policy-making processes through the cases of the European Union (EU) and Finland. The EU pursues normative leadership in cybersecurity by promoting integrated governance through legislation, institutional coordination, and resilience policies. The NIS2 Directive, the Cyber Resilience Act, the Digital Services Act, the General Data Protection Regulation (GDPR), and the Artificial Intelligence Act collectively form the normative foundation of the Union's comprehensive digital security framework. However, implementation disparities among member states continue to limit the overall effectiveness and sustainability of these strategies. Finland's 2024–2035 National Cybersecurity Strategy, on the other hand, represents an operationally robust model that integrates participatory governance, public–private cooperation, cryptography, artificial intelligence applications, and national monitoring

Önerilen Atıf /Suggested Citation

Ekinci Özyardımcı, E., 2026, Dijital Yönetimlerin Siber Güvenlik Stratejileri: AB ve Finlandiya İncelemesi, *Üçüncü Sektör Sosyal Ekonomi Dergisi,* 61(2), 2200-2216.

mechanisms. Finland conceptualizes cybersecurity not merely as a technical defense tool but as an integral component of economic development, democratic governance, and the digital dimension of national sovereignty. The findings indicate that sustainable cybersecurity depends not only on technological capacity but also on institutional resilience, international cooperation, skilled human resources, and societal awareness. When the EU and Finland are considered together, Europe's potential to create a holistic and resilient digital security ecosystem is increasingly strengthened.

Keywords: Cyber security strategy, european union, finland, public administration, digital administration.

1. Giriş

Bilişim ve iletişim teknolojilerindeki akıl almaz gelişmeler, özellikle son yıllarda gittikçe genişleyerek pek çok alanın alt yapısını temelinden değiştirmiştir. Bu gelişmelere paralel olarak ciddi güvenlik sorunları da ortaya çıkmıştır. Siber güvenlik, bilgi sistemlerinin korunması ve güvenliklerinin sağlanması hususunda; peç çok uzmanın, mühendisin, araştırmacının ve yöneticilerin odak noktası haline gelen ve geleceğe dair endişe yaratan önemli bir konudur. Dijitalleşmenin yaygın hale gelmesiyle birlikte, teknolojinin hızlı gelişimi, siber tehditlerin daha da karmaşık hale gelmesi ve zorunlu yasal düzenlemelerin gerekliliği, kamu yönetiminin son yıllarda siber güvenlik alanındaki çalışmalarını daha da önemli kılmıştır (Michael vd., 2025, s.3).

Daha güvenli bir internet ortamı oluşturmak ve bilişim sistemlerinin güvenliğini sağlamak, günümüzün en önemli güvenlik sorunlarından biri haline gelmiştir. İnternetin, insan hayatının her alanına nüfuz etmesi, güvenilir çevrimiçi platformların oluşturulmasında; bireyler, toplumlar, kurumlar, devletler ve uluslararası kuruluşlara önemli misyonlar yüklemiş ve "internet güvenliği" tüm paydaşları daha büyük önlemler almaya sevk etmiştir. Siber güvenlik; hükümet politikalarıyla, kamu hizmetleriyle, bilişim ve iletişim teknolojileriyle kenetlenmiş bir kavram olmuştur.

Yönetimlerin bilgi ve iletişim teknoloji araçlarına yönelik yaptıkları yatırımlar, son yıllarda önemi daha da artan siber güvenlik stratejileri ve politikalarının geliştirilmesi açısından önem arz etmektedir. Dijital ortamda sunulan kamu hizmetlerine ve kişisel verilere yönelik siber saldırılardan korunmak ve siber güvenliğin sağlanması; kamu yönetimlerin en temel politikalarından biri haline gelmiştir (Riberio vd., 2025, s. 2). Günümüzde bilgi ve iletişim teknolojilerinin benimsenerek kalkınma politikalarının gerçekleştirilmesi, ulusal ve küresel arenada hükümetlerin ve uluslararası kuruluşların en temel hedefidir. Yerel, ulusal ve global alanda teknolojik rekabetin artması, dijital yönetimlerin karmaşık birçok unsurla mücadelesini beraberinde getirmiştir (Igboauna vd., 2025, s. 1-2).

Dijital yönetimler siber güvenliği sağlama hususunda önemli bir yol kat etmiş olsalar da gelinen noktada halen güvenlik açıkları ve yasal boşluklar bulunmaktadır (Riberio vd., 2025, s. 2). Dijital platformların büyük bir kısmı, güncellenmemiş protokollere sahip olmaları ve fark edemedikleri güvenlik açıklarından dolayı, siber saldırılara karşı mücadele edemeyecek durumdadır. Bu tespitlerden yola çıkarak, dijital platformlar, siber güvenlik politikalarını yeniden gözden geçirmeli ve güncellemeli, proaktif güvenlik yaklaşımıyla hareket etmeli, bu platformların güvenlik alt yapılarının geliştirilmesine yönelik olarak, dijital hükümetler gerekli çalışmaları yaparak, önemli yazılım şirketleri ve işin uzmanlarıyla birlikte koordineli bir şekilde faaliyetlerini gerçekleştirmeleri gerekmektedir (Riberio vd., 2025, s. 2).

En üst düzey güvenlik standartları; bilgilerin korunması, güvenilir internet portalları, yüksek korumalı internet, verilerin gizliliği ve siber güvenlik tedbirleriyle mümkündür. Siber güvenliğin gerçekleştirilmesi ile siber tehditlerden ve saldırılardan üst düzeyde koruma elde edilebilmektedir. Bilgi güvenliğinin sağlanması, siber güvenliğin en temel konularından biridir (Saltzer ve Schroeder, 1975, s.1280).

Hem ulusal hem de uluslararası alanda dijital araçlarla birlikte gelişmenin gerçekleştirilmesi, yeniliklere açık bir toplumun inşasını zorunlu kılmıştır (Balay, 2004). Kurumsal ve kişisel verilerin saklanması, bilginin güvenliğinin sağlanıp siber tehditlere karşı korunması, bilgi ve iletişim teknolojileri araçlarının hayatın her alanında uygulanmasının bir sonucu olarak ortaya çıkmış ve önemli bir amaç haline gelmiştir (Aldemir ve Kaya, 2020, s. 7).

Bu çalışmada siber güvenlik tanımından bahsedilerek; Finlandiya ve Avrupa Birliği'nin siber güvenlik stratejilerine değinilecektir. Siber güvenliğin sağlanmasına ilişkin oluşturulan stratejilerin ulusal ve

küresel düzeyde ne kadar etkili oldukları, birbirlerini ne ölçüde etkiledikleri ve Finlandiya'nın siber güvenlik alanında, birlik içindeki diğer ülkeler arasındaki lider konumunun, AB'nin bu alandaki konumunu ne ölçüde etkilediği, sonuç bölümünde değerlendirilecektir. Çalışmanın metodunu; AB ve Finlandiya'nın geçmişten günümüze yayımladığı ve en son yürürlükte olan siber güvenlik stratejileri, çıkarılan yasalar, AB'nin ve Finlandiya'nın mevcut politika ve stratejilerine ilişkin bir takım yazarların görüşlerden oluşan çok geniş bir yelpazeye dayalı olan literatür, arşiv ve belge taramasına dayalı nitel araştırma yöntemi oluşturmaktadır. Ayrıca "AB Siber Güvenlik Stratejisi" ile "Finlandiya Siber Güvenlik Stratejisi" detaylı incelenerek karşılaştırma yapılmıştır. Bu bağlamda Finlandiya ve AB'ye ait resmi strateji belgeleri, AB'nin çıkardığı NIS2 (İkinci Ağ ve Bilgi Güvenliği Direktifi), Dijital Hizmetler Yasası (DSA), Siber Dayanıklılık Yasası, Avrupa Birliği Yapay Zekâ Yasası, Genel Veri Koruma Yönetmeliği (GDPR), Finlandiya'nın "Finlandiya Ulusal Siber Güvenlik Stratejisi ve Uygulama Planı", "Finlandiya Ulusal Yapay Zeka Stratejisi" çalışma içerisinde ayrıntılı incelenen önemli belgelerdir. Bu çalışma iki temel soru etrafında şekillenmiştir. Birincisi; Finlandiya'nın bilgi ve iletişim teknolojilerini kullanmadaki güçlü rolü ve siber güvenlik alanına ilişkin yapmış olduğu önemli çalışma ve stratejileri; AB'nin siber güvenlik politikalarını ne ölçüde etkilemiştir ve AB siber güvenlik politikalarına ne gibi avantajlar sağlamıştır? Çalışmanın diğer ulaşmak istediği sonuç ve ikinci temel sorusu ise; Finlandiya'nın siber güvenlik vizyonunun AB'ye yansıması, AB'nin siber güvenlik alanında hedefleği en güçlü versiyonuna ulaştıracak mı? Siber güvenlik stratejilerinin birbirlerini etkileme ve geliştirme bağlamında Finlandiya-AB ilişkisinin bu çalışmada birlikte ele alınarak incelenmesi ve sonuç bölümünde karşılaştırmalı bir analiz yapılarak önerilerde bulunulması, literatüre önemli bir katkı sağlayacaktır.

2. Siber Güvenlik ve Siber Güvenlikle Bağlantılı Kavramlar

Siber güvenliğin tanımını yapmadan önce "siber"in sözcük anlamından; siber ortam, siber uzay, siber suç, siber terörizm, siber savaş gibi siber güvenlikle bağlantılı kavramlardan bahsetmek yerinde olacaktır. Siber kelimesi, "Cybernetics" den türemiştir. "Cyber" kelimesi dilimizde "siber" olarak kullanılmaktadır. İlk olarak 1948 yılında Amerikalı bir bilim insanı Norbert Weiner tarafından kullanılan sibernetik kavramı; hayvanlarla ve makinelerle iletişim kurma ve onlara hükmedebilme bilimi olarak adlandırılmıştır (Çakmak ve Demir, 2009). "Siber" kavramı yerine "bilişim" kavramı da sık sık tercih edilmektedir (Sayedi, 2020, s. 7). Fakat "bilişim" kavramı "siber" kelimesininde ilerisinde, daha geniş bir anlam ihtiva etmektedir. Yani siber kelimesi, bilişim sistemleri alanını; bilişim ise, elektronik ve bilişim sistemlerinden en iyi derecede faydalanma ve bu alan vasıtasıyla bilginin işlenmesi manasına gelmektedir (Sandilaç, 2022, s. 156).

