Journal of Information Systems and Management Research
Bilişim Sistemleri ve Yönetim Araştırmaları Dergisi

http://dergipark.gov.tr/jismar

Araştırma Makalesi / Research Article

Birleşik Krallık'ın Siber Güvenlik Politikasını Güç ve Caydırıcılık Üzerinden Anlamlandırmak

İbrahim Çağrı ERKUL*,a

[a,*] *Osmaniye Korkut Ata Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Uluslararası İlişkiler Bölümü, Osmaniye, Türkiye*

MAKALE BİLGİSİ

Alınma: 02.05.2024
Kabul: 04.06.2024

Anahtar Kelimeler:
Birleşik Krallık, Siber Güvenlik, Siber Caydırıcılık, Siber Uzay.
Sorumlu Yazar
e-posta:
ibrahimcagrierkul@osmaniye.edu.tr

ÖZET

Bilgisayar korsanlarının eylemlerinin ve yetkinliklerinin anlaşılmasına paralel olarak, 1980'li yıllarda siber uzayın Birleşik Krallık tarafından güvenlikleştirilmeye başlandığı görülmüştür. Web sitelerinin oluşturulmasının ardından tehdidin çeşitlenmesi ise siyasetin hem ulusal hem de uluslararası alanda konuya odaklanmasını mümkün kılmıştır. 1990'lı yılların hemen başında siber güvenliğin sağlanması noktasında kurumsallaşmaya yönelik adımlar atılmış olsa da siber saldırıların etkileri, hükümet ve çeşitli sektörler üzerinde hissedilmeye devam etmiştir. 2000'li yıllarda ise Birleşik Krallık siber uzayda gerçek bir anarşinin hüküm sürdüğü gerçeğiyle yüzleşerek, siber saldırılar karşısındaki savunmasızlığını giderecek siber güvenlik stratejileri belirlemek durumunda kalmıştır. Bu yönüyle makale, siber uzayın Birleşik Krallık için önemli hale gelme sürecini de dikkate alarak, 2009 ve sonrasında açıklanan siber güvenlik stratejileri üzerinden Birleşik Krallık'ın siber güvenlik politikasını ve siber yetkinliklerini analiz etmeyi amaçlamaktadır. Makale, realist bir perspektif üzerinden Birleşik Krallık'ın siber güvenliğini yalnızca savunmada kalarak elde etmesinin mümkün olmadığını ortaya koyarak, siber caydırıcılık ve saldırı kapasitesini realist temelde artırmasının gerekli olduğu iddiasındadır. Makalede realist anlayışa bağlı olarak arttırılması gereken siber güç ve saldırı kapasitesine rağmen siber uzayda dost ve müttefik aktörlerle iş birliğinin gerekliliği üzerinde de durulmuştur.

DOI: 10.59940/jismar.1477284

Interpreting the UK's Cyber Security Policy in Terms of Power and Deterrence

ARTICLE INFO

Received: 02.05.2024
Accepted: 04.06.2024

Keywords:
United Kingdom, Cyber Security, Cyber Deterrence, Cyberspace.
Corresponding Authors
e-mail:
ibrahimcagrierkul@osmaniye.edu.tr

ABSTRACT

In the 1980s, in parallel with understanding hackers' actions and capabilities, the United Kingdom (UK) began securitizing cyberspace. The diversification of the threat following the use of websites has made it possible for politicians to focus on cyberspace both nationally and internationally. Although institutionalization steps were taken to ensure cyber security in the early 1990s, the effects of cyber attacks impacted the government and various sectors. In the 2000s, the United Kingdom had to face the fact that there was absolute anarchy in cyberspace and determine cyber security strategies that would eliminate its vulnerability to cyber-attacks. In this respect, the article aims to analyze the UK's cyber security policy and cyber competencies through the cyber security strategies announced in 2009 and later, considering how cyberspace has become important for the UK. From a realistic perspective, the article claims that the UK can't achieve cyber security only through cyber defense and that it is necessary to increase her cyber deterrence and attack capacity on a realistic basis. The article also focuses on the necessity of cooperation with friendly and allied actors in cyberspace, even though the UK needs to increase its cyber power and attack capacity based on a realistic approach.

DOI: 10.59940/jismar.1477284

1. GİRİŞ *(INTRODUCTION)*

Birleşik Krallık Kabine Ofisi'nin 2009'da parlamentoya sunulması için hazırladığı bir strateji belgesinin sonuç bölümünde yer alan "*Nasıl ki 19. yüzyılda ulusal güvenliğimiz ve refahımız için denizleri, 20. yüzyılda havayı güvence altına almamız gerekiyorsa, 21. yüzyılda da siber uzaydaki konumumuzu güvence altına almamız gerekiyor*." [1] ifadesi, siber uzayın Birleşik Krallık için ne kadar önemsendiğini ortaya koymak açısından önemli bir kalkış noktası oluşturmaktadır. Buradan hareketle, Birleşik Krallık için siber uzayın güvenli hale getirilmesi sahip olunan büyük güç statüsünün devamı için de hayati bir yere sahiptir.

Birleşik Krallık'ın siber uzaya verdiği önem ve bu alanda güvenliğini sağlayabilmek için ortaya koyduğu çaba, 1980'li yıllara kadar geri gitmektedir. Zaman içerisinde siber tehdidin çeşitlenmesi ve bu alanda yetkinliklerini arttıran aktörlerin yapabilecekleri tahribatın anlaşılması, Birleşik Krallık'ın mevcut kurum ve yatırımlarla siber uzayda güvende kalamayacağını açıkça ortaya koymuştur. Devlet ve devlet destekli siber saldırılar başta olmak üzere tüm siber saldırılara karşı hazır olma ve bunlara cevap verebilecek bir siber kapasiteye sahip olma isteği, Birleşik Krallık'ın siber uzaya yaptığı kurumsallaşma çabalarının yanında, yatırımlarını da belirli stratejiler çerçevesinde gerçekleştirmesini gerekli kılmıştır.

Siber saldırıya uğrayan devletin, saldırının failini cezalandırılma ihtimalinin uluslararası hukuk nezdinde düşük olduğu dikkate alındığında, siber uzay anarşinin hüküm sürdüğü bir alan olarak değerlendirilebilir. Bu anarşi ortamında dost ve müttefik aktörler arasında ikili ve kurumsal temelde iş birliği imkânlarının önemsenmesi gerekmekle birlikte, Birleşik Krallık'ın başlıca tehdit aldığı Rusya, Çin, Kuzey Kore ve İran'a karşı realist bir temelde (saldırı ve caydırıcılığı da içerecek şekilde) oluşturulacak siber strateji izlemesi elzemdir.

Birleşik Krallık hem siber uzaydaki savunmasızlığını azaltmak ve caydırıcı olmak hem de bu alanda lider aktörlerden biri olabilmek amacıyla açıkladığı siber güvenlik stratejilerinin bir bütün olarak anlaşılmasını sağlamanın yanında, Birleşik Krallık'ın niçin realist temelde bir siber güvenlik stratejisi izlemesi gerektiğini gerekçelendirmeye çalışan bu makale, giriş ve sonuç bölümleri dışında üç bölümden oluşmaktadır. İlk bölümde siber uzayın Birleşik Krallık için önemli hale gelme süreci güvenlikleştirme kavramı ve yaşanan siber saldırılar üzerinden değerlendirmeye tabi tutulmuştur. İkinci bölümde ilki 2009'da açıklanan siber güvenlik strateji belgeleri üzerinden, Birleşik Krallık'ın siber güvenlik politikaları siber saldırılar, siber kapasite ve bu alandaki kurumsallaşmayı da içerecek şekilde detaylıca incelenmiştir. Son bölümde ise Birleşik Krallık'ın siber alanda izlediği/izlemesi gereken küresel iş birliğinin mümkün ve gerekli olduğu kabul edilerek, Birleşik Krallık için siber caydırıcılığı merkeze alan realist bir yaklaşımın gerekliliği ortaya koyulmuştur.

2. SİBER UZAYIN BIRLEŞİK KRALLIK İÇİN ÖNEMLİ HALE GELME SÜRECİ *(THE PROCESS OF CYBERSPACE BECOMING IMPORTANT FOR THE UNITED KINGDOM.)*

Siber casusluğun ilk örneklerinden biri olarak, 1986'da Lawrence Berkeley Ulusal Laboratuvarı'nın muhasebe sistemindeki küçük bir tutarsızlığın izini süren Clifford Stoll ve iş arkadaşları, tutarsızlığın sebebine yönelik olarak yaptıkları araştırmalarında, ABD'den bilgi çalarak KGB aracılığıyla Sovyetler Birliği'ne satan ve Batı Almanya'da ikamet eden bir bilgisayar korsanına ulaşmışlardır [2]. Yaşanan bu casusluk olayı, aktörlerin dikkatlerini dijital casusluğa çevirmelerini beraberinde getirmiştir.

Aynı dönemde Birleşik Krallık'ta siber güvenlik, bankacılık sektörü üzerinden ön plana çıkmaya başlamıştır. Bankaların bu noktada güvenliklerine yatırım yapmalarına rağmen bilgisayar dolandırıcılığı sebebiyle güvende olmadıkları ve büyük meblağlarda kayıp yaşadıkları iddia edilmiştir. Ortaya çıkan bu yeni tehdide karşı Birleşik Krallık'ta faaliyet gösteren çok sayıda banka, bilgisayar dolandırıcılığına karşı araştırma yapma ve bilgi paylaşımını içeren bir koordinasyon mekanizmasına dahil olmuştur. Yaşanan gelişmelere ve sektörde yaşanabilecek sorunların ortaya koyulmasına paralel olarak, bilgisayar güvenliğini sağlamak ve yönetmek, 1980'lerin ikinci yarısında Birleşik Krallık'ta giderek daha karmaşık bir hale gelmiştir [3].