Siber uzay kavramı ise ilk kez 1980'li yıllarda bilim kurgu yazarı William Gibson tarafından kullanılmıştır. T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı tarafından bu kavram şu şekilde açıklanmıştır: "Siber Uzay, uzayda ve dünyada gittikçe genişleyen bilişim sistemleri ile bu sistemleri birbirine kenetleyen ağlardan meydana gelen bağımsız bilgi platformlarıdır" (T.C. UHDB, 2016). Siber uzay; uzay da dâhil olmak üzere; kara, hava ve deniz yoluyla haberleşme kanallarına gerek duyulmadan, haberleşme imkânlarını kullanabilen "sanal bir ortam" olarak adlandırılmaktadır. Siber uzayı, gerçek ve fiziksel dünyadaki insanlar, varlıklar ve donanımlar oluşturmaktadır. Fiziksel dünya ile kurulan bağlar ve iyi iletişim, ileri teknoloji sayesinde oluşacaktır. Yalnız siber uzayın varlığı, sadece teknoloji ile değil aynı zamanda ülkelerin teknolojik ve internet alt yapılarının yeterli ve güçlü olmasıyla da ilgilidir (Sayedi, 2020, s. 8). Siber uzayı, fiziksel varlığından sanal dünyaya bağlayan kısım olan kodlar katmanında, fiziksel tüm varlıklar (anakart, RAM'lar, işlemciler gibi), kodlar vasıtasıyla ele alınmaktadır. Siber olay; endüstriyel ve bilişim sistemlerindeki verilere erişim yasağının kırılması, gizlilik ihlalinin yaşanması durumudur. Elektrik kesintileri, doğal afetler gibi fiber optik hatlarda meydana gelen düzensizlikler ve bozukluklar, siber olaya örnek verilebilir (Sayedi, 2020, ss. 9-10).

Siber Suç kavramından bahsedecek olursak öncelikle şu bilgiye değinmekte fayda vardır. 1960'lı yıllarda Amerika' da siber suçların patlak vermesiyle birlikte "bilgisayar suçu" kavramı daha yaygın bir biçimde kullanılmıştır. Ülkelerin bilişim ve iletişim teknolojilerinin kullanımı ve alt yapısı birbirinden farklı olduğu için, genel bir tanımı henüz mevcut değildir. Günümüzde "bilişim suçu" kavramı, ülkelerin mevzuatları içerisine yerleşmiştir (Akarslan, 2012, s. 33). Teknolojinin ilerlemesi ile birlikte bilişim sistemlerine ilişkin suçlarda git gide artış gözlemlenmiştir. Siber suç; bilişim sistemlerinin gizliliği çerçevesinde korunan verilere veya bilişim sistemi kullanıcısına yönelik suçlardır. En önemli

özelliği ise bilişim sistemi vasıtasıyla bu suçun işleniyor olmasıdır. Bilişim sistemlerine yönelik her suç, siber suç niteliği taşımayacağından, özellikle bilişim sistemlerine illegal şekilde izinsiz ve kötü amaçlar için erişilmesi, hukuka aykırılık teşkil etmesi bakımından bilişim suçu olarak adlandırılmktadır. Bilişim suçlarında hedef, bilişim sisteminin kullanıcısı, bilişim sisteminin kendisi ya da sistem içerisinde ulaşılmak istenen veriler olabilmektedir (EGM, 2025). Bilişim suçu, geleneksel ceza hukuku terimleri ile açıklaması zor olan yeni kriminolojik bir kavramdır. Bilişim alanında artan suçlar ve hak ihlalleri sebebiyle, ülkeler mevzuatlarında bilişim suçları adı altında çeşitli düzenlemeler yapmak zorunda kalmışlardır.

Siber savaşın en kısa ve en temel tanımı şu şekildedir: "Siber dünyada meydana gelen iyi ya da kötü her türlü misillemedir". Bir ülkenin kendi güvenliğini sağlamak ve çıkarlarını korumak amacıyla, karşı ülkenin bilişim sistemlerini durdurmak ya da yok etmek istemesi veyahut zarar vermesi olarak açıklanabilir (Sağıroğlu-Alkan, 2018, ss. 21-42). Siber savaşı, klasik savaşlardan ayıran en önemli farklar şunlardır; (Cornish vd. 2010, s. 1);

- Topla tüfekle değil, stratejiyle hareket edilmesi,
- Savaşın, kara, hava, deniz ve uzayda değil de, daha önce de tanımı yapılan siber uzayda gerçekleşiyor olması,
- Fiziksel baskı ve çatışmadan ayrı olarak yapılması,
- Küçük aktörlere orantısız güç sağlanmasıdır.

Siber suçlarla mücadelede daha titiz olunması ve daha kapsamlı bir yaklaşım sergilenmesi günümüzde son derece önemlidir. Yalnızca teknik açıdan önlem alınması, siber suçlarla mücadelede yeterli değildir. Kolluk personelinin de siber suçlarla ilgili olayları etkili ve doğru bir şekilde soruşturmaları ve kovuşturmaları gerekmektedir. Az gelişmiş ülkelerden gelişmiş ülkelere kadar hemen hemen bütün ülkeler, siber suçlarla mücadelenin ciddiyetinin farkına vararak; daha kapsamlı politikalarla ve keskin yasalarla hareket etmektedirler (Admass vd., 2024, s.1-2).

Bu bahsedilen kavramların bir kısmı özellikle de siber güvenlik kavramı, siber alanda güvenlik tehditlerinin tezahür etmesiyle türemiş bir kavramdır. İnternetin yaygın hale gelmesiyle birlikte siber ortamda gizli tutulan bilgiye erişme eğilimi, siber güvenliği tehdit eden en önemli unsur olmuştur. Kişisel ya da kamusal alanda bilgisayarlar ya da mobil telefonlara gelen sahte e-mailler, reklamlar ve bilgisayara rahatça indirilen ücretsiz bazı programlar, tehdit içerikli olup; bilgisayar içinde saklı olan her türlü verinin üçüncü kişiler tarafından ele geçirilmesine sebebiyet vermektedir (Tunca, 2019, s.3).

Siber güvenlik; kamu kurumları ve özel sektör kuruluşlarında; askeri güvenlikte; akademik camiada; sağlık, eğitim, enerji, iletişim ve ulaşım alanlarında kişisel bilgilerin korunması ve güvenliklerinin sağlanmasında; gizli bilgilerin ele geçirilmesini önlemede, kurumlar ve bireyler için hayati öneme sahip olan alt yapıları güvence altına almada, etkin bir rol üstlenmektedir. "Yapay zekâ" unsuru da tam bu noktada devreye girerek, bilişim ve iletişim teknoloji araçlarının üstündeki yükü hafifletip, daha hızlı ve etkin bir biçimde ağ güvenlik açıklarını tespit etmede son derece etkilidir. Makine öğrenimi, yapay zekâ gibi araçlar, güvenlik açıklarını belirleyebilir, kötü niyetli yazılımları ve saldırıları bulup analiz etme becerisine sahip olduklarından bunun gibi pek çok görevi otomatikleştirebilirler (Admass vd., 2024, s.1-6).

Siber güvenlik; şifreleme, savunma ve saldırıları tespit eden mekanizma olma özelliğiyle, güvenli bir ortam oluşturarak tehditleri önler, bilgilerin gizliliğini korur. Siber güvenliğin pek çok uygulama alanı mevcuttur. Akıllı şebeke olma özelliği, siber güvenliğin uygulama alanlarından biridir. Elektriğin üretilmesi, tüketilmesi ve dağıtımında optimum fayda sağlayan bilgi ve iletişim teknolojilerini kullanan akıllı şebekeler; güvenirliği sağlama hususunda pek çok avantaj sunmaktadır. Akıllı şebekelere yönelik siber saldırılar sonucunda yaşanılacak elektrik kesintileri, finansal çöküntüler ve güvenlik açıkları gibi risklere karşı siber güvenlik önlemlerinin alınması yani güçlü şifreleme ve kimlik doğrulama mekanizmalarının devreye girmesi önemlidir (Admass vd., 2024, s.2). Siber güvenlik uygulama alanlarından bir diğeri de akıllı şehirlerde siber güvenliğin sağlanmasıdır. Şehirlerde insanların refah ve huzur ortamı içinde yaşamaları ve yaşam standartlarının yükseltilmesi; kentsel güvenlik altyapısının oluşturulmasıyla yakından ilişkilidir. Kentlerde ulaşım, iletişim, elektrik gibi hayati sistemleri koruyan,

kent trafiğini kontrol altına alan siber güvenlik araçlarından sensörler, nesnelerin interneti (IoT) ve kameralar vasıtasıyla, insanların kişisel verileri korunur ve güvenlikleri sağlanır. Yol güvenliği ve trafik kontrolünü sağlayan araç içi iletişimde güvenlik; siber güvenliğin uygulama alanı içinde yer alır. Araç içindeki elektronik sensörler ile diğer yazılım ve donanımlar sayesinde siber güvenlik sağlanarak, yolcuların güvenliği teminat altına alınır, araç sürücüsüne sürüş esnasında kolaylık sağlanır, sürücü ve yolcuların kişisel verileri korunur (Admass vd., 2024, s.2). Siber güvenliğin yaygın kullanım alanlarından biri de sağlık sisteminde kendisini göstermektedir. İnsanların sağlık kayıtları artık IoT tabanlı sağlık uygulamaları, internete bağlı akıllı telefonlar, çeşitli tıbbi cihazlar vasıtasıyla toplanarak gerçekleştirilmektedir. Yalnız son yıllarda Dünya Ekonomik Forumu'nun yapmış olduğu araştırmalara göre, 10 milyonu aşkın hasta kaydı ve insanların tüm sağlık verileri, çeşitli kötü amaçlı hackerlar vasıtasıyla çalınmış durumdadır. Hassas olan hasta kayıtlarını korumak, tüm insanların sağlık verilerini güvence altına almak, kişilere ve sağlık kuruluşlarına zarar verecek her türlü kötü saldırıların önlenmesi için siber güvenliğin sağlanması istenilmektedir (Admass vd., 2024, s.2).

3. Avrupa Birliği Siber Güvenlik Stratejisine Genel Bir Bakış

AB siber güvenlik stratejileri; bünyesindeki vatandaşları ve kuruluşları siber tehlike ve tehditlerden koruyarak, güvenilir bilgi ve iletişim teknolojilerinin kullanımını teşvik eden politikalar gütmektedir. Teknolojinin dur durak bilmeyen hızlı gelişimi; aynı zamanda çeşitli güvenlik tehditlerinin türemesine de yol açmakta ve ülkeleri ulusal-uluslararası arenada stratejilerini ve politikalarını yenileyip güçlendirme yoluna sevk etmektedir. Avrupa Komisyonu ve AB Dış İlişkiler ve Güvenlik Komisyonu Yüksek Temsilcisi, yenilenen AB siber güvenlik stratejisini ilan etmiştir. Bu stratejinin amacı, AB'nin güvenli bir dijitalleşme süreci yaşaması ve siber güvenlikle ilgili oluşturulan politikalarının düzgün işleyebilmesi için yasaların güncellenmesidir (Europen Comission, 2025).

Temel hak ve hürriyetlerin siber alanda korunmasının hayata geçirilmesini amaçlayan AB, uluslararası arenada devletler ve uluslararası kuruluşlarla işbirliği içerisinde hareket edilmesi, kişisel ve kamusal verilerin korunarak ifade özgürlüğünün sağlanması gibi pek çok ilkenin yanında, global işbirliği ve yönetişimi baz alan bir model önerisi sunmaktadır (Ministry For Foreign Affairs To Finlad, 2025). Bu amacın gerçekleştirilmesi için; hükümet, halk, STK'lar ve özel sektör kuruluşlarının işbirliği içerisinde hareket ederek bu sorumluluğu yüklenmelerinin gereğine vurgu yapılmıştır. AB'nin dijital egemenliği ve üstünlüğünü, bununla ilişkili tüm hizmet ve araçların sağlam olması ile ilişkilendirmiştir. Kolluk kuvvetlerinin, politikacıların, ulusal organların ve savunma ile bağlantılı olan dört ayrı siber topluluğunun, siber saldırılar ve tehditlere karşı birlikte hareket etmeleri ve yönetişimin gerçekleştirilmesinin gerekliliği belirtilmiştir. Siber saldırılar karşısında topyekûn birlikte hareket edilmesinin AB'yi güçlü kılacağı, yeniden ifade edilmiştir. Bu strateji ile olası büyük siber saldırılar ve tehditlere karşı ortak hareket edilmesi amaçlanmaktadır. Siber uzayda uluslararası güvenliğin sağlanması hususunda da diğer uluslar ve uluslararası paydaşlarla birlikte hareket edilmesi ve ortak planlar yapılmasının gerekliliği üzerinde durulmuştur. AB, bu yeni strateji için diğer stratejilere yaptığı yatırımın dört katını yapacağını; daha somut ve düzenleyici öneriler içeren bu stratejiye üstün destek sağlayacağını ifade etmiştir (Europen Commission, 2025).

AB, son yıllarda siber güvenlik krizleri ile siber güvenlik olayları arasındaki ilişkiye dikkat çekerek, bu durumu yeni siber güvenlik yasalarında özellikle vurgulamıştır. Siber güvenlik krizleri; AB'deki tek bir üye devleti aşarak en az iki üye devleti etkileyecek düzeyde olan büyük çaplı siber güvenlik olaylarıyla aynı kefede tutulmuştur. AB, yeni yasalarında, büyük çaplı siber güvenlik olaylarının yanında her türlü siber olayı raporlamayı zorunlu hale getirmiştir. Ancak, kurulan yeni yönetişim aktörlerine ve yasalarca zorunlu hale getirilen önlemlere rağmen, AB'nin siber güvenlik kriz yönetiminde halen boşluklar ve belirsizlikler yer almaktadır (Ruohonen vd., 2025, s. 6-7).

Avrupa'nın 15 yıldır kriz yönetiminde olduğu iddia edilse de bu durum siber güvenlik alanını kapsamamaktadır. Avrupa' da şu ana kadar büyük çaplı ve tüm Avrupa'yı içine alan bir siber güvenlik krizi yaşanmamıştır. Yalnız Avrupa Komisyonu, üye ülkeleri içine alacak olası büyük çaplı bir siber güvenlik kriz yönetimi ile ilgili önemli bir teklif yayımlamıştır (Rouhınen vd., 2025, s. 1). AB'nin en yeni siber güvenlik stratejisinin üç sac ayağı bulunmaktadır. Bunlar; önleme, tespit ve müdahaledir. AB'nin bu stratejisi, yasalarla çerçevelendirilmiştir. Yasalara; finansman, eğitim ve inovasyon projeleri, yönetim organları gibi pek çok çevreden destek verilmektedir. "İkinci Ağ ve Bilgi Güvenliği Direktifi"

(NIS2) ile "Siber Dayanıklılık Yasası" en önemli siber güvenlik yasalarındandır (CRA) (Rouhonen, vd., 2025, s. 4). NIS2 Direktifi, AB içindeki pek çok üye devletin siber güvenlik krizini tanımlayan nitelikte olmaktan ziyade, ulusal yasaları ve ulusal stratejilerindeki eksikliği kapatan, bir nevi tamamlayıcı nitelikteki bir yasadır. AB'nin siber güvenlik stratejileri incelenirken, yapılan yasaları oluşturan organların/idari birimlerin işlevlerinin araştırılması ve bu araştırmanın şeffaflık, âdemi merkeziyetçilik, hesap verebilirlik, işbirliği ve koordinasyon kıstasları ele alınarak ayrı ayrı değerlendirmesi gerekmektedir. Siber güvenlik olayları ve krizleri arasındaki ilişkiyi, Avrupa Birliği derinden algılayamadığı için, diğer ülkelerin ulusal siber güvenlik stratejileri hakkında kıyaslama ve araştırma yapması, iki kavram arasındaki farkın anlaşılması açısından gerekli görülmektedir (Rouhinen vd., 2025, s.10).

AB'nin Siber Güvenlik Yasaları arasında öne çıkan; Dijital Hizmetler Yasası (DSA), Siber Dayanıklılık Yasası, Avrupa Birliği Yapay Zekâ Yasası, Genel Veri Koruma Yönetmeliği (GDPR); birbirleriyle koordineli hareket ederek uygulanmaktadırlar. Siber güvenliğin sağlanması için oluşturulmuş bu yasalar özellikle siber güvenlikte yapay zekânın kullanımını teşvik etmekte ve kolaylaştırmaktadır. Yapay zekânın öngören ve analiz eden algoritmalar olması, denetim mekanizmasını düzenlemesi gibi önemli özelliklerinin olmasından ötürü, günlük hayatta kullanımı giderek yaygınlaşmaktadır. Siber güvenlik alanında yapay zekâya duyulan ihtiyaç, güçlü algoritmik temeller üzerinde oturtulmasını ve önemli düzenlemeler yapılmasını gerekli kılmıştır (Beltran, 2025, s.2).

Yapay zekâ yasası, yapay zekâ sistemlerini risk temelli bir anlayışla ele alır. Yasanın 5 ve 6. Maddeleri; kabul edilemez riskteki yapay zekâ uygulamalarını, denetim altında tutulması gereken yüksek riskli yapay zekâ sistemlerini ve en düşük riskli yapay zekâ sistemlerini kapsamaktadır. 8. ve 15. Maddeler arasında, yüksek riskli yapay zekâ sistemlerinin taşıması gereken bir takım unsurlar yer almaktadır. Bu unsurlar; veri yönetimi, yüksek riskli yapay zekâ sistemlerinin yaşam boyu denetimini sağlayacak ve sürekli güncellenecek bir risk yönetiminin oluşturulması, şeffaf olunması ve kullanıcılara bilgi aktarılması, yapay zekânın yasalara uygunluğunu belirten ayrıntılı teknik bir dokümantasyonun bulunması, insan denetimine yatkın bir sistem haline getirilmesi, manipüle edilemeyen ömür boyu tutarlı ve güvenilir bir yaşam sürdürecek şekilde tasarlanmış, saydam yapıya sahip sistemler olması ve son olarak yüksek riskli yapay zekâ sistemlerinin güçlü bir şekilde siber güvenliği sağlaması ve siber tehditlerden korumasıdır. Yapay Zekâ Yasası'nın denetlenmesi ve uygulanması, öncelikli olarak üye devletler ile AB arasında paylaştırılmış ve nihai olarak Avrupa Komisyonu ve Yapay Zekâ Kurulu tarafından yerine getirilmiştir. Yapay zekânın siber tehditleri tespit etmesi ve siber güvenliği sağlaması ile ilgili olarak yapılan çalışmalar incelendiğinde; olay yönetimi, veri depolama gibi konularda sıkıntı çıkabileceğini; yapay zekânın bu alanda daha yaygın kullanıldığında, gizlilik ve güvenlik alanında yeni tehditlerin doğabileceği belirtilmiştir. AB'nin Yapay Zekâ Yasası, son teknolojik gelişmeleri içeren yapısıyla büyük risk içeren yapay zekâ sistemleri için sağlam bir teknik altyapının gerekliliğini ön görmektedir. Ancak yapay zekânın gelişme hızı ve karmaşık yapısı, "son teknoloji" kavramını açıklamada yetersiz bırakmakta ve kurumların "son teknoloji"ye uyumlamasını zorunlu hale getirmektedir. "Avrupa Veri Toplama Kurulu" da işte tam bu amaçla, geçmişte "son teknoloji"nin uygulanması açısından veri koruması adı altında denetim yapmak ve kontrol etmekle yükümlü tutulmuştur. Çıkarılan yasaların (CRA, GDPR, DSA ve Yapay Zeka Yasası gibi), bütünleşik bir politika izlenerek birlikte ele alınmaları ve uyumlu hale getirilmeleri gerekmektedir ki, siber güvenlik sağlanabilsin. Bu amaçla da karmaşık olan alanların ve belirsizliklerin sağlıklı yorumlanması elzemdir (Beltran, 2025, s. 4-5).