1980'lerin sonlarında ise bilgisayar güvenliğine ilişkin konular, Birleşik Krallık'ta en üst düzeyde siyasetin gündemine gelmiştir. Bunda bilgisayarların artık yalnızca bilgi saklayan araçlar olmaktan çıkarak, operasyonel olarak çok sayıda sektörde kilit rol oynamaya başlaması önemli olmuştur. Finans sektörünün operasyonlarını baltalamaya yönelik kötü niyetli girişimlere bağlı olarak ortaya çıkan tehditler de Birleşik Krallık'ta farkındalığı arttırmıştır. Bankalar bilgisayar virüslerine karşı güvende olmak için büyük yatırımlar yapmayı gerekli görmüşlerdir [3]. Bu dönemde yaşananlarla Birleşik Krallık'ta siber uzay güvenlikleştirilmeye başlamıştır.

Barry Buzan'ın ifadesiyle güvenlikleştirme "*Güvenlikleştirme, bir şeyin, değerli olduğu kabul*

edilen bir öznenin varlığına yönelik bir tehdit olarak kurgulanması ve bu kurgulamanın buna mukabil alınan istisnai tedbirleri desteklemek için kullanılmasıdır." Diğer bir ifadeyle güvenlikleştirme, daha önce tehdit olarak görülmeyen bir konunun artık tehdit olarak kabul edilmesi ve bu tehdidin, zihni yönden inşa edilmesi olarak belirtilebilir [4]. Bu açıdan bakıldığında Birleşik Krallık, kendi varlığına yönelik olarak siber uzayda ortaya çıkan tehdidi güvenlikleştirmeye başlayarak, bu konuda atacağı adımları da halk nezdinde gerekçelendirme çabası içinde olmuştur.

Ayrıca şu da belirtilmelidir ki 1980'li yıllarda bilgisayar etiği konusu, ABD ve Birleşik Krallık'ta çok sayıda bilim insanının ilgisini çekmiştir. Bu konuya akademik anlamda odaklanılması, konuyu toplumun gündemine de taşımıştır [5]. Diğer taraftan en başından itibaren Birleşik Krallık'ın siber saldırıların yalnızca mağduru olmadığı, aynı zamanda bu saldırıları gerçekleştirdiği de unutulmamalıdır. CERN'deki bilim insanlarının ilk web sitesini oluşturmalarının hemen ardından birçok aktör, ağlar üzerinden gerçekleştirilebilecek casusluk faaliyetlerine yönelik bilgi sahibi değildi. İşte bu noktada Birleşik Krallık ortaya çıkan bu fırsatı değerlendirmiş ve ilk hedeflerinden biri olarak, Pakistan'ın nükleer programını seçmiştir. Bu programda çalışan bilim insanları, Birleşik Krallık Hükümet İletişim Merkezi[1] karşısında savunmasız kalmıştır [6].

Birleşik Krallık'ta gerçekleşen ilk siber suçlara bağlı olarak bu konuda yasal düzenleme yapılması kaçınılmaz hale gelmiştir. Bu bağlamda 29 Haziran 1990'da Bilgisayar Kötüye Kullanma Yasası kabul edilmiştir. Yasa metni incelendiğinde bilgisayar ve verilere yetkisiz erişimin ön planda olduğu belirtilmelidir. Ayrıca bu yasada cezai yaptırımların da detaylı bir şekilde düzenlendiği dikkate alınırsa, yasanın suç işleme niyetinde olanlar için caydırıcı bir yönü de bulunmaktaydı [7].

1990'lı yıllar web siteleri üzerinden siber güvenliği farklı bir noktaya taşımıştır. Bu noktada hacktivism Birleşik Krallık'ın siber suçlara yönelik farkındalığını arttıran bir diğer eylem olarak değerlendirilebilir. Birleşik Krallık'ta yaşanan ilk hacktivist olay, 1994 yılında "Zippies" ismindeki Kaliforniyalı grubun dönemin başbakanı John Major'un açık havada yapılacak gösteri ve festivallerine yönelik yasaklama kararı sonrasında, Birleşik Krallık'taki web sitelerini çökerten bir siber saldırı gerçekleştirmesiyle meydana gelmiştir [8]. Bireysel veya grup halinde hareket eden internet korsanlarının siyasi tepkilerini ortaya koymak için gerçekleştirdikleri eylemler, devlet düzeyinde sahip olunan imkân ve tecrübeden yararlanılması durumunda, casusluk da dahil olmak üzere karşılaşılabilecek zararlar üzerinde düşünülmesini gerekli kılmıştır.

Geleneksel yöntemlerle gerçekleştirilen casusluk, halen Birleşik Krallık için bir tehdit olmakla birlikte, iletişim alanındaki küresel gelişmeler siber uzayın bir casusluk aracı olarak kullanılmasını da beraberinde getirmiştir. Siber uzayın casusluk eylemleri için önemi, siber casusluğun güvenli bir mesafeden operasyon yapılmasını mümkün kılması ve saldırıları yapanlara suçlama atfedilmesini zorlaştırmasıyla ilişkilidir. Böylece aktörlerin casuslukla bağlantılı siyasi sorumluluk/suçlama riski de minimize edildiği için [9] siber casusluk yaygın olarak kullanılmaya başlanmıştır. Birleşik Krallık siber casusluğu hem uygulayan hem de bu konudan mustarip olan bir aktör olarak nitelendirilebilir.

Siber alanda yaşanabilecek güvenlik sorunlarına karşı, Birleşik Krallık'ın görece erken bir dönemde önlemlerini almaya başlaması önemlidir. Bu bağlamda Birleşik Krallık hükümeti ilk bilgisayar güvenliği ekibini 1992 yılında UNIRAS (Birleşik Olay Müdahale ve Uyarı Hizmeti) ismiyle kurmuştur. Ancak ekibin kurulduğu ilk dönemde nasıl bir görev yaptığı anlaşılamadığı için büyük ölçüde işlevsiz kalmıştır. Diğer taraftan Birleşik Krallık, gelebilecek saldırılara yönelik temkinli olması nedeniyle, parlamento yetkililerinin ofislerinden internete erişmelerine müsaade edilmemiştir. Tony Blair'in 1997'de başbakan olmasından sonra ise bu uygulama kaldırılmıştır. Şu husus ayrıca ifade edilmelidir ki Birleşik Krallık Hükümeti'nin internete Amerikalılardan daha geç ulaşması[2], siber güvenlik konusunda daha fazla düşünebilmesi için de bazı fırsatlar sunmuştur. ABD'nin 1990'lı yıllarda bilgisayar korsanları için Birleşik Krallık'a nazaran daha ilgi çekici bir hedef olması, Birleşik Krallık için güvenli internetin sağlanması noktasında önemliydi. Çünkü bu dönemde hükümet siber uzayı araştırırken, karşılaşılabilecek tehlikelerin de farkına varmaya başlamıştır. Bu farkındalığa rağmen kısa süre sonra Çin kaynaklı olduğu düşünülen siber saldırılar, hükümeti ve havacılık sektörünü etkilemeye başlamıştır [6].

2000'li yılların ortalarına gelindiğinde, Birleşik Krallık Ulusal Altyapı Güvenliği Koordinasyon

[1] Government Communications Headquarters (GCHQ).

[2] Hükümet yetkililerinin ofislerinde internet kullanmaları açısından.

Merkezi[3] bir süredir devam eden siber saldırıların, son dönemde karmaşıklığının arttığı uyarısında bulunmuştur. Bu dönemde aralarında savunma, iletişim ve hükümet sistemlerinin yer aldığı yüzlerce devlete bağlı kurum ve kritik kabul edilebilecek işletmenin hedef alındığı dikkate alınmalıdır [6]. Bu saldırıların Çin merkezli olduğu ve aralarında ABD'nin de olduğu çok sayıda devleti etkilediği not edilmelidir.

Her ne kadar MI5[4] Çin'in siber saldırılarına yönelik görüşünü 2007'de belirtmiş olsa da Birleşik Krallık'ın Çin'den aldığı siber tehdit, MI5'ın 2008'de hazırladığı bir raporla görünür hale gelmiştir. 2009'da Ortak İstihbarat Komitesi[5] de Çin'in Birleşik Krallık'a yönelik siber saldırılarıyla ilgili bir uyarıda bulunmuştur. Devam eden süreç içerisinde Çin'den alınan siber tehdit, Birleşik Krallık tarafından resmi olarak tekrar tekrar vurgulanmıştır [10]. Bu dönemde Birleşik Krallık karşılaştığı siber saldırılarla, siber uzayda gerçek bir anarşinin hüküm sürdüğünü tecrübe etmek durumunda kalmıştır. Kısaca anarşinin hüküm sürdüğü bir alanda pasifist[6] olmak, gerçeklikten kopmak anlamına geleceği için Birleşik Krallık siber uzaya realist temelde bakmak mecburiyetini hissetmiştir.

Realist teorinin önemli isimlerinden Thomas Hobbes, anarşi kavramını açıklarken kullandığı Leviathan'ı her ne kadar yerel toplumlara yönelik kullansa da ortaya koyduğu fikirlerinin uluslararası politikayı da kapsadığı ileri sürülebilir. Uluslararası politikada düzeni sağlayacak bir Leviathan'ın (egemen gücün) yokluğunda ortaya çıkacak anarşinin, beraberinde getireceği savaş/çatışma ise kaçınılmaz olacaktır. Devletlerin böyle bir ortamda güvenliklerini sağlayabilmeleri için ihtiyaç duydukları şey güçtür. Haliyle devletlerin güçlerini artırarak güvenliklerini sağlama yoluna gitmeleri ise bir zorunluluk olarak görülür [12].

Şu husus vurgulanmalıdır ki realist bakış açısıyla savaş, küresel siyasal kültürün bir parçası olarak kabul edilmiştir. Bahsi geçen siyasal kültüre göre savaştan kaçmak değil onunla baş etmek ve savaştan sağ çıkmak esastır [13]. Bu bağlamda gelinen noktada Birleşik Krallık için en iyi tercih siber uzayda yaşanabilecek "savaşlardan" kaçınmak değil, bu savaşlardan sağ çıkmak olacaktır. Siber savaşlardan sağ çıkabilmek için ise ortaya koyulacak gerçek bir iradenin yanında siber stratejilere de ihtiyaç duyulmuştur.