AB'nin Dijital Hizmetler Yasası (DSA); internet ortamının ve çevrimiçi platformların şeffaf olması, bu platformların hesap verebilir olmaları ve algoritmaların bu ilkeler altında adaleti yerine getirmesi için dijital hizmetlere bir takım ödev ve yükümlülükler getirmiştir. Yasa, zararlı programlar ve yasa dışı içeriklerle mücadele ederek, güvenilir bir internet ortamı oluşturmaya çalışmaktadır. Yasanın 28. maddesi, özellikle çocukların korunmasına ilişkin olarak, çevrimiçi platformların dezavantajlarından ve bu platformlardan gelebilecek her türlü tehlikelerden çocukların ve kişilerin haklarının korunmasını amaç edinmiştir. Algoritmik sistemlerin hizmetlerini analitik bir süzgeçten geçirerek, işleyişi ile ilgili sistemsel aksaklıkların/arızaların önlenmesi, risklerin önceden tespit edilmesi için denetleme ve değerlendirme yapmaktadır (Çevik, 2023).

Genel Koruma Yönetmeliği; gerçek kişilerin temel hak ve özgürlüklerinin teminat altına alınması, kişisel verilerin korunması, muhafaza edilmesine yönelik yükümlülükleri ve kişisel verilerin serbest dolaşımına ilişkin esasları ortaya koymaktadır. Bu yönetmeliğin özellikle 12. ve 23. maddeleri arasındaki düzenlemeleri, bu amaçlarla ilişkilendirilmiş ve algoritmik sistemlerin kişisel verilerin kullanılması, sunulması ve güvenliğinin sağlanmasını yerine getirecek şekilde tasarlanmıştır. 04.05.2016 tarihinde Resmi Gazetede yayımlanan "Genel Veri Koruma Yönetmeliği", Avrupa ekseninde tüm verilerin gizliliğine ilişkin kuralları uyumlu hale getirmeyi amaçlamış ve 25.05.2018 tarihinden itibaren AB'ye üye tüm ülkelerde geçerli hale gelmiştir (GDPR Madde1, 2025).

Siber Dayanıklılık Yasası (CRA), 10 Aralık 2024 tarihinde yürürlüğe girmiş ve dijital içerikli ürünlerin siber güvenliklerinin sağlanması hususunda önemli atılımlar gerçekleştirmiştir. Bu kapsamda ihracatçılara, üreticilere ve distribütörlere yeni sorumluluklar yüklenmiştir. Siber güvenliğin en ince ayrıntısına kadar sağlanmasını amaçlayan bu düzenleme; akıllı ev aletlerinden endüstriyel kontrol sistemlerine, yazılım uygulamalarından, bileşenlerine kadar pek çok dijital ürün çeşidini içermektedir. Üreticilerin en erken 5 yıl içinde ya da ürünün ömrü daha kısa ise ürünün yaşam süresi içerisinde güvenlik açıklarını ortadan kaldırıp, güvenilir tasarım ilkelerini, ürüne entegre etmeleri istenmektedir. Yani amaç, dijital güvenlik açıklarının en aza indirilerek ya da ortadan kaldırılarak tüm üretim sürecinin bu saikle devam ettirilmesini sağlamaktır. Ayrıca ürünlerin siber güvenliğine ilişkin detaylı bir rapor hazırlayıp, ciddi bir siber güvenlik tehdidinin fark edilmesi halinde 24 saat içerisinde Avrupa Birliği Siber Güvenlik Ajansı'na (ENISA) bildirilmesi zorunlu tutulmuştur (Ergene, 2024).

AB Komisyonu'nun İç İlişkiler ve Göçten Sorumlu Üyesi Magnus Brunner'ın 2025 yılında verdiği demeçte Magnus Brunner, güvenliğin önemine vurgu yaparak, kolluk teşkilatının güçlendirilmesinin gereğine ve dijitalleşen toplumda suçların dijital ortamda sürdürülerek devam ettiğine işaret etmiştir. Siber saldırılar, dolandırıcılık, kara para aklama, şiddet olayları gibi suçların çevrimiçi platformlarda artış gösterdiğini belirtmiştir. Bu bağlamda verilerin korunması ve bu suçların önlemesi için, AB'nin siber güvenlik stratejileri ile politikalarının ve siber suçlara ilişkin önlemlerin yetersiz kaldığını, stratejilerin daha etkin hale getirilmesi, caydırıcı cezalarla suçların önlenmesi ve kolluk personeli ile kolluk teşkilatının güçlendirilmesi ve son olarak siber güvenlik politikalarının geliştirilmesi için yeni çalışmalar yapıldığını dile getirmiştir. Ayrıca Avrupa Komisyonunun suç örgütlerine ilişkin olarak "suç örgütü" tanımını yenileyen, bu örgütlere ilişkin yaptırımlarını kuvvetlendiren yeni bir yasa tasarısının hazırlığının yapıldığını ve 2026 yılında sunulacağını da bildirmiştir (haberler.com, 2025).

AB, soğuk savaşın ilk yıllarında güçlü bir duruş ve başarılı bir yapı sergilerken, bugün güçlü taraflarını öne çıkarma konusunda eski ihtişamını ve etkisini sergileyememektedir. Bu duruma etki eden iki unsur vardır. İlki AB'nin ortaklarıyla küresel politika oluşturması hususundaki eksikliğidir. İkincisi ise, kendi bünyesindeki devletlerin farklı yapılara sahip olması ve onları ortak karar alma noktasında dengeleme sıkıntısıdır. Küresel arenada çıkış yakalayan yeni güçlü devletler ağırlıklarını sergilemektedirler ve AB, bu küresel güçlerle olan ilişkilerini geliştirmek için öncelikle kendi içinde yer alan ayrı görüşteki devletleri; ortak hareket etmeye, ortak kararlar almaya ve uyum içinde olmaya yöneltmelidir. AB'nin; NATO, BM, Çin, Rusya gibi küresel arenadaki güçlü uluslararası kuruluşlar ve devletlerle ilişkilerinde etkin olabilmesi için öncelikle kendi içindeki üye devletlerin kendi aralarında uyumlu olmaları ve fikir birliğinin sağlanması gerekmektedir. Birliğin yeniden küresel bir güç dengesi potansiyelini yaratması, bu şartları oluşturmasına bağlı gibi görünmektedir (Stokes ve Whitman, 2013, s. 1102-1103).

AB'nin siber güvenlik alanında önemli bir küresel temsilci olduğu doğrudur fakat bu bilgi, içerisinde eksiklikleri de barındırmaktadır. Bu durumun altındaki etmenler ise, az önce bahsedilen siber güvenlik alanında, birliğe üye ülkeler arasındaki ortak vizyonun istenilen düzeyde oluşturulamamasıdır. Birlik bu amaçla hem bir kuruluş olarak hem de kendisine bağlı devletler arasında fikir birliği sağlama hususunda daha etkili politikalar güdeceğini, siber güvenlik alanındaki etkinliğini artıracağını belirterek daha yoğun bir performans gösterme sürecine girdiğinin teminatını vermiştir. Bu bağlamda da siber güvenlik stratejilerinin etkinliğinin artırılması için, yasal düzenlemeler ve uygulamalar üzerinde çalışarak geliştirilmesi planlanmıştır. Üye ülkeler her ne kadar siber güvenlik noktasında önemli tedbirlerin alınmasını ve birlikte hareket edilmesini öne sürseler de henüz bu hedefin en ileri noktaya ulaşamadığının, tap noktasına gelmediğinin altını çizmişlerdir (Altın, 2023, s. 499).

Bu görüşler doğrultsunda Avrupa Birliği'ne üye ülkeler arasında siber güvenlik politikaları ve stratejileri açısından en iyilerinden alınacak destek, Avrupa Birliği'ni siber güvenlik alanında önemli bir konuma getirecektir ki bu konuda çok başarılı olan Finlandiya örneğinin incelenmesi ve stratejisinin ele alınması, çalışmamız açısından önem arz etmektedir.

4. Finlandiya Siber Güvenlik Stratejisi

Finlandiya Avrupa'nın en doğu sınırında yer almaktadır. Jeopolitik konumu itibariyle güvenlik konusu oldukça önemlidir. Siber güvenlik teknolojisinde Finlandiya, global düzeyde başı çeken bir konumda yer almaktadır. Yalnız dijital teknolojileri kullanımda lider olmak ile halkın siber güvenliğini sağlayacak politikalar üretmek ve stratejiler oluşturmak arasında önemli bir fark bulunmaktadır (Griffith, 2018, s. 407-408).

2010 yılında çıkarılan "Toplum İçin Güvenlik Stratejisi", Finlandiya için oldukça önemli stratejik politikaları içermektedir. Bunlar; Finlandiya'nın savunma sistemi, uluslararası uygulamalar ve hükümetin iç güvenliğin işleyişi için gerekli alt yapının sağlanmasına yönelik politikalarıdır. Siber güvenliğin sağlanması, siber alanın güvenilir bir ortam sunması ve siber güvenliğin işleyişinin halkın refahını ve mutluluğunu artıracak düzeyde gerçekleştirmesi, Finlandiya hükümetinin varmak istediği nihai amaçlardır. İlk olarak 2013 yılında hazırlanan Finlandiya Siber Güvenlik stratejisi ile; bilgi toplumunda bilgi ağları ve sistemlerini kullanma, alt yapı oluşturma ve bunlara ilişkin aksaklıkların ortaya çıkması ihtimalleri göz önüne alınarak, Finlandiya'nın oldukça yetersiz ve savunmasız bir durumda olduğu raporlanmıştır. "Siber alan" kavramına değinilen bu strateji, toplumun hayati işlemlerinin güvence altına alınması, bilgi ve iletişim teknolojilerinin entegre süreci, bilgi ve veriye erişimin kolaylaşması, açık ağların kullanımı, internete bağımlılık; kriz durumunda toplumun ve tek tek insanların yaşamlarını güvence altına almak konularında hayati bir öneme sahiptir. Stratejide ayrıca siber saldırı ve siber suç kavramları açıklanarak, siber alana yönelik tehditlerin ciddi sonuçlarının olabileceğini, suçluların daha profesyonel ve tehlikeli olduklarını, siyasi ve ekonomik baskı aracı olarak kullanılabileceğini ileri sürmüştür. "Siber alan" bir kaynaktır ve iyi işlerse uluslararası yatırımcılar için cazibe alanına dönüşür. Finlandiya şirketlerinin güçlü ve başarılı olması, siber güvenliğin de başarılı şekilde sağlanmasıyla ilişkilidir (Finland's Cyber Security Strategy, 2013, s. 1-2).