3. SİBER GÜVENLİK STRATEJİ BELGELERİ BAĞLAMINDA BİRLEŞİK KRALLIK'IN SİBER GÜVENLİK POLİTİKASI *(CYBER SECURITY POLICY OF THE UNITED KINGDOM IN THE CONTEXT OF CYBER SECURITY STRATEGY DOCUMENTS)*

Birleşik Krallık'ın ilk siber güvenlik strateji belgesini 2009'da ortaya koyduğu dikkate alındığında, ilk ulusal siber güvenlik stratejisini 2003 yılında yayınlayan ABD'nin zamansal olarak gerisinde kaldığı ileri sürülebilir. 11 Eylül 2001'de gerçekleşen terör saldırıları, bu noktada ABD için motive edici olmuşken, Birleşik Krallık için ise 2007'de Estonya'ya karşı gerçekleştirilen siber saldırılar, siber uzayda karşılaşılabilecek zorlukları görünür kılmış ve siber güvenlik stratejisinin ilan edilmesinde dikkate alınmıştır [14].

Estonya'nın 2007'de II. Dünya Savaşı'nda ölen Sovyet askerleri anısına inşa edilen bir anıtı, şehir merkezinden kaldırarak kenar mahallelere taşıma kararı almasının hemen ardından, Estonya'da Rusça konuşan topluluk eş zamanlı olarak fiziksel bir isyan başlatmıştır. Estonyalı yetkililere göre arkasında Rusya'nın olduğu bu siber saldırı, Estonya'yı hedef almıştır. Başlatılan siber saldırıyla 85 bin bilgisayar hacklenmiş ve önemli kabul edilebilecek 58 web sitesi de ele geçirilmiştir [15]. Siber alandaki en karmaşık tehditlerin farklı teknikleri bir arada kullanan ve siber kapasiteleri yüksek olan devletler tarafından yapıldığının [1], Estonya'da yaşananlarla bir kez daha görülmesi, Birleşik Krallık'ın da devleti merkeze alan bir siber güvenlik stratejisi ile sürece adım atmasına gerekçe olmuştur.

Ayrıca 2009'da hükümetin, Birleşik Krallık çıkarlarının siber operasyonlara karşı savunmasızlığını ve siber operasyonların Birleşik Krallık çıkarları üzerindeki etkisini azaltma hedefinde olunduğunun belirtilmesi önemlidir [1]. Bu noktada siber uzay kavramının ağ bağlantılı her türlü dijital etkinliğin yanında, dijital ağlar üzerinden gerçekleşen eylemleri de kapsadığı dikkate alındığında [1], güvenlik ihtiyacının ne kadar geniş bir alanda sağlanması gerektiği ve Birleşik Krallık'ın bunu başarabilmek için gerçek bir iradeye ihtiyaç duyduğu açıktı.

Bu dönemde konunun ne kadar ciddiye alındığının görülmesi bakımından, Birleşik Krallık'ın en yüksek önceliğe sahip ulusal güvenlik konusu olarak kabul

---

[3] The National Infrastructure Security Co-ordination Centre (NISCC).
[4] Military Intelligence, Section 5 (MI5).
[5] Joint Intelligence Committee (JIC).

[6] Keane'nin belirttiği üzere pasifizm "*şiddetle karşı karşıyayken bile, şiddete başvurmayı açıkça ve ilkeli bir tarzda reddetmek*" şeklinde tanımlanırsa [11] pasifist bir yaklaşımın caydırıcılığı tamamen sonlandıracağı açıktır.

ettiği siber güvenliğin ekonomiyi[7] de kapsaması [9], Birleşik Krallık için iş dünyasını siber anlamda güvenli kılınmasının önemini ortaya koymuştur. 2011'de açıklanan "Birleşik Krallık Siber Güvenlik Stratejisi: Birleşik Krallık'ı Dijital Dünyada Korumak ve Desteklemek" başlığını taşıyan siber güvenlik strateji belgesinde, 2015'e kadar ulaşılması istenen bazı hedefler belirlenmiştir. Buna göre Birleşik Krallık'ın siber suçlarla mücadele ve siber uzayda iş yapmak için dünyanın en güvenli yerlerinden biri olması, siber saldırılara karşı dayanıklı ve siber uzaydaki çıkarlarını daha iyi koruyabilecek bir konuma gelmesi, Birleşik Krallık halkının güvenle kullanabileceği ve açık toplumları da destekleyen açık, istikrarlı ve canlı bir siber alana sahip olmasına destek olunması ve Birleşik Krallık'ın siber güvenlik hedefleri için ihtiyaç duyduğu ortak bilgi, beceri ve yeteneğe ulaşması hedeflenmiştir [17]. Burada siber güvenliğin ancak bütüncül bir yaklaşımla sağlanabileceğinin altının çizilmesi önemlidir.

2011'de dönemin başbakanı David Cameron'un hükümetin yayınladığı yeni siber güvenlik stratejisine yönelik olarak ifade ettikleri önemlidir:

> *"İnternet şüphesiz sosyal ve politik faydaya yönelik bir güç ve ekonomimizin büyümesi açısından da hayati önem taşıyor olsa da güvenliğimize yönelik tehditlere karşı korunmamız gerekiyor. Bu strateji yalnızca teröristlerin ulusal güvenliğimize yönelik tehdidini değil, aynı zamanda refahımızı tehdit eden ve siber suçlar yoluyla birçok sıradan insanın hayatını mahveden suçluları da ele alıyor. Siber güvenlik hükümet için en önemli önceliklerden biridir ve Birleşik Krallık'ın iş yapmak için dünyadaki en güvenli yerlerden biri olarak kalmasını sağlamak için polis, güvenlik hizmetleri, uluslararası ortaklar ve özel sektörle yakın iş birliği içinde çalışmaya devam edeceğiz*" [18].

Açıklanan siber güvenlik stratejisine bağlı olarak, Birleşik Krallık'ın siber güvenlik için ayırdığı bütçede de bir artış yapılmıştır. Buna göre 2011-2012 döneminde 105 milyon Pound olan bütçe, 2012-2013 döneminde 155 milyon Pound'a yükseltilmiştir. 2011-2015 yılları arasında ayrılan kaynağın toplam 650 milyon Pound olduğu da dikkate alınırsa, bu dönemde hükümet siber güvenlik için artan oranlarda kaynak ayırmaya devam ettiği görülecektir [18].

Birleşik Krallık, Soğuk Savaş döneminde diğer birçok aktör gibi büyük ölçüde öngörülebilir bir biçimde askeri veya nükleer tehditlerle karşılaşmıştır. Soğuk Savaş döneminde hissedilen bu varoluşsal tehdit, öngörülebilirliği üzerinden değerlendirildiğinde, bugün tehditlerin öngörülmesi zorlaşmıştır. Bugünün uluslararası ilişkilerinde aktörler geleneksel savaştan daha ucuz,[8] daha kolay erişilebilir ve daha az suçlama yapılabilecek/atfedilebilebilecek tehdit ve saldırı araçları arayışındadırlar. Buna bağlı olarak düşman tanımlaması farklılaştığı gibi, karşılaşılan tehditler de çeşitlenmektedir. Bu tehditlerin arasında siber saldırı ve kritik hizmetlerin kesintiye uğratılması da yer almaktadır [9]. Tüm dünyada siber güvenlik çekincelerini artmasına sebep olan Stuxnet saldırıları, Birleşik Krallık'a kritik alt yapı güvenliğinin önemini bir kez daha hatırlatmıştır.

Stuxnet kötü amaçlı yazılımı üzerinden İran'ın nükleer tesislerine yönelik gerçekleştirilen saldırıların sorumluluğunu hiçbir grup veya ülke üstlenmemesine rağmen uzmanlar gelişmiş ve karmaşık yapısı üzerinden Stuxnet'in bir devlet tarafından geliştirilmiş olması gerektiğine inanmışlardır. Bu bağlamda ABD, İsrail, Birleşik Krallık, Rusya, Çin ve Fransa Stuxnet'i geliştirebilecek maddi ve teknik becerilere sahip ülkeler arasında değerlendirilmiştir. İran'ın Stuxnet sebebiyle NATO'nun yanında özellikle ABD ve İsrail'i suçladığı da not edilmelidir [20].

Stuxnet saldırıları iki ayrı sebeple önemli kabul edilebilir: Stuxnet enerji ve diğer birçok endüstriyel kontrol merkezindeki sistemlerin ne kadar savunmasız olduğunu ortaya çıkarmıştır. Kritik alt yapı unsurları da benzer sistemlere sahip olduğu için siber saldırılara karşı güçlendirilmesi gerekli hale gelmiştir. İkinci olarak Stuxnet gibi kötü amaçlı yazılımlar, diğer aktörler tarafından kopyalanmasının ardından geliştirilerek yeni bir siber silah olarak farklı amaç ve hedefler üzerinde kullanılabileceği unutulmamalıdır [21].

Birleşik Krallık'ta 1980'ler ve 1990'larda gerçekleştirilen özelleştirilmelerden önce devletin ulusal kritik alt yapı unsurları üzerinde doğrudan kontrolü az olmakla birlikte, devam eden süreçte ulusal kritik altyapı unsurlarının büyük ölçüde özel sektöre geçmesi ve özel sektör tarafından işletildiği [22] dikkate alındığında, tehlike ve Birleşik Krallık'ın sorumluluğu daha net görülecektir. Osborne'un belirttiği üzere yalnızca elektrik alt yapısının işlevsiz kalması durumunda bile bankalar ve hastanelerin çalışmayı durdurması veya hükümetin kendisinin

---

[7] Birleşik Krallık'ın ekonomik sebeplerle siber güvenliği önemsemesi fazlasıyla anlaşılabilir. Örneğin kötü amaçlı bir yazılım olan "NotPetya", bir Birleşik Krallık şirketi olan Reckitt Benckiser'i 120 milyon Pound zarara uğratmıştır [16].