Finlandiya İçişleri ve Savunma Bakanlığı 15 Şubat 2022 yılında; siber suçlarla mücadele, ulusal çapta siber güvenliğin sağlanması, siber güvenliği sarsan her türlü olay ve krize karşı toplumun korunması için mevcut halde bulunan ve geleceğe yönelik yapılması gereken plan ve çalışmaların değerlendirildiği bir proje başlatmıştır. Bakanlıklar ve kurumlar arasında kapsamlı işbirliği çerçevesinde hazırlanan bu rapor; mevcut ulusal siber güvenlik politikalarını eleştirerek ülkede uygulanan çalışma modelinin daha etkili olabilmesi için mevzuat değişikliği yapılmasını, kurumlar arasında işbirliğini yaygınlaştırıp, kurumlar arası iletişimin geliştirilmesini ve kurumların eksikliklerinin belirlenmesine ilişkin önerileri içeren bir takım tespitlerde bulunmuştur (Valtioneuvoston Julkaisuja, 2023). "Finlandiya Ulaştırma ve İletişim Ajansı", "Finlandiya Güvenlik ve İstihbarat Servisi", "Finlandiya Savunma Kuvvetleri", "Finlandiya Polisi" gibi kurumlar, Finlandiya' da siber suç ve saldırı durumunda bunları tespit edecek ve gerektiğinde savunmaya geçecek kurumlar ve organlardır (Valtioneuvoston Julkaisuja, 2023).

Finlandiya 2024-2035 yıllarını kapsayan Yeni Ulusal Siber Güvenlik Stratejisi ve Uygulama Planı'nı yayımlamıştır. Bu yeni strateji ve uygulama planının amacı; bireylerin ve toplumun güvenliğini sağlamak, siber sistemlerin problemsiz bir şekilde çalışmasını gerçekleştirmek ve siber tehditlere her an karşılık verebilecek nitelikte olmaktır. Finlandiya, siber güvenlik alanında, aynı zamanda uluslararası tartışma platformlarına katılarak ve bu alandaki işbirliklerini çoğaltıp geliştirerek, siber güvenliği güçlendirmeyi hedeflemektedir. Ulusal siber güvenlik stratejisinin ulaşmak istediği noktayı, on temel madde de belirtmiştir. Finlandiya'nın siber güvenlik stratejisinin uygulamasından Güvenlik Konseyi sorumluyken, strateji ile ilgili uluslararası paydaşlarla ilişkilerin sağlanması ve koordinasyonun gerçekleştirilmesinden Finlandiya Dışişleri Bakanlığı sorumludur (Ministry For Foreign Affairs to Finlad, 2025).

Dışişleri bakanlığı, Finlandiya'nın uluslararası işbirliklerini yönetme ve kontrol etmede yani yerel, bölgesel, ulusal ve uluslararası alanda siber güvenlikle ilgili müzakerelerde önemli roller üstlenmektedir. Siber alan ile ilgili tartışmalar AB, AB Konseyi, NATO, OECD, ASEAN Bölgesel Forumu ve OAS gibi uluslararası kuruluşların çatısı altında gerçekleştirilmektedir. Siber alan ve siber

güvenlik konusu, devletler arasında tartışılması ve belirlenmesi gereken önemli bir konudur. AB, siber güvenlik alanında Finlandiya ve diğer Avrupa ülkeleri için önem teşkil eden yasalar ve yaptırımlar geliştirmiştir. Finlandiya'nın en son yayımladığı Siber Güvenlik Stratejisi 2024-2035 yıllarını kapsamaktadır ve 10 Ekim 2024 tarihinde onaylanmıştır. Siber Güvenlik Stratejisinin hazırlanma süreci; kamu kesimi, özel sektör, STK'lar ve akademik camia olmak üzere toplumun bütün kesimlerinin katkılarıyla gerçekleştirilmiştir. Strateji uygulama planı, siber güvenlik stratejisinin hedeflerine kavuşmasına rehberlik eden ve tedbirler alan önemli bir plandır. Uygulama planı; her yıl izlenecek, denetlenecek ve ihtiyaç duyulduğunda güncellenebilecektir. Uygulama planını izleyecek Devlet sekreterlerinden oluşan bir yönlendirme grubu bulunmaktadır ve Siber güvenlik Stratejisi'ni denetlemektedir (FI_ACTION_PLAN, 2024, s. 1).

Uygulama planı; stratejik amaçlardan ve kalkınma önerilerinden oluşmaktadır. Bu nihai amaçlar aynı zamanda ulusal siber güvenlik hedefleri ve politikalarını da oluşturmaktadır. Planda iki önemli ana başlık yer almaktadır (FI_ACTION_PLAN, 2024, s. 3). Bunlar;

1. Kısa vadeli, çok kritik olan ve yüksek etkilere sahip stratejik amiral gemisi projeleri,
2. Uzun vadeli ve daha az kritik olan projelerdir.

Tüm tedbirler ve hedefler, bunların hangi makamlar ya da aktörler tarafından yerine getirileceği ve finansmanına ilişkin bilgiler, açıkça uygulama planında belirtilmiştir. Siber güvenlik stratejisinin uygulama ayağı, yıllık olarak takip edilmektedir. Bu faaliyetlerin takibinin koordinasyonunu gerçekleştiren kurum ise Ulusal Siber Güvenlik Direktörlüğü Ofisi'dir. Ofis, hazırladığı raporların özeti mahiyetindeki kopyalarını kamu yöneticileri ve siyasi yöneticilere taktim eder. 1 Kasım 2024 tarihinden itibaren Siber Güvenlik Stratejisi'nin uygulanmasını takip etme ve denetimini sağlama amaçlı bir izleme grubu oluşturulmuştur. Siber Güvenlik Stratejisi İzleme Grubu; izleme raporları için ne kadar ilerlendiğine dair kayıt oluşturur, uygulama planını organize eder, gerektiğinde şartlara göre revize eder. Sorumlu idari birim ise; katılımcı olarak ya da ana sorumlu makam olarak kalkınma tedbirlerini faaliyete geçirir. Bunun gibi pek çok ana ve yardımcı birime, ortaklara ve paydaşlara görev ve yetkiler dağıtmıştır (FI_ACTION_PLAN, 2024, s. 2-3).

Ulusal Siber Güvenlik Direktörü Ofisi'nin başlıca görevleri şunlardır (FI_ACTION_PLAN, 2024: 4);

- Stratejinin faaliyetlerini ve uygulama planının ilerlemesini değerlendirmek için paydaşlarla bir araya gelerek yılda bir toplantı etkinliğini düzenlemek,
- İzleme grubundan alınan görüşleri değerlendirerek faaliyet raporu oluşturmak,
- Hazırlanan faaliyet raporlarını ilgili birimlere aktarmaktır. (Bu birimler; Güvenlik Komitesi, Sosyal Dönüşümle İlgili Bakanlık Çalışma Grubu, Hükümet güvenlik yönetimi işletme modeli geliştirme projesini denetlemekle görevli devlet sekreterlerinden oluşan yönlendirme grupları ve diğer paydaşlardır)

Finlandiya Ulusal Siber Güvenlik Stratejisi'nin amaçları detaylı olarak aşağıda belirtilmiştir. Bunlar; (FI_ACTION_PLAN, 2024, s. 5-38);

- Verilere ulaşımını zorlaştıran ve şifreleyerek koruyan kriptografi teknolojisinin uygulanabilirliğini kolaylaştırmak,
- Kriptografi teknolojisi alanında ulusal bir karakter geliştirmek, bu teknolojinin AB ve NATO'nun kriptografi ürünlerine cevap verebilir niteliğe büründürerek uyumlulaştırmak ve bu şekilde Finlandiya'yı, NATO ve AB'nin bilgi güvenliği sistemlerine cevap verebilen bir ülke haline getirmek,
- Ulusal siber güvenlik ve kriptografi eğitim programlarını oluşturmak ve ülke genelinde yaygınlaştırmak,
- Ulusal düzeyde siber güvenliği sağlayan her türlü mekanizmayı, sistemi ve kriptografi ürünlerini üretecek bir laboratuvar kurmak,
- Siber güvenliğin gelişimi için işbirliklerinin güçlendirilmesi,

- Siber güvenlik politikasında etkinlik analizinin yapılması,
- Toplumda siber güvenlik uzmanlığının geliştirilmesi,
- Ulusal verileri koruma yeteneklerinin artırılması, gerekli şifreleme yöntemlerinin oluşturulması ve verilerin bütünlüğünün korunması,
- Siber güvenlikle ilgili olarak bugün ileri görüşlü planlar yaparak geleceğe dair öngörüde bulunmak ve uluslararası standartta bir plan oluşturmak,
- Hem iş dünyası hem de kamu otoritelerince kullanılmak üzere, siber güvenlikle ilgili günümüzde ve gelecekle ilgili tehditleri algılayan/ analiz eden verilerin üretilmesi,
- Kamu kesimiyle özel kesimin ortaklaşa ve uyum içinde hareket ederek, siber tehdit ortamı ile ilgili birlikte senaryolar oluşturmaları,
- Finlandiyalı aktörlerin ve şirketlerin, ulusal ve uluslararası arenada yeni ortaklar bulmalarını kolaylaştırmak,
- Siber güvenlik çalışmaları ve araştırmaları hususunda ortak bir fon oluşturmak, projelere katılım için yeterli düzeyde finansman sağlamak,
- AB ve NATO'nun kalkınma fonlarının kuvvetlendirilmesinin sağlanması,
- Savunma ve siber güvenlik sektörünün millileştirilmesi,
- Siber güvenlik işbirliği ağının kurulması,
- Finlandiya İnternet Merkezi'nin çalışmalarını desteklemek,
- Vatandaşların siber güvenlik konusunda bilinçlendirilmesine yönelik her türlü çalışmayı destekleyerek, farklı nüfus gruplarına ilişkin siber tehditlere karşı iletişim ve işbirliği sağlanması/ geliştirilmesi,
- Siber kriz durumunda özel kesimin ve kamu kesiminin ulusal savunma ve askeri krizlere uyum sağlayabilme potansiyelini geliştirme, kamu/özel sektörün siber krizlere karşı tedbirler almalarını sağlama,
- Merkezi hükümetin yerel yönetimlerle işbirliği içerisinde siber güvenlik konusunda ortak hareket etmesi; yerel yönetimlerin siber güvenlik kaynaklarını planlaması,
- Siber güvenlik alanında uluslararası kuruşların standartizasyon çalışmalarına etki etmek ve özel sektörü de teşvik etmek,
- Sağlık ve sosyal alanda kişisel verilerin korunmasına ilişkin çalışmaların artırılması, temel gereksinimleri karşılaması,
- Finlandiya Savunma Kuvvetlerinin kendi savunma ve şifreleme sistemlerinin ulusal ve uluslararası standartlara uygunluğunun sağlanması/geliştirilmesi,
- Risk temelli değerlendirme prosedürlerinin geliştirilmesi; açık, saydam ve anlaşılabilir düzeye getirilmesi,
- Finlandiya'nın, AB ve NATO'nun çok uluslu siber tatbikatlarına katılımının gerçekleştirilmesi,
- Kamuda operatörler arasında mobil ağların geliştirilmesi konusunda koordineli hareket etmelerinin teşvik edilmesi,
- Telekomünikasyon operatörleri ile dijital alt yapının, olası siber saldırı ve tehditlere karşı güçlendirilmesi,
- AB Uzay Programı vasıtasıyla kamu kurumları ve kritik altyapıya sahip alanlarda sertifikalı uydu hizmetlerinin sağlanması,
- Finlandiya radyo frekanslarının uydu işleme operasyonlarında kullanılabilir kılınması,

- Siber Dayanıklılık Yasası'nın uygulanabilmesi için sertifikasyon gerekliliğinden dolayı, ulusal düzeyde sertifikasyon sağlayacak yetkili organları teşvik etmek/desteklemek,
- Ulusal Siber Güvenlik Merkezi'nin siber güvenlik açıklarını tespit etme becerisinin güçlendirilmesine destek olmak,
- Finlandiya'nın, AB ve NATO gibi uluslararası kuruluşların siber güvenlik çalışmalarına katılımını desteklemek, aktif rol almasını gerçekleştirmek,
- Siber güvenlik kavramını güncellemek, aktörler arasındaki bilgi alışverişini revize ederek koordineli çalışmalarını sağlamak,
- Kritik kuruluşlara yardım edebilmek için gerektiğinde mevzuatı değiştirebilme esnekliğinin olması,
- Siber savunma ve devlet egemenliğine ilişkin yasal mevzuatı güncelleyerek güçlü hale getirmek, siber savunma düzeyinin yerel, bölgesel ve ulusal düzeyde güçlendirilmesini sağlamak,
- Siber güvenlik ve siber savunma hakkında gerekli yasal mevzuatın tamamlanması ve siber savunma durumunda tüm aktörlerin ve kamu otoritelerinin rollerinin belirlenmesi,
- Uluslararası hukukun uygulanmasında hükümet kararlarının gözden geçirilmesi,
- Yaygın siber suçların, işleniş biçimlerinin ve cezai zararların araştırılması irdelenmesi,
- Çevrimiçi dolandırıcılıkla mücadelede iş dünyası ile işbirliği içerisinde hareket edilmesidir.

Bunlara ek olarak Finlandiya İstihdam ve Ekonomi Bakanı, 2017 yılında Finlandiya'nın Ulusal Yapay Zekâ Stratejisi olan "Yapay Zekâ Çağı" adlı programını yayımlamıştır. Finlandiya'nın dijital dönüşümünde yapay zekânın rolüne ve etkilerine odaklanan bu strateji, Finlandiya'nın bu alandaki güçlü ve zayıf yönlerine vurgu yapmıştır. Yapay Zekâ Stratejisi' nde; Finlandiya'nın dijital çağda güçlü olması, küresel çapta ekili rollere sahip olması için geçerli olacak politika ve planlardan bahsedilmiştir (Europen Commission, 2021).

Finlandiya Yapay Zeka Stratejisi, "açık veri politikası"nı baz alarak hareket etmiştir. Yapay Zekâ Stratejisi şu üç hedefi benimsemiştir (Europen Commission, 2021);

1. Kamu hizmetlerinin sunumunda hızlılığı ve etkinliği artırmak,
2. Özel sektör alanında piyasayı canlandırmak, sanayi kesiminin rekabet edebilirliğini artırmak,
3. Vatandaşların hizmetten en iyi şekilde faydalanmalarını sağlamak, kalite ve huzuru yerleştirmektir.

2018 yılında Yapay Zekâ Stratejisi'ne "Yapay Zekâ Çağında İş" adı altında bir rapor eklenmiş; 2019 yılında da "Yapay Zekâ Çağına Öncülük Etmek" adlı ikinci bir ek rapor daha yayımlanmıştır.

Finlandiya'nın en büyük hedefi, 2035 yılına kadar AB' nin siber güvenlik ve genişletilmiş sanal gerçeklik alanlarında öncü ülkesi haline gelmek ve küresel çapta başı çekmektir (Wolfenstein, 2023).

5. Sonuç ve Değerlendirme: Finlandiya ve AB Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi

AB ile Finlandiya'nın siber güvenlik alanındaki ilişkisine bakıldığında, Finlandiya AB'yi siber güvenliğin ana aktörü olarak değerlendirmektedir ve stratejilerini bu çerçevede şekillendirmektedir. Başka bir değişle Finlandiya nezdinde AB, siber güvenliğin merkez yöneticisi ve rehberi konumundadır. AB'nin siber güvenlik alanında çok çeşitli stratejilerle ve politikalarla öne çıktığı görülmektedir. Hem küresel çapta diğer uluslararası kuruluşlar ve devletlerle eşgüdümün sağlanması hem de kendi bünyesinde ki devletlerle uyumlu hareket ederek siber alanda başarılı politikalar ve stratejiler üretmesi, AB'nin siber güvenliğin en güçlü versiyonunu yaratmak için titiz çalışmalar yürüttüğünü kanıtlar niteliktedir.

Finlandiya'nın 2024–2035 Ulusal Siber Güvenlik Stratejisi; AB'nin Siber Dayanıklılık Yasası, Yapay Zekâ Yasası ve NIS2 Direktifi gibi düzenlemeleriyle uyum içinde tasarlanmıştır. Bu yönüyle Finlandiya,

Avrupa'daki en uyumlu ulusal model örneklerinden birini temsil etmektedir. Ülke, siber güvenliği yalnızca teknik bir savunma alanı olarak değil, aynı zamanda demokratik yönetimin ve ekonomik sürdürülebilirliğin vazgeçilmez bir bileşeni olarak konumlandırmıştır.

AB'nin siber güvenlik stratejileri ise, dijital dönüşüm sürecinde bütünleşik bir güvenlik ekosistemi oluşturmayı hedeflemektedir. Bu bağlamda çıkarılan yasal düzenlemeler, Avrupa dijital pazarında güvenilirlik, şeffaflık ve hesap verebilirliği temel ilkeler olarak benimsemiştir. Ancak AB düzeyinde politika üretimi ve üye devletler arasında eşgüdüm sağlama konusundaki zorluklar, stratejilerin etkinliğini sınırlamaktadır. Finlandiya gibi örneklerin önemi, bu eşgüdüm eksikliğini uygulama düzeyinde dengeleyebilme kapasitesinden kaynaklanmaktadır.

Finlandiya'nın stratejisi, sadece savunma reflekslerine değil, aynı zamanda önleyici mekanizmalara da dayanmaktadır. Her yıl denetlenen ve güncellenen uygulama planı, aktif bir yönetişim modeli oluşturmuş; kamu, özel sektör ve sivil toplum paydaşlarını sürece dâhil etmiştir. Kriptografi, yapay zekâ, veri yönetimi ve ulusal sertifikasyon sistemleri üzerinden geliştirilen bu yapı, AB standartlarıyla tam uyum içinde işleyen örnek bir ulusal model sunmaktadır. Finlandiya'nın siber güvenliği; ekonomik kalkınmanın, toplumsal istikrarın ve ulusal egemenliğin temel unsurlarından biri olarak tanımlaması, ülkenin stratejik vizyonunu daha da derinleştirmektedir.

Sonuç olarak, AB'nin oluşturduğu normatif çerçeve ile Finlandiya'nın uygulama temelli yönetişim modeli arasında tamamlayıcı bir ilişki bulunmaktadır. AB, siber güvenlikte ortak hukuk ve standartlar geliştirerek dijital egemenliğini güçlendirmeye çalışırken, Finlandiya bu vizyonun somut yansımasını ulusal düzeyde hayata geçirmektedir. Bu iki yapının karşılıklı uyumu, Avrupa'nın küresel siber güvenlik mimarisinde daha dirençli ve sürdürülebilir bir konum elde etmesini mümkün kılacaktır.