[8] Son dönemde bazı bilim insanları ve politikacılar arasında konvansiyonel savaş hazırlıklarının fazlasıyla maliyetli olduğu ve bu maliyete rağmen hazırlıkların ulusal güvenliğe olumsuz etkide bulunduğu yönündeki düşünce yaygınlaşmaktadır [19]. Bu noktada siber uzayda yaşanabilecek savaşlara karşı yapılacak hazırlıklar önemli bir alternatif olarak ön plana çıkmaktadır.

artık faaliyet gösteremeyecek bir hale gelmesinin oluşturduğu etki, Birleşik Krallık toplumunu felakete sürükleyebilir. Bu sebeple Birleşik Krallık'ın kritik sektörlerin korunmasına yönelik sorumluluğu olmakla birlikte, bahsi geçen sektörlerdeki şirketlerin de kendi siber dayanıklılıklarını sağlama sorumluluğu bulunmaktaydı [23].

Birleşik Krallık'ın 2011 siber güvenlik stratejisine göre, siber uzayda Birleşik Krallık'a yönelik en karmaşık olarak değerlendirilebilecek tehditlerin bir kısmı, casusluk temelinde diğer devletlerden gelmekteydi. Bu devletler aynı zamanda Birleşik Krallık'ın askeri, endüstriyel ve ekonomik varlıklarını hedef almalarının yanı sıra Birleşik Krallık'ta ikamet eden ve kendi rejimlerine muhalif olan kişileri de takip etmekteydiler. Diğer taraftan olası bir çatışma durumunda düşman olarak nitelendirilebilecek bir aktör, siber uzaydaki güvenlik açıklarından yararlanarak Birleşik Krallık ordusunun teknolojik anlamda sahip olduğu avantajı azaltabilir ve bunu Birleşik Krallık'ın kritik altyapı unsurlarına saldırmak için kullanılabilirdi [17]. Tüm bunları dikkate alan Birleşik Krallık, devam eden süreç içerisinde siber uzaydaki yetkinliklerini artırmaya çalışmakla beraber bir ikilemle karşılaşmıştır.

2013'te Edward Snowden'ın aralarında Birleşik Krallık'ın da bulunduğu Batılı devletlerin istihbarat teşkilatlarının iletişim verilerine müdahale ettiğine yönelik yaptığı ifşaatları, devletlerin izleme yetkilerinin genişletilmesine karşı olan lobinin güçlenmesine sebep olmuştur [24]. Esasında Birleşik Krallık İç İşleri Bakanlığı'nın "siber suç stratejisi" başlığını taşıyan 2010 yılına ait belgede de belirtildiği üzere vatandaşların güvenliğini ve yaşam hakkını korumak için gerekli önlemleri alırken, bu önlemlerin Birleşik Krallık için hayati öneme sahip olan temel haklar üzerindeki etkisini dengelemeye çalışılması [25], zorlayıcı olmuştur. Konuya yönelik artan farkındalık gizlilik ve insan hakları yasaları, istihbarat teşkilatlarının faaliyetlerine giderek daha fazla kısıtlama getirmeye devam etmektedir. Bu nedenle aralarında Birleşik Krallık'ın da yer aldığı çok sayıda Batılı ülkenin istihbarat teşkilatları, veri koruma ve diğer yasaları izlemek için avukatlar ve halkla ilişkiler uzmanları çalıştırmak durumunda kalmaktadırlar [26]. Snowden'ın ifşası bu noktada Birleşik Krallık için demokratik bir aktör olarak, demokratik olmayanlara göre siber güvenliği sağlamasının daha zor olacağı bir dönemi başlatması sebebiyle önemliydi.

Özetle Lucas'ın da belirttiği üzere, casuslukta kapalı toplumlar açık olanlara göre üstün bir konuma gelmiştir. Diğer taraftan Batılı ülkelerin Çin, İran, Rusya gibi aktörler üzerinde gözetleme yapması zorlaşırken, bu ülkelerin istihbarat servislerinin dünyanın geri kalanını gözetlemesi kolaylaşmıştır [26]. Ayrıca şu husus da belirtilmelidir ki Birleşik Krallık ve ABD, baskıcı rejimlere sahip olan ülkelerde faaliyet gösteren muhalif gruplara siber temelde verdiği destekle, internet kullanıcılarının gözetim ve sansüründen kaçmasına yardımcı olmaktadır. Baskıcı rejimler ise bunu bir çeşit siber saldırı olarak değerlendirmektedir [27]. Bu yönüyle Batılı liberal demokrasiler ve otoriter devletlerin siber uzaydan aldıkları tehdit farklılaşmaktadır. Otoriter devletler için bu noktada temel endişe kaynağı rejimin benimsediği dünya görüşü ve kontrol altında tuttuğu bilgi akışının sorgulanmasına ve eleştirilmesine yol açacak siber destekli eylemler ve devrimlerin ortaya çıkmasıdır. Buradan hareketle siber suçlar otoriter devletler için de bir sorun olmakla birlikte, siber uzay rejimlerinin devamı için bir tehdit olarak görülmüştür [28].

2016 yılının sonlarıyla birlikte başlatılmış olan yeni siber güvenlik stratejisi ise ortaya koyulan stratejinin bir parçası olarak Birleşik Krallık veri, sistem ve ağlarını savunmanın yanında, düşmanlar için caydırıcı olmayı, siber güvenlik sektörünü büyütmeyi ve siber alanda kritik yeteneklerini geliştirme amacındaydı. Bunu gerçekleştirmek için, 1,9 milyar Pound yatırım yapılmasının planlanmış olması dikkate değerdir [29].

Bu dönemde Birleşik Krallık siber güvenlik temelinde sahip olduğu pozisyona güvenmekle birlikte, dünya çapında az sayıda devletin kendi güvenliğine ve refahına ciddi bir tehdit oluşturacağı yönünde bir düşünceye sahipti. Bu devletler, yıkıcı olanlar da dahil olmak üzere, Birleşik Krallık'ın altyapısı ve endüstrisi için tehdit oluşturma potansiyeline sahip olarak değerlendirilmekteydi. Diğer taraftan çok sayıda devletin de geliştirmeye devam ettikleri siber programlar aracılığıyla Birleşik Krallık için gelecekte tehdit oluşturmaları mümkün olarak kabul edilmiştir. Burada dikkat edilmesi gereken husus, bazı devletlerin cezalandırılmayacaklarını düşünerek gerçekleştirdikleri siber saldırılarla diğer aktörleri benzer eylemler için motive edebileceklerinin belirtilmiş olmasıdır [30]. Siber güvenlik stratejisinde üzerinde durulan devlet veya devlet destekli eylemlerin yanıtsız bırakılmaması düşüncesi, yalnızca savunmayı değil saldırı imkanlarının arttırılmasını da gerekli kılmıştır.

Siber güvenlik kavramı sıklıkla tehdit, saldırı ve savunma gibi kelimelerle bir arada kullanıldığı için askeri bir sorun gibi algılanabilse de yalnızca askeri bir sorun değildir. Çünkü siber güvenlik, bir bütün olarak ve tüm toplum için bir sorun olarak ortaya çıkmıştır. Bu bağlamda geniş, işbirlikçi ve çok sayıda kurumun dahil olduğu bir müdahaleyi de gerektirmektedir [31]. Birleşik Krallık geniş bir

temelde siber güvenliğe önem vermek durumundadır. Bahsi geçen gereklilik Birleşik Krallık tarafından kabul edilmiştir. Buradan hareketle siber güvenlik yalnızca hükümete yönelik bir tehdit olarak değerlendirilmemiş, özel sektör ile vatandaşlar da bu kapsamda önemsenmiştir [9].

2016'ya dair değinilmesi gereken bir diğer gelişme, Birleşik Krallık'ta Hükümet İletişim Merkezi siber güvenliğe ilişkin konularda ana organ olmaya devam etse de kurulan Ulusal Siber Güvenlik Merkezi[9]aracılığıyla, ulusal düzeyde siber güvenliği sağlayacak merkezi bir yapılanma[10] oluşturulmasıdır. Ulusal Siber Güvenlik Merkezi'nin ulusal düzeydeki siber olayları yönetme, siber güvenlik konusunda uzmanlık ve tavsiye sunmanın yanında, siber güvenlik endüstrisini destekleme çabasında olması amaçlanmıştır [30]. Bu bağlamda ulusal düzeydeki siber güvenlik konularında Birleşik Krallık'a işlevsel katkı sunmaya başlayan Ulusal Siber Güvenlik Merkezi aktif bir siber savunma üzerinden Birleşik Krallık'ın siber saldırılara karşı daha güçlü olmasını mümkün kılmıştır [33]. Aktif siber savunma stratejisinin uygulanmasına paralel olarak Birleşik Krallık'ta siber suç tehdidinin azaldığı dikkate alınırsa [34], aktif siber savunmanın işlevsel olarak Birleşik Krallık'ın siber güvenlik stratejisine katkı sunduğu belirtilmelidir.

Siber güvenlik stratejilerinde hedeflendiği şekilde yetkinliklerini arttıran Birleşik Krallık, siber uzayda önemli bir aktör olmakla birlikte, geniş bir alanda çevrimiçi sistemlere sahip olması ve ekonomisini dijital bir temele oturtması sebebiyle, aynı zamanda siber saldırılara karşı korunmasız kalma riskini de sürdürdüğüne inanmaktadır [35]. Ulusal Siber Güvenlik Merkezi'nin verilerine göre Birleşik Krallık'ta Eylül 2020 ile Ağustos 2021 arasında Ulusal Siber Güvenlik Merkezi'nin tarafından yönetilen 777 siber güvenlik olayının yaklaşık %40'ının kamu sektörünü etkilediği göz önünde bulundurulursa, kamu siber saldırılar için cazip bir hedef olmayı sürdürmektedir [36].

İşte bu sebeple Birleşik Krallık 2022-2030 yıllarını kapsayan siber güvenlik strateji belgesinde bulunan siber dayanıklılık hedefi, izlenmek istenen siber stratejinin merkezinde yer almaktadır. Siber dayanıklılığın siber saldırılara rağmen bir kuruluşun temel işlevlerini ve hizmetlerini sürdürme ve verilerinin korunmasını sağlama yeteneği olduğu dikkate alındığında, Birleşik Krallık'ta hükümetin ekonomi ve toplumsal temeldeki hizmetleri sunma sorumluluğunda olması, siber dayanıklılığı vazgeçilmez kılmaktadır. Bu bağlamda Birleşik Krallık'ın 2022-2030 vizyonu, dijitalleşen temel/kritik hükümet işlevlerinin 2025 yılına kadar siber saldırılara karşı önemli ölçüde sağlamlaştırılması ve kamu sektörü genelinde faaliyet gösteren tüm hükümet kuruluşlarının en geç 2030 yılına kadar bilinen güvenlik açıklarına ve saldırı yöntemlerine karşı dayanıklı hale getirilmesi amaçlanmaktadır [36].