Siber güvenliğin geleceği; hukuki çerçevenin güncelliği, teknolojik yeniliklere uyum kapasitesi ve paydaşlar arası koordinasyonun sürekliliğiyle doğrudan ilişkilidir. Finlandiya örneği göstermektedir ki, güçlü bir stratejik planlama, izleme-değerlendirme mekanizması ve uluslararası işbirliği kültürü, siber tehditlere karşı uzun vadeli bir dayanıklılığın anahtarıdır. Avrupa Birliği'nin bu yaklaşımı benimsemesi, sadece dijital güvenliği değil, aynı zamanda demokratik değerlerin ve toplumsal güvenin dijital çağda korunmasını da garanti altına alacaktır.

Ortak tehdit ve krizlere karşı ortak savunma geliştirmek, sadece güvenli bir siber güvenlik geleceğini inşa etmek değil, aynı zamanda Avrupa'nın bütünleşmesinin özüyle ve ruhuyla yani tam manasıyla özdeşleşerek gerçekleştirilmesi açısından önem arz etmektedir.

Finlandiya Siber Güvenlik Stratejisi ile AB Siber Güvenlik Stratejisi'nin güçlü ve zayıf yönlerini daha net belirtmek ve neden AB'nin Finlandiya modelini merkezine alarak hareket etmesi gerektiğini göstermek için, temel kıstaslar üstünden kıyaslamak faydalı olacaktır

1. Finlandiya'nın siber güvenlik stratejisi daha bütüncül ve merkezi bir yaklaşımla çerçevelenmiştir. Mevcut hali ile oldukça başarılı olan Finlandiya siber güvenlik stratejisi; toplumu, kamu ve özel sektör kuruluşlarını ortak bir paydada birleştirme konusunda da oldukça başarılı görünmektedir. Siber güvenlik Finlandiya için; teknik bir meselenin ötesine geçmiş, toplumsal dayanıklılık ve beka meselesi haline gelmiştir. AB siber güvenlik stratejisi çok katmanlı ve koordinasyon odaklı özelliklere sahiptir. Başarılı olunması için, üye devletler arasında uyum sağlanması gerekmektedir. Siber Güvenlik stratejisi ve çıkarılan yasalar ile üye devletler arasında bir strandart yakalanmaya çalışılmaktadır. Ortak politika üretme çabası başarılı, fakat uygulamada sıkıntı yaratan bir yapı sergilemektedir.

2. Stratejilerin yönetimi kurumsal açıdan incelendiğinde, Finlandiya'da ulusal koordinasyonun çok güçlü olduğu ve buna yönelik güçlü örgütler kurulduğu gözlemlenmektedir. Bu kurumların karar alma süreçleri hızlı ve etkindir. AB' ye bakıldığında ise, siber güvenlik strateji ve politikalarını üretmede pek çok kurumun aktif rol aldığı söylenebilir. Fakat örgüt yapısının fazla olması, karar alma ve uygulama sürecini geciktirmektedir ve bürokrasinin geciktirici yanı ön plana çıkmaktadır.

3. Mevzuat açısından bakıldığında, Finlandiya'nın Ulusal Siber Güvenlik Yasası, AB direktiflerini en hızlı ve verimli biçimde uygulayacak şekilde tasarlanmış esnek ve güçlü yapıya sahiptir. AB' de de ise; NIS2 Direktifi, Siber Güvenlik Yasası, Siber Güvenlik yasasını destekleyici CRA, GDPR, DSA ve Yapay Zeka Yasaları oldukça başarılı, birlik çıkarları ile örtüşen, siber güvenlik hususunda çıkacak

herhangi bir krizde birliği yönlendirici güçlü yasalardır. Fakat uygulama istenilen düzeyde başarılı değildir ve üye ülkeler arasında farklılıklar gözlemlenmektedir.

4. Toplumun siber dayanıklılık düzeyi incelendiğinde, Finlandiya'nın siber güvenlik hususunda vatandaşları oldukça bilinçlidir ve verilen eğitimlerle farkındalık düzeyleri artırılmaktadır. "Toplum siber güvenlik alanında savunmanın en önemli parçasıdır" düsturu ile hareket edilmektedir. AB' de siber güvenlik alanında çeşitli eğitimler düzenlenmektedir fakat birlik içindeki ülkelerin siber güvenlik alanındaki bilinç ve eğitim düzeyi, ülkeden ülkeye değişiklik arz etmektedir.

5. Teknolojik alt yapıları açısından kıyaslandığında, Finlandiya siber alanda teknolojik alt yapının geliştirilmesine yoğun bir ilgi göstermiştir. Dijital teknolojileri kullanmadaki başarısından dolayı hayati nitelikte yüksek düzeyde entegre koruma sistemini oluşturmuştur. AB içinde bu konu oldukça önemlidir fakat yüksek düzeyli koruma sistemleri, AB'ye üye ülkeler açısından farklılık arz etmektedir. Bunun en önemli sebebi, ülkelerin teknolojik alt yapılarını geliştirmelerine yönelik yatırımların ve kapasitelerinin farklı seviyelerde olmasıdır.

6. Finlandiya özellikle Rusya tehdidinden dolayı AB ve NATO ile sıkı ilişkiler içerisindedir. Avrupa Birliği, küresel ölçekte NATO ve ABD ile yakın işbirlikleri kurmuştur. Fakat AB, geniş ölçekte küresel ağlara sahip olmasına ve birlik içindeki ülkeleri bütünleştirici politikalar üretmesine rağmen, üye ülkelerle ortak hareket etmediği müddetçe istenilen amaçlara ulaşmada zorlanacaktır.

Yukarıdaki karşılaştırmalı analizden hareketle AB ve Finlandiya'nın siber güvenlik stratejilerine ilişkin şu çıkarımlarda bulunulabilir: AB'nin, AB Siber Güvenlik Stratejisinde belirttiği önemli hedeflere ulaşabilmesi ve dijital yönetimin güçlendirilmesi için bazı yapısal ve uygulamaya ilişkin adımlarını kuvvetli hale getirmesi gerekmektedir. Öncelikli olarak metin içinde de vurgulandığı üzere, birliğe üye devletlerin arasında siber güvenlik politikaları arasında uyum sağlanması, politikaların aynı standartta uygulanması, gerçekleştirilmesi gereken son derece önemli bir adımdır Kamu-özel sektör iş birliği güçlendirilmelidir. Ortak siber savunma doktirini oluşturarak, aktif savunma kapasitesi kriz anlarında hazır ve güçlü halde bulundurulmalıdır. Yapay zeka destekli saldırılara hazırlık yapılması, geleceğe yönelik tehditlerin bugünden belirlenerek proaktif bir tutum sergilenmesi gerekmektedir. Kurumsal ve hukuki çerçeve, bu hedeflere ulaşmaya zemin hazırlayacak şekilde revize edilmeli ve etkin hale getirilmelidir. Teknik alt yapı ve insan kapasitesinin de belirlenen amaçlara uyumlu hale getirilmesi ve hazır bulundurulması gerekmektedir. Finlandiya Ulusal Siber Güvenlik Stratejisi, belirlediği hedefler doğrultusunda güçlü atılımlar gerçekleştirmekte ve dijital teknolojileri başarılı bir biçimde kullanmaktadır. Bu açıdan, Finlandiya Ulusal Siber Güvenlik Stratejisi, AB Siber Güvenlik Stratejisi'nin etkin uygulanmasının anahtarıdır ve entegrasyonunun artırılması gerekmektedir. Bu amaçlar doğrultusunda AB, küresel ölçekte rekabet edebilecek bir güç haline gelecektir. Aksi taktirde stratejiler "kağıt üzerinde güçlü ama uygulamada vasat" olma ihtimalini taşıyacaktır.

KAYNAKÇA

Admass, W. S., Munaye, Y. Y., ve Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, *2*, 100031.

Akarslan, H. (2012). *Bilişim suçları.* Ankara: Seçkin Yayıncılık.

Altın, O. (2023). AB'nin siber güvenlik alanındaki politikalarının ve uygulamalarının etkinliği: bir siber güvenlik temsilcisi olarak AB'nin yeterliliği. *Çankırı Karatekin Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *13*(2), 482-507.

Balay, R. (2004). Küreselleşme, bilgi toplumu ve eğitim. *Ankara Üniversitesi Eğitim Bilimleri Fakültesi Dergisi,* 37(2), 61-82.

Beltrán, M. (2025). AI algorithms under scrutiny: GDPR, DSA, AI Act and CRA as pillars for algorithmic security and privacy in the European Union. *Computers & Security*, 104628.

Çakmak, H. B., ve Demir, M. (2009). Katarakt ameliyatlarında bilgilendirilmiş onam. *Journal of Glaucoma-Cataract/Glokom-Katarakt*, *4*(2), 130-136.

Çevik, İ. (2023). Avrupa Birliği Dijital Hizmetler Yasası'nın değerlendirmesi. *Yıldırım Beyazıt Hukuk Dergisi*, (2), 387-419.

Cornish, P., Livingstone, D., Clemente, D., ve Yorke, C. (2010). *On cyber warfare* (pp. 21-22). London: Chatham House.

EGM (2025). *Siber suç nedir?* Erişim tarihi: 21 Ekim 2025, ***https://www.egm.gov.tr/siber/sibersucnedir***.

Ergene, G. Ç. (2024). *Avrupa Birliği Siber Dayanıklılık Yasası Yürürlüğe Girdi.* Erişim Tarihi: 12 Kasım 2025.***https://www.erdem-erdem.av.tr/bilgi-bankasi/avrupa-birligi-siber-dayaniklilik-yasasi-yururluge-girdi***.

Europen Commission (2025) *Cybersecurity*. Erişim tarihi: 21 Ekim 2025, ***https://digital*** strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

FI_ACTION_PLAN (2021). *Implementation plan for Finland's Cyber Security Strategy 2024-2035.* Erişim tarihi: 21 Ekim 2025, ***https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/action-plans/FI_ACTION_PLAN_2024_en.pdf***

Finland's Cyber Security Strategy (2013). *Finland´s cyber security strategy.* Erişim tarihi: 21 Ekim 2025, ***https://afyonluoglu.org/PublicWebFiles/strategies/Europe/Finland%202013%20Cyber%20Security%20Strategy-EN.pdf***

GDPR Madde1 (.2025). *General data protection regulation.* Erişim tarihi: 21 Ekim 2025, ***https://gdpr-info.eu/***.