Birleşik Krallık'ın 2022-2030 vizyonunda kurulması öngörülen Hükümet Siber Koordinasyon Merkezi[11] ile hükümete bağlı kuruluşların operasyonel siber güvenlik çabalarını daha iyi koordine etmek ve hükümetin kurumlarıyla birlikte "tek vücut" olarak savunma yeteneğini geliştirmesi hedeflenmektedir [36]. Siber uzayın bütüncül bir biçimde korunması gerekliliği dikkate alındığında, bu merkezin kurulması fazlasıyla rasyoneldir.

Birleşik Krallık'ın güncel siber güvenlik stratejisinde üzerinde durulan bir diğer husus, toplumda siber kültür oluşturulmasının gerekliliğidir. Bu noktada kamu çalışanlarına odaklanılmış ve oluşturulacak olan siber güvenlik kültürüyle, kamu görevlilerinin siber güvenlik farkındalığını ve bilgilerini arttırarak kendilerini ve çalıştıkları devlet kuruluşlarını daha iyi koruyabilmelerinin sağlanması amaçlanmıştır [36].

4. BİRLEŞİK KRALLIK'IN SİBER GÜCÜNÜN GELECEĞİ *(THE FUTURE OF THE UNITED KINGDOM'S CYBER POWER)*

Siber saldırıların uluslararası niteliği saldırının faillerinin gizlenmesini kolaylaştırmakla birlikte, saldırıyı gerçekleştirenler amaçlarına ulaşmaları durumunda açığa çıkmaktan da görece endişe etmezler. Diğer taraftan, devlet onaylı veya devlet destekli olarak gerçekleştirilen siber saldırıların cezalandırılma ihtimali, mevcut uluslararası yasal çerçeve dikkate alındığında düşüktür. Nihai olarak ise siber eylemi sebebiyle hiçbir yaptırımla karşılaşmayan bir aktörün faaliyetlerine devam etme olasılığı da yüksektir. Bu aktöre karşı etkili bir ceza/karşılık verilmediği takdirde diğer aktörlerin de benzer siber saldırılara teşvik edilmesi de ihtimal dahilindedir [37]. Bu sebeple siber saldırılara karşı aktörlerin savunmada kalmak yerine saldırı yeteneklerini geliştirmelerinin mümkün olduğunu [38] kabul etmeleri ve buna uygun bir strateji

[9] The National Cyber Security Centre (NCSC).
[10] Birleşik Krallık'ın siber güvenlik alanında özel sektör ile kamu sektörü arasındaki boşluğu doldurması ve Ulusal Siber Güvenlik Merkezi'nin sağlamakta olduğu siber hizmetlere erişilebilirliği artırılması, ulusal siber güvenliğin sağlanmasına yardımcı olacaktır [32].
[11] Government Cyber Coordination Centre (GC3).

izlemeleri ulusal siber güvenliğin sağlanması için elzemdir.

Savunmada kalmanın ulusal güvenliği sağlayacağı düşüncesinin sorunlu olduğu, Maginot Hattı üzerinden verilecek bir örnekle belirtilebilir. Bilindiği üzere 19. Yüzyılda gerçekleşen Alman-Fransız rekabeti, Almanya'nın lehine sonuçlanmıştır. I. Dünya Savaşı'nda da Almanya, Fransa için büyük bir tehdit olmuştur. Bu sebeple I. Dünya Savaşı sonrasında Fransa, Almanya'ya karşı kendisini koruyacağına inandığı bir savunma hattı inşa etmeye başlamıştır. Dönemin Fransa Savunma bakanının adıyla anılan Maginot Hattı'nın hem Almanya'ya karşı caydırıcı olacağına hem de yeni bir Alman saldırısına karşı aşılmaz bir set çekeceğine inanılmıştır. Ancak 1940'ta Maginot Hattı, Alman saldırılarına karşı başarısız olarak sabit istihkama dayalı bir savunma düşüncesinin işe yaramayacağını kanıtlamıştır [39]. Bu örnek siber uzay üzerinden yeniden yorumlanırsa, Birleşik Krallık'ın ulusal siber güvenlik duvarlarını tahkim ederek güvende kalması mümkün değildir. Nasıl Alman zırhlıları farklı stratejiler ve hattın zayıf noktalarını değerlendirerek Maginot'u aştılarsa, ulusal savunmayı sağlayacak siber stratejinin de yalnızca savunmada kalarak bunu mümkün kılması olası değildir. Tarihsel tecrübe dikkate alındığında, güvenliğin savunma ve saldırı unsurlarının bir arada kullanılmasıyla sağlanabileceği ileri sürülebilir.

Ayrıca şu husus belirtilmelidir ki uluslararası hukuk öğretileri dikkate alındığında, belirli koşulların karşılanması koşuluyla, ulusların bir siber saldırının failine karşı savunma ve saldırı temelinde gerçekleştirebilecekleri eylemler bulunmaktadır [40]. BM Hükümet Uzmanları Grubu'nun 2013'te mevcut uluslararası hukukun aynı zamanda devletlerin siber faaliyetlerine yönelik olarak uygulanmasını onaylamasına ek olarak, 2015'te BM Uzman Grubu, BM Şartı'nın bütünüyle siber uzaya uygulandığını kabul etmiştir. Buna bağlı olarak silahlı saldırı eşiğini aşan bir siber operasyona yanıt olarak saldırıya uğrayan devletin meşru müdafaa yönünde hareket etme hakkının geçerliliği de kabul edilmiştir [41]. İşte bu noktada Birleşik Krallık'ın 2019'da kurduğu 6. Tümen, istihbarat, siber ve elektronik savaşta uzmanlaşmış tugayları da bünyesinde bulundurmaktadır. Konvansiyonel olmayan yöntemlerin de içeren yöntemlerle savaşabilecek şekilde oluşturulan bu tümen, Birleşik Krallık'ın gelecek dönemde çıkabilecek savaşlara ilişkin öngörüsünün de bir sonucu olarak değerlendirilebilir [42].

Siber güvenliğe yönelik alınan tehditlerde, silahlı kuvvetlere de ayrı bir yer açılması elzemdir. Silahlı kuvvetlerin bilgi ve iletişim teknolojisine artan ihtiyacı, silahlı kuvvetlerce kullanılan sistemlerin bir siber saldırıya maruz kalmasını mümkün kılmaktadır. Böyle bir saldırı sonucunda silahların çalışma yeteneklerinin büyük bir şekilde tehlikeye girebileceği dikkate alınmalıdır. Bu bağlamda siber tehdidin hızla değişen doğası, Birleşik Krallık Savunma Bakanlığı'nın siber güvenlik temelinde araştırma ve geliştirmeye önem vermesini zorunlu hale getirmektedir [43] ki siber savaş, aynı zamanda askeri teçhizat üreten büyük savunma şirketleri için de cazip bir alan haline gelmiştir [27].

İşe yarar olup olmayacağı kesin olmamakla birlikte, Birleşik Krallık'ın olası bir savaş durumunda kullanılmak üzere siber silahlar geliştirdiği bilinmektedir [6]. Devletler nasıl silahlarını test etmek için tatbikat yapıyorsa, siber uzayda da durum görece benzerdir. Devlet güdümlü[12] bir zararlı yazılım olduğuna inanılan "NotPenya" ile ağırlıklı olarak Ukrayna üzerinde bir siber silahın etkilerinin test edildiği ileri sürülebilir [16].

Siber operasyonlar, devletlerin güç projeksiyonunu ortaya koyabilmeleri[13] açısından giderek daha önemli hale gelmektedir. Birleşik Krallık, düşman devlet aktörlerine, teröristlere ve ciddi örgütlü suçlulara karşı saldırı operasyonları yürütme hedeflerine yardımcı olmak için 2020'de Ulusal Siber Güç'ü[14] oluşturmuştur. Ulusal Siber Güç, aynı zamanda Birleşik Krallık'ın düşmanlarını tespit etmesine, onlara zarar vermesine ve en nihayetinde siber uzayda caydırıcı olmasına destek olma potansiyeline sahiptir [45]. Ulusal Siber Güç, Birleşik Krallık ve müttefiklerinin güvenliklerini siber uzayda sağlamakla yükümlüdür. Bu kurumu farklı kılan savunma ve istihbarat alanında faaliyet gösteren personellerin uzmanlık ve kaynaklarını tek bir yapı altında birleştirmesinin yanında, Birleşik Krallık dış politikasına bağlı olarak siber uzayda operasyon düzenleme yetki ve kabiliyetine sahip olmasıdır. Diğer bir ifadeyle Ulusal Siber Güç siber savunmanın yanında devlet, terör ve suç örgütlerine yönelik olarak siber saldırı düzenlemekle yetkilendirilmiştir [33]. Ayrıca şu husus belirtilmelidir ki Ulusal Siber Güç'ün

[12] Rusya.

[13] Bilindiği üzere görece az sayıda devletin sahip olduğu uçak gemileri, bir güç projeksiyonu aracı olarak ön plana çıkmaktadır. Hemen hemen dünyadaki tüm devletlere saldırabilme imkanını sağlaması, uçak gemilerini güç projeksiyonu olarak ön plana çıkaran hususların başında gelmektedir [44]. Benzer bir bakış açısı siber yetkinlikler üzerinden kurgulanırsa, siber uzay dünyanın tamamına yönelik saldırı düzenleyebilmeyi mümkün kıldığı için güç projeksiyonu için önemli bir araç olarak değerlendirilebilir.

[14] National Cyber Force (NCF).

oluşturulmasında Rusya'dan alınan tehdit en önemli güdüleyici sebeplerden biri olarak öne plana çıkmıştır [45].

Birleşik Krallık Hükümet İletişimleri Başkanlığı, Rusya'yı siber uzayda etkili olabilecek operasyonları yürütme konusunda kapasitesi olan ve oldukça yetenekli bir siber aktör olarak değerlendirmektedir. Rusya'nın demokratik seçim sonuçlarını etkileme çabasının yanında, aralarında Birleşik Krallık'ın da olduğu devletlerin kritik altyapı unsurlarına saldırı düzenlemesi, kamu kurumlarına siber saldırıda bulunması ve organize suç örgütleriyle iş birliği kurarak siber alanda diğer aktörlere zarar verme girişimleri, Birleşik Krallık'ın Rusya'yı ulusal güvenliği için tehdit olarak görmesine neden olmuştur [46].

Rusya'nın yanında teknik anlamda kat ettiği gelişme ve sahip olduğu siber güvenlik gücüne bağlı olarak, Çin'in Birleşik Krallık için en büyük tehdit unsuru olması öngörülmektedir. Görece daha basit yöntemlerle siber saldırılarda bulunmakla birlikte, İran'ın da çeşitli casusluk ve yıkıcı siber yetenekleriyle, Birleşik Krallık tarafından saldırgan bir siber aktör olarak değerlendirildiği not edilmelidir. Diğer taraftan Birleşik Krallık'ın Kuzey Kore'yi, Rusya, Çin ve İran kadar gelişmiş siber imkanlara sahip olmasa da siber uzayda yetenekli bir aktör olarak görmeye devam ettiği belirtilmelidir [47]. Birleşik Krallık siber uzayda belirli yeteneklere sahip olan bu aktörlere karşı caydırıcı olmalıdır. Aynı zamanda devlet destekli saldırılara karşı da caydırıcı olmalı ve bu alanda caydırıcılığını görünür kılmalıdır.[15]

Libicki, siber saldırıyı gerçekleştiren bir aktörün kendisine yapılacak misillemelerin büyüklüğü noktasında öngörü sahibi olmaması durumunda, misillemenin etkilerini abartma ya da küçümseme yoluna gidilebileceğini ileri sürmektedir. Diğer bir ifadeyle, büyüklüğü bilinmeyen veya öngörülemeyen bir tehditle karşı karşıya kalmaları durumunda aktörler, kötümser olup durumu olduğundan kötü bir yere konumlandırabilir veya iyimser bir yaklaşımla tehdidi küçümseyebilirler. Libicki'ye göre istisnaları olsa da büyüklüğü ve etkisi daha öngörülebilir olan bir misilleme, öngörülemeyen bir misillemeden daha fazla caydırıcı olacaktır [49]. Goodman da benzer bir şekilde aktörlerin siber caydırıcılık mesajlarını görünür kılmamalarının siber saldırıların yaygınlaşmasına etki ettiğine değinmiştir [50]. Bu noktada Birleşik Krallık'ın siber güç unsurlarını siber caydırıcılığı sağlayabilmek için görünür kılması ayrıca önemli hale gelmektedir.

Suz Tzu'nun "Savaş Sanatı" isimli eserinde ifade ettiği "güçlüyken onlardan sakın" ifadesi [51], realist temelde caydırıcı olmanın önemini ortaya koyar. Birleşik Krallık siber alanda caydırıcı olmasına rağmen, bir saldırıyla karşılaşması durumunda ise yapılan saldırıya misliyle karşılık vererek caydırıcılığını korumalıdır. Yine realist bir temelde bakılırsa, Machiavelli'nin devletin başındaki liderlerin hem kendilerinin hem de devletlerinin bekasını sağlamak için başvuracakları bütün araçları doğru ve övgüye değer olarak değerlendirdiği [52] dikkate alındığında, Birleşik Krallık'ın da kendisine karşı gerçekleştirilen siber saldırılara karşılık verebileceği araçlar arasında ahlakiliği devre dışı bırakma eğiliminde olması, bir gereklilik olarak düşünülebilir.

Caydırıcılık, düşmana yapmayı planladığı saldırı sonucunda ortaya çıkacak yüksek maliyetin gösterilmesi ve düşmanın henüz başlatmadığı saldırıdan vazgeçirilmesini ifade etmektedir. Caydırıcılıkta dikkat edilmesi gereken temel husus, düşmana yapacağı saldırının sonucunda elde edeceği faydanın, zarardan daha az olacağının açıkça hissettirilmesidir. Bu noktada düşman, muhtemel saldırısı öncesinde uyarılmalıdır. Düşman buna rağmen saldırı yapması durumunda bedel ödeyeceğini bilmeli ve bu yetkinliğe sahip olduğunuza inanmalıdır. Düşman yapacağı fayda/zarar hesabına rağmen bir saldırı düzenlemesi durumunda ise cezalandırılmalıdır [39]. Birleşik Krallık'ın siber yetkinlikleri üzerinden oluşturduğu caydırıcılığa rağmen bir saldırıya uğraması durumunda cezalandırma mekanizmasının işletilebilmesi,[16] siber saldırı yeteneklerinin önemini ortaya çıkarmaktadır.

McKenzie'nin ABD'nin siber caydırıcılığına yönelik ifade ettiği hususların Birleşik Krallık için de geçerli olduğu ileri sürülebilir. McKenzie'ye göre ABD'nin siber caydırıcılığının inandırıcı olması için ortaya koyulan ceza tehdidinin muhatap aktörde karşılık bulması gerekmektedir. Düşman aktörün ceza tedbirlerinden korkarak saldırı düzenlemekten vazgeçtiği bir durum yaratılması için cezalandırma

[15] Diğer aktörlerin davranışlarını etkilemeye dönük olarak kullanılmayan unsurların güç olarak nitelendirilemeyeceğine yönelik düşünce [48] dikkate alınırsa caydırıcılığın görünür kılınması gücün kullanılması olarak da düşünülebilir.

[16] Siber uzayda cezalandırma mekanizması işletilirken şu husus unutulmamalıdır ki siber silahlar, nükleer silahlar veya diğer konvansiyonel silahlar kadar şiddetli bir tahribat yaratamayabilir. Yapılacak bir siber saldırıda kritik altyapı unsurları hedef alınması durumunda bile nükleer silahların kullanımındaki gibi yıkıcı bir etki öngörülemez. Bu anlamda siber saldırıların/misillemenin büyüklüğü ve kapasitesinin görece sınırlı olacağı [53] dikkate alınmalıdır.

mekanizmasının işetilmesinde istekli olunması önem arz etmektedir. Uygulanabilir bir caydırıcılık stratejisi üzerinden kurgulanan caydırıcılık, saldırgan bir yöne sahip olarak bir tür misillemeyi içerir. Bu misilleme siber uzayda olabileceği gibi orantılılık esasına dayanarak saldırıyı düzenleyen aktöre karşı siyasi ve ekonomik eylemlerde bulunulmasıyla [54] da desteklenebilir. Bu noktada siber caydırıcılığın bir tür misilleme üzerinden yalnızca siber uzayda verilmesi zorunlu değildir. Sahip olunan diğer güç unsurları üzerinden ve yapılan saldırıyla orantılı olarak caydırıcılığın sağlanması da ihtimal dahilindedir.

Nye'a göre siber uzayda cezalandırma hem devletlere hem de suça dahil olan aktörlere yönelik olarak mümkün olmakla birlikte, siber uzayda caydırıcılığın gerçek anlamda işe yarayıp yaramayacağı sorusunun cevabı bazı değişkenlere bağlı olarak farklılaşabilir. Diğer taraftan tüm siber saldırılar eşit öneme sahip olmadıkları için ulusal güvenlik üzerinde bir tehdit olarak değerlendirilmez. Bu sebeple bu tür düşük düzeyli saldırılara karşı caydırıcılık kullanılamayacağı için politikacıların önemli saldırılara odaklanması gerekir [55].

Devletlerin dışında, devlet destekli olmayan siber terörizm de Birleşik Krallık için önemli bulunmuş ve ciddiye alınarak güvenlikleştirilmiştir. Teröristler fiziki zarar verebilecekleri terör eylemlerine öncelik vermekle birlikte, Birleşik Krallık'a karşı zarar verici siber faaliyetler yürütmeyi de hedeflemektedirler.[17] Bu saldırılar, devlet olarak Birleşik Krallık için büyük bir tehdit potansiyeline sahip olmasa da düşük kapasiteli siber saldırıların etkisi orantısız derecede yüksek olmaktadır. Örneğin hacklenen kişisel bilgilerin çevrimiçi olarak yayınlanması, medyanın ilgisini çektiği için halkın korkutulmasını da beraberinde getirmektedir. Bahsi geçen orantısız etki dikkate alındığında, terör örgütlerinin siber kapasitelerindeki görece küçük bir artış bile Birleşik Krallık ve onun çıkarları için ciddi bir tehdit oluşturabilir [30].

ABD'nin Ulusal Güvenlik Ajansı[18] siber casusluk konusunda ilk sırada yer alsa [57] da Birleşik Krallık'ın son dönemde Hükümet İletişim Merkezi ile Ulusal Güvenlik Ajansı'na yakın bir kapasiteye ulaştığı düşünülmektedir. Özellikle 2009 sonrasında Birleşik Krallık'ın siber güvenlik alanında yaptığı yatırımlar ve konuya verdiği önemin bunda etkili olduğu söylenebilir.

Ortaya koyulan çabaya bağlı olarak Birleşik Krallık, siber güvenlik yatırımlarının sonuçlarını almaya başlamıştır. Birleşmiş Milletler Uluslararası Telekomünikasyon Birliği'nin (ITU), 2018'de yayınladığı Küresel Siber Güvenlik Endeksi'ne göre Birleşik Krallık, siber güvenlik temelinde yapılan bir sıralamada ilk sırada [58] (ITU, 2019: 62), ITU'nun 2020 yılı Küresel Siber Güvenlik Endeksi'ne göre ise ABD'nin hemen ardından ikinci sırada yer almaktadır [59] (ITU, 2021: 25). Bu noktada Birleşik Krallık'ın yapması gereken siber güvenlikteki sahip olduğu öncü rolü, dünyadaki konumunun temel bir parçası haline getirmektir [60] (Prince & Sullivan, 2019: 17). Siber uzayda kazandığı yeteneklere rağmen Birleşik Krallık'ın küresel bir tehditle yalnız başa çıkması mümkün değildir. Bu noktada tercih edilecek en rasyonel yol, ulusal siber gücün arttırılmasının yanında dost ve müttefik aktörlerle iş birliği yapmaktır.