Griffith, M. K. (2018). A comprehensive security approach: Bolstering Finnish cybersecurity capacity. *Journal of Cyber Policy*, *3*(3), 407-429.

haberler.com (2025, 21 Ekim). *AB güvenlik stratejisi üzerine uyarı: 'her geçen yıl geride kalıyoruz'.* Erişim tarihi: 28 Ekim 2025, ***https://www.haberler.com/guncel/ab-guvenlik-stratejisi-uzerine-uyari-her-gecen-yil-geride-kaliyoruz-19170250-haberi/***.

Igboanua, C. O., Sinkovics, R. R., ve Kuivalainen, O. (2025). The role of regional policy for Industry 4.0 adoption: A study of Finnish South Karelia. *European Management Journal*, 1, 1-11.

Michael, K., Herold, R. ve Roussos K. (2025). Security and regulation: Cybersecurity, privacy, and trust- protecting information and ensuring responsible technology use. *Computers & Security*. Available online 9 December 2025, 104804.

Ministry For Foreign Affairs To Finlad, (2025). *Cyber security and the cyber domain.* Erişim tarihi: 28 Ekim 2025, ***https://um.fi/cyber-security-and-the-cyber-domain***.

Ribeiro, D., Fonte, V., Ramos, L. F., & Silva, J. M. (2025). Assessing the information security posture of online public services worldwide: Technical insights, trends, and policy implications. *Government Information Quarterly*, *42*(2), 102031.

Ruohonen, J., Rindell, K., ve Busetti, S. (2025). From Cyber Security Incident Management to Cyber Security Crisis Management in the European Union. *arXiv preprint arXiv:2504.14220*.

Sağıroğlu Ş., ve Alkan, M. (2018). *Siber güvenlik ve savunma farkındalık ve caydırıcılık.* Ankara: Grafiker Yayınevi.

Saltzer, J. H., ve Schroeder, M. D. (1975). The protection of information in computer systems. *Proceedings of the IEEE*, *63*(9), 1278-1308.

Sandilaç, N. (2022). Siber suç, siber terör ve siber savaş üçgeninde siber dünya. *Bilişim Hukuku Dergisi*, *4*(1), 81-140.

Sayedi, S. O. (2020). *Ulusal siber güvenlik stratejisi oluşturma süreç analizi ve Türkiye İle Afganistan'ın ulusal siber güvenlik stratejisinin değerlendirilmesi.* Yüksek Lisans Tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne.

Stokes, D., ve Whitman, R. G. (2013). Transatlantic triage? European and UK 'grand strategy'after the US rebalance to Asia. *International Affairs*, *89*(5), 1087-1107.

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı (2016-2019). *2016-2019 Ulusal siber güvenlik stratejisi.* Erişim Tarihi: 18 Ekim 2025.***https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf***.

Tunca, S. (2019). Modern çağda siber güvenlik kavramı. *Dumlupınar Üniversitesi İİBF Dergisi*(*3-4*), 1-7.

Valtioneuvoston julkaisuja, (2023). *Valtioneuvosto*. Erişim tarihi: 21 Ekim 2025, ***https://julkaisut.valtioneuvosto.fi/items/647374c1-e029-476b-81c5-ba6267e6d1ab***

Wolfenstein, K. (2023). *Finlandiya Metaverse Stratejisi: AB ülkesi Finlandiya, 2035 yılına kadar genişletilmiş ve sanal gerçeklik (XR, VR, AR, MR) ile küresel bir öncü olmak istiyor.* https://xpert.digital/tr/finlandiya-meta-veri-dizisi/

Review Article

Dijital Yönetimlerin Siber Güvenlik Stratejileri: AB ve Finlandiya İncelemesi

Cybersecurity Strategies of Digital Administrations: A Review of The EU and Finland

Elif EKİNCİ ÖZYARDIMCI
Dr. Öğr. Üyesi, Erzincan Binali Yıldırım Üniversitesi
İktisadi ve İdari Bilimler Fakültesi
eekinci@erzincan.edu.tr
https://orcid.org/0000-0002-5067-5685

Extended Summary

The incredible advancements in information and communication technologies, especially in recent years, have expanded and fundamentally transformed the infrastructure of many fields. Parallel to these developments, serious security problems have also emerged. Cybersecurity, concerning the protection and security of information systems, has become a focal point for many experts, engineers, researchers, and managers, and is a significant issue raising concerns for the future. Creating a safer internet environment and ensuring the security of information systems has become one of the most important security challenges of our time. The penetration of the internet into every aspect of human life has placed significant responsibilities on individuals, societies, institutions, states, and international organizations in creating reliable online platforms, and "internet security" has prompted all stakeholders to take greater precautions. Today, the adoption of information and communication technologies and the implementation of development policies are the most fundamental goals of governments and international organizations at the national and global levels. This study examines the impact of increasingly complex cyber threats on public administration and policy-making processes, using the examples of the EU and Finland. The effectiveness of cybersecurity strategies at the national and global levels, the extent to which they influence each other, and how Finland's leading position in cybersecurity among other EU countries affects the EU's overall position in this area will be evaluated in the conclusion. Examining the Finland-EU relationship in the context of how cybersecurity strategies influence and improve each other will make a significant contribution to the literature. EU cybersecurity strategies pursue policies that protect citizens and organizations within its borders from cyber threats and dangers, and promote the use of reliable information and communication technologies. The European Commission and Security Policy have announced the renewed EU cybersecurity strategy. Aiming to ensure the protection of fundamental rights and freedoms in the cyber realm, the EU proposes a model based on global cooperation and governance, alongside principles such as cooperation with states and international organizations on the international stage, the protection of personal and public data, and the guarantee of freedom of expression. The strategy emphasizes the need for governments, the public, NGOs, and private sector organizations to cooperate and share responsibility for achieving this goal. The EU has linked its digital sovereignty and supremacy to the robustness of all related services and tools. It has emphasized the need for law enforcement, politicians, national bodies, and the four separate cyber communities linked to defense to act together and achieve governance against cyberattacks and threats. It has been reiterated that comprehensive action against cyberattacks will strengthen the EU. This strategy aims for joint action against potential major cyberattacks and threats. The NIS2 Directive, the Cyber Resilience Act, the Digital Services Act, the General Data Protection Regulation (GDPR), and the Artificial Intelligence Act form the basis of the Union's efforts to establish a comprehensive framework for digital security. While it is true that the EU is a significant global

representative in the field of cybersecurity, this understanding also contains shortcomings. The underlying factors in this situation are the failure to establish a shared vision among member states of the Union in the field of cybersecurity. To this end, the Union has pledged to pursue more effective policies, both as an organization and among its member states, to achieve consensus and increase its effectiveness in the field of cybersecurity, thus guaranteeing a more intensive performance process. In this context, it is planned to improve the effectiveness of cybersecurity strategies by working on legal regulations and practices. In line with these views, support from the best in cybersecurity policies and strategies among EU member states will bring the European Union to a significant position in the field of cybersecurity; therefore, examining the example of Finland, which has been very successful in this area, and analyzing its strategy is of great importance for this study.

From the perspective of cybersecurity policies, Finland holds a leading position globally in cybersecurity technology. The Finnish Cybersecurity Strategy, first prepared in 2013, reported that Finland was in a rather inadequate and vulnerable position in the information society, considering the use of information networks and systems, infrastructure development, and the potential for disruptions. On February 15, 2022, the Finnish Ministry of Internal Affairs and Defence launched a project to evaluate existing and future plans and initiatives for combating cybercrime, ensuring national cybersecurity, and protecting society against all kinds of events and crises that threaten cybersecurity, thereby criticizing existing national cybersecurity policies. Finland has published its new National Cybersecurity Strategy and Implementation Plan covering the years 2024-2035. The aim of this new strategy and plan is to ensure the security of individuals and society, to ensure the smooth operation of cyber systems, and to be able to respond to cyber threats at any time. Finland also aims to strengthen cybersecurity by participating in international discussion platforms and by increasing and developing collaborations in this field. Finland's 2024–2035 National Cybersecurity Strategy is designed in line with EU regulations such as the Cyber Resilience Act, the Artificial Intelligence Act, and the NIS2 Directive. Some of the ultimate goals of this law are: to develop a national character in the field of cryptography technology, to harmonize this technology by making it compatible with EU and NATO cryptography products, and thus to make Finland a country capable of responding to NATO and EU information security systems. Some of the objectives of Finland's 2024-2035 Cybersecurity Strategy are: developing networking and collaboration in the advancement of cybersecurity; conducting effectiveness analyses in cybersecurity policy; developing cybersecurity expertise within society; increasing national data protection capabilities, establishing necessary encryption methods, and protecting data integrity; making forward-looking plans for cybersecurity today and predicting the future, and creating a plan of international standard; establishing a joint fund for cybersecurity studies and research; ensuring sufficient funding for project participation; strengthening EU and NATO development funds; nationalizing the defense and cybersecurity sector; establishing a cybersecurity cooperation network; supporting the work of the Finnish Internet Centre; and supporting all efforts to raise public awareness about cybersecurity, thereby facilitating/improving communication and cooperation against cyber threats affecting different population groups. In this respect, Finland represents one of the most harmonious national model examples in Europe. The country has positioned cybersecurity not only as a technical defense area but also as an indispensable component of democratic governance and economic sustainability. Finland's strategy is based not only on defensive reflexes but also on preventive mechanisms. The implementation plan, which is audited and updated annually, has created an active governance model; it has involved public, private sector and civil society stakeholders in the process. This structure, developed through cryptography, artificial intelligence, data management and national certification systems, presents an exemplary national model operating in full compliance with EU standards. There is a complementary relationship between the normative framework established by the EU and Finland's practice-based governance model. While the EU is seeking to strengthen its digital sovereignty by developing common law and standards in cybersecurity, Finland is implementing this vision concretely at the national level. The mutual compatibility of these two structures will enable Europe to achieve a more resilient and sustainable position in the global cybersecurity architecture. Finland is a key player in combating cyber threats and fostering cooperation.