Romalı tarihçi Tacitus'un devletler kendilerini ilgilendiren bir tehlikeye karşı birleşmek yerine bu tehlikeyle teker teker mücadele eder ve mağlup olurlar yönündeki düşüncesi [61], siber uzayda karşılaşılan tehdide karşılık devletlerin realist temelde kendi kapasitelerini geliştirme çabaları ve bunun sonucunda yaşanabilecek başarısızlık üzerinden uyum içerisindedir. Diğer bir ifadeyle realizmin ön gördüğü self help (kendi kendine yardım) kavramı, siber uzayda aktörler açısından geçerliğini korumakla birlikte, başarılı olmak için iş birliğinin sağlanması gerekmektedir.

Bu yönüyle düşünüldüğünde siber güvenliğin sağlanabilmesi için yalnızca yurt içinde siber güvenliğe ilişkin savunma imkanlarının geliştirilmesi yeterli olmayacaktır. Çünkü yapısı gereği internetin ulusötesi olması, devletlerin karşılaşacağı tehditlerin kaynağını da sınır ötesine taşımaktadır. Bu noktada Birleşik Krallık'ın siber alanda ihtiyaç duyduğu güvenliği tek başına sağlayamayacağı dikkate alınarak, diğer ülkelerle ortaklıkların yapılması elzemdir [17] (Cabinet Office, 2011: 22). Siber uzayda uluslararası iş birliğini mümkün kılmak önemli ve gereklidir. 2016 ve 2019 yılları arasında Birleşik Krallık'ta başbakanlık görevinde bulunan Theresa May de organize suçlara karşı güçlü ortaklıklar kurulmasını gerekli görmektedir. May'e göre terörle mücadele nasıl yalnızca ülke sınırları içerisinde ortaya koyulan çabayla sona erdirilemez ve hükümetler arası bir stratejiye ihtiyaç duyarsa, burada da benzer bir durum bulunmaktadır [62]. Bu

[17] Siber terörizm her ne kadar bombalı bir terör eyleminin ve bu eylemdeki can kaybının medyaya yansıyan görsel etkisine sahip olmasa da bir ülkenin önemli ağlarına yapılacak saldırılarla kaosa sebebiyet verebilirler. Teröristlerin temel amaçları arasında yer alan hükümetin halkını koruyamadığı algısının [56] siber saldırılar üzerinden verilebileceği dikkate alındığında terörizm temelinde siber güvenliğin önemi daha iyi anlaşılacaktır.

[18] National Security Agency (NSA).

farkındalığa sahip olan Birleşik Krallık, siber suçlar başta olmak üzere siber alanda operasyonlar, politika, araştırma, bilgi paylaşımı ve askeri iş birliğini de kapsayan çok sayıda siber paylaşım anlaşması imzalamıştır [63]. Tüm bunlar dikkate alındığında, Birleşik Krallık siber konularda ikili ilişkilere ve çok taraflılığa değer veren bir ülke olarak değerlendirilebilir.

Birleşik Krallık istihbarat ve siber güvenlik alanında, ABD'nin önemli bir müttefiki olarak ön plana çıkmaktadır [64]. Birleşik Krallık ve ABD'nin 4 Ekim 2019'da imzaladıkları antlaşma, tarafların iletişim hizmeti sağlayıcılarından ciddi suçların önlenmesi, tespiti, soruşturulması veya kovuşturulmasına ilişkin elektronik verileri yapılan anlaşmaya uygun bir şekilde elde edebilmesini mümkün kılması [65], siber alanda yakın ilişkilerin önemli göstergelerinden birisidir.

Siber güvenlik ve çok taraflılık üzerinden ifade edilmesi gereken bir diğer konu, Birleşik Krallık, ABD, Kanada, Avustralya ve Yeni Zelanda'nın dahil olduğu önemli ve gelişmiş bir istihbarat sistemi olan Echelon'dur. Echelon'un küresel internet ve iletişimi denetleme, ilgili istihbarat servislerini uyarma ve elde ettiği bilgileri/verileri arşivleme yeteneklerine sahip olduğu [66-67] dikkate alındığında, siber uzayda kolektif bir yaklaşım sergilemenin önemi yeniden hatırlanacaktır.

Birleşik Krallık'ın daha güçlü kolektif eylem için NATO ittifakının siber güvenlik yeteneklerinin geliştirilmesini desteklemeye devam edeceğini beyan etmesi [33] de önemsenmelidir. Siber uzayı operasyonel bir alan haline getirme yönünde bir irade ortaya koyan Birleşik Krallık'ın kendi geliştirdiği modellerin nasıl çalıştığını ve askeri operasyonlarının bir parçası olarak siber etkileri nasıl kullanmayı planladığını NATO ile paylaşması önemlidir. Birleşik Krallık'ın bu noktada istekli ve gönüllü bir tavır ortaya koyması da ayrıca kıymetlidir [16] Son olarak Birleşik Krallık aynı zamanda Küresel Dijital Erişim Programı kapsamında 10 milyon Pound'luk bir yardım ile şimdiye kadarki en büyük denizaşırı siber kapasite geliştirme projesini gerçekleştirmiştir. Bu kapsamda Brezilya, Nijerya, Güney Afrika, Kenya ve Endonezya'da çok sayıda projeye destek verilmiştir [68].

5. TARTIŞMA ve SONUÇ *(DISCUSSION and CONCLUSION)*

1980'li yıllarda siber uzayı güvenlikleştirmesi gerektiğini kavrayan Birleşik Krallık, sonrasındaki süreçte siber uzaydaki konumunu güven altına almayı, ulusal güvenliği sağlamanın ön koşulu olarak değerlendirmiş ve bu konuyu fazlasıyla önemsemiştir. Siber uzayda karşı karşıya kalınan tehditlerin çeşitlenmesine bağlı olarak siber güvenlik yatırımlarını arttıran Birleşik Krallık lider aktörlerden biri haline gelmiştir. Siber güvenlik stratejileri özelinde analiz edildiğinde, Birleşik Krallık bu stratejileri ortaya koyma noktasında görece geç kalmış olsa da siber uzaya gereken önemi vermiştir.

Siber güvenlik stratejilerinin açıklanmasına paralel olarak siber güvenlikte kurumsallaşma da hızlanmıştır. Hükümet İletişim Merkezi halen Birleşik Krallık'ın siber güvenliğini sağlayan ana çatı olmakla birlikte, farklı birimler arasındaki iletişim ve uyumu mümkün kılan mekanizmaların oluşturulması, siber güvenlik ve caydırıcılığın sağlanması için rasyonel bir politika olarak değerlendirilebilir. Birleşik Krallık'ta silahlı kuvvetlerin de siber uzayda yaşanan gelişmeleri dikkate alarak savunma ve saldırı yetenekleri üzerinden kendisini yeniden yapılandırdığı not edilirse, siber uzayda Birleşik Krallık'ın daha etkili bir siber güç olmasının da önü açılmıştır.

Makalede üzerinde durulduğu üzere, aktif siber savunmanın işlevsel olarak siber güvenlik stratejisine katkı sunduğu görülse de Birleşik Krallık'ın yalnızca ulusal siber güvenlik duvarlarını tahkim ederek güvende kalması mümkün değildir. Bunun farkında olan Birleşik Krallık, elektronik savaş yöntemleri ve siber uzayda operasyon düzenleme kabiliyetine sahip olmayı önemsemektedir. Devlet, devlet destekli, terör ve suç örgütlerine yönelik siber uzayda caydırıcı olunabilmesi için siber savaş ve siber saldırı yetkinliklerinin geliştirilmeye devam edilmesi hayati öneme sahiptir. Birleşik Krallık'ın siber yetkinlikleri üzerinden oluşturduğu caydırıcılığa rağmen bir saldırıya uğraması durumunda, saldırıyı düzenleyen aktör Çin ve Rusya gibi siber kabiliyetleri yüksek olan aktörler bile olsa, cezalandırma mekanizmasının işletilebilmesi yeni saldırılara karşı güvende olabilmek için elzemdir. Diğer bir ifadeyle siber operasyonlar, devletlerin güç projeksiyonunu ortaya koyabilecekleri bir alan olarak değerlendirildiğinde, Birleşik Krallık'ın geliştirmiş olduğu yetkinliklerini gerçekleştireceği siber operasyonlarla görünür kılması gerekmektedir. Kısaca Birleşik Krallık'ın siber güvenliğini yalnızca savunmada kalarak elde etmesi mümkün olmadığı için siber caydırıcılık ve saldırı kapasitesini realist temelde arttırması mühimdir. Burada bir hususun ayrıca açıklanması gerekir ki caydırıcı ve saldırı potansiyeli yüksek olan bir siber güç oluşturabilmek için iş birliği imkanları önemsenmeli ve aşağıda açıklanacak saldırgan realizm ile karıştırılmamalıdır.

Saldırgan realizmin hegemonya hedefine ulaşabilmesi için peşinden gittiği daha fazla güce sahip olma dürtüsü, diğer aktörler tarafından istenmeyeceği için hegemon olma yolundaki aktörün gücünün dengelenmesini beraberinde getirebilir. Diğer taraftan savunmacı realistler, hegemonyaya sahip olma çabasını stratejik bir hata olarak nitelemekte ve gücü maksimize etmek yerine yeterince güce sahip olmayı gerekli görmektedirler [69]. Bu noktada gücü bir araç olmaktansa amaç olarak düşünmek,[19] iş birliği imkanını dost ve müttefik aktörler için bile sınırlandırmanın ötesinde sorunlu hale getirmektedir. Ayrıca siber uzayın anarşik yapısı da self help düşüncesi üzerinden işbirliği imkanlarını sıklıkla gereksiz kılmaktadır. İşte bu noktada makalede Tacitus'a atıfla ifade edilen ortak tehdide karşı teker teker mücadele edilip birlikte mağlup olunmasına yönelik düşünce dikkate alındığında, Birleşik Krallık'ın gücü bir amaç olmaktansa araç haline getirerek müttefikleriyle iş birliği imkanlarını dışarıda bırakmaması önem arz etmektedir.

KAYNAKLAR *(REFERENCES)*

[1] Cabinet Office. (2009). *Cyber security strategy of the United Kingdom. safety, security and resilience in cyber space*. London: The Stationery Office.

[2] Applegate, S. (2015). Cyber conflict: disruption and exploitation in the digital age. Frederic Lemieux (Ed.), *Current and Emerging Trends in Cyber Operations Policy, Strategy, and Practice*. Palgrave Macmillan, 19-36.

[3] Sweetman, A. (2022). *Cyber and the city securing London's banks in the computer age*. Springer.

[4] Buzan, B. (2008). Askeri güvenliğin değişen gündemi. *Uluslararası İlişkiler*, *5*(18), 107-123.

[5] Ning, H. (2022). *A brief history of cyberspace*. CRC Press.

[6] Corera, G. (2015). *Intercept: the secret history of computers and spies*. London: Weidenfeld & Nicolson.

[7] Computer Misuse Act 1990. (1990). https://www.legislation.gov.uk/ukpga/1990/18/pdfs/ukpga_19900018_en.pdf

[8] Healey, J. (2013). A brief history of US cyber conflict. Jason Healey (Ed.), *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Cyber Conflict Studies Association, 14-87.

[9] HM Government. (2010). *A strong Britain in an age of uncertainty: the national security strategy.* London: The Stationery Office.

[10] Hjortdal, M. (2011). China's use of cyber warfare: espionage meets strategic deterrence. *Journal of Strategic Security*, *4*(2), 1–24.

[11] Keane, J. (1998). *Şiddetin uzun yüzyılı*, Bülent Peker (Çev.), Ankara: Dost Kitabevi.

[12] Viotti, P. R., Kauppi, M. V., (2016). *Uluslararası ilişkiler teorisi*, (Metin Aksoy, Çev. Ed.), Ankara: Nobel.

[13] Vasquez, J. A. (2015). *Savaş bulmacası,* Haluk Özdemir (Çev.), Uluslararası İlişkiler Kütüphanesi.

[14] Tumkevič, A. (2018). Uncertain security community: building Western cyber-security order. *Journal of Information Warfare, 17*(1), 74–86.

[15] Rid, T. (2013). Cyberwar and peace: hacking can reduce real-world violence. *Foreign Affairs, 92*(6), 77–87.

[16] Shea, J. (2017). How is NATO meeting the challenge of cyberspace? *PRISM*, *7*(2), 18–29.

[17] Cabinet Office. (2011). The UK cyber security strategy: protecting and promoting the UK in a digital world. https://assets.publishing.service.gov.uk/media/5a78a991ed915d04220645e2/uk-cyber-security-strategy-final.pdf

[18] National Audit Office. (2013). *The UK cyber security strategy: Landscape review*. London: The Stationery Office.

[19] Tinker, J. A. (2015). Güvenlik revizyonu. Ken Booth & Steve Smith (Ed.), *Uluslararası İlişkiler Kuramları*, Muhammed Aydın (Çev.), Uluslararası İlişkiler Kütüphanesi. 175-197.

[20] Keshavarz, A. (2017). Stuxnet. Paul J. Springer (Ed.), *Encyclopedia of Cyber Warfare*. ABC-CLIO, 279-282.

[21] Umbach, F. (2012). Critical energy infrastructure and risk of cyber attack. Konrad Adenauer stiftung-international reports, 35-66.

[19] Güç "*bir şeylerin olmasını sağlamak için diğerlerinin davranışlarını etkileme becerisine sahip olma*" [70] anlamında değerlendirilirse burada önemli olan en güçlü olmak değil muhatap aktörün davranışını etkileyebilme yeteneğidir.

[22] Stoddart, K. (2016). Live free or die hard: U.S.-UK cybersecurity policies. *Political Science Quarterly*, *131*(4), 803–842.

[23] Osborne, G. (2015). Chancellor's speech to GCHQ on cyber security. https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security

[24] Richards, J. (2014). *Cyber-war: the anatomy of the global security threat*. Palgrave Macmillan.

[25] Home Office. (2010). *Cyber crime strategy*. London: The Stationery Office.

[26] Lucas, E. (2019). The spycraft revolution. *Foreign Policy*, *232*, 20–27.

[27] Singer, P. W. & Friedman, A. (2014). *Cybersecurity and cyberwar: what everyone needs to know*. Oxford: Oxford University Press.

[28] Steed, D. (2019). *The politics and technology of cyberspace*. Routledge.

[29] Cabinet Office. (2016). The UK cyber security strategy 2011-2016 annual report. https://assets.publishing.service.gov.uk/media/5a81bae5e5274a2e8ab558ca/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf

[30] HM Government. (2016). National cyber security strategy 2016-2021. https://data.parliament.uk/DepositedPapers/Files/DEP2016-0790/National_Cyber_Security_Strategy_v20.pdf

[31] Cornish, P., Hughes, R., Livingstone, D. (2009). *Cyberspace and the national security of the United Kingdom: threats and responses*. Chatham House.

[32] Montasari, R. (2023). *Countering cyberterrorism the confluence of artificial intelligence, cyber forensics and digital policing in US and UK national cybersecurity.* Springer.

[33] HM Government. (2021). National cyber strategy 2022 pioneering a cyber future with the whole of the UK. https://assets.publishing.service.gov.uk/media/620131fdd3bf7f78e469ce00/national-cyber-strategy-amend.pdf

[34] Stevens, T., O'Brien, K., Overill, R., Wilkinson, B., Pildegovičs, T., Hill, S. (2019). *UK active cyber defence a public good for the private sector*. King's College London.

[35] House of Commons Committee of Public Accounts. (2019). Cyber security in the UK ninety-ninth report of session 2017–19. https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/1745/1745.pdf

[36] HM Government. (2022a). Government cyber security strategy building a cyber resilient public sector 2022-2030. https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf

[37] Oxford Economics. (2014). Cyber-attacks: effects on UK companies July 2014.

[38] Harrop, W & Matteson, A. (2015). Cyber resilience: a review of critical national ınfrastructure and cyber-security protection measures applied in the UK and USA. Frederic Lemieux (Ed.), *Current and Emerging Trends in Cyber Operations Policy, Strategy, and Practice*. Palgrave Macmillan, 149-166.

[39] Roskin, M. G., Berry, N. O. (2014). *Uluslararası ilişkiler: ui'nin yeni dünyası*. Özlem Şimşek (Çev.), Ankara: Adres Yayınları.

[40] Kramer, F. D., & Butler, R. J. (2019). *Cybersecurity: changing the model,* Atlantic Council.

[41] Wright, J. (2018). Cyber and international law in the 21st century. https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

[42] Elefteriu, G. (2020). United Kingdom: thinly global. G. J. Schmitt (Ed.), *A Hard Look at Hard Power: Assessing the Defense Capabilities of Key US Allies and Security Partners.* Strategic Studies Institute, US Army War College, 359–390.

[43] House of Commons Defence Committee. (2013). *Defence and cyber-security sixth report of session 2012–13*. London: The Stationery Office Limited.

[44] Goldstein, J. S., Pevehouse, J. C. (2017). *Uluslararası ilişkiler*, Haluk Özdemir (Çev.), Ankara: BB101 Yayınları.

[45] Devanny, J., Dwyer, A., Ertan, A., & Stevens, T. (2021). *The national cyber force that Britain needs?*. King's College London.

[46] Intelligence and Security Committee of Parliament. (2020). Russia. https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf

[47] The National Cyber Security Centre. (2022). Annual review 2022 making the UK the safest place to live and work online.

https://www.ncsc.gov.uk/files/NCSC-Annual-Review-2022.pdf

[48] Özdemir, H. (2008). Uluslararası ilişkilerde güç: çok boyutlu bir değerlendirme. *Ankara Üniversitesi SBF Dergisi, 63*(03), 113-144.

[49] Libicki, M. C. (2018). Expectations of cyber deterrence. *Strategic Studies Quarterly*, *12*(4), 44–57.

[50] Goodman, W. (2010). Cyber deterrence: tougher in theory than in practice?. *Strategic Studies Quarterly*, *4*(3), 102–135.

[51] Tzu, S. (2014). *Savaş sanatı*. Hasan İlhan (Çev.), Ankara: Alter Yayıncılık.

[52] Machiavelli, N. (1999). *Hükümdar*. Selahattin Bağdatlı (Çev.), İstanbul: Der Yayınları.

[53] Chen, J. (2017). Cyber Deterrence by Engagement and Surprise. *PRISM*, *7*(2), 100–107.

[54] McKenzie, T. M. (2017). *Is cyber deterrence possible*? Air University Press.

[55] Nye, J. S. (2017). Deterrence and Dissuasion in Cyberspace. *International Security*, *41*(3), 44–71.

[56] Viotti, P. R., Kauppi, M. V., (2014). *Uluslararası ilişkiler ve dünya siyaseti*. Ayşe Özbay Erozan, (Çev.), Ankara: Nobel.

[57] Aid, M. M. (2013). Espionage moves into the cyber age: the National Security Agency's shift to cyber espionage. R. Huisken, O. Cable, D. Ball, A. Milner, R. Sukma, & Y. Wanandi (Ed.), *CSCAP Regional Security Outlook 2014*, 24–27.

[58] ITU. (2019). Global cybersecurity index (GCI) 2018. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

[59] ITU. (2021). Global cybersecurity index 2020. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

[60] Prince, C., & Sullivan, J. (2019). *The UK cyber strategy: challenges for the next phase*. Royal United Services Institute.

[61] Erkul, İ. Ç. (2021). *Commonwealth'i anlamak: beşikten mezara Britanya İmparatorluğu*. Konya: Çizgi Kitabevi.

[62] HM Government. (2013). *Serious and organised crime strategy.* London: The Stationery Office.

[63] Hitchens, T., & Goren, N. (2017). International cybersecurity information sharing agreements. Center for International & Security Studies, U. Maryland.

[64] Billon-Galland, A. (2019). *UK defence policy and Brexit: time to rethink London's European strategy*. European Defence Policy Brief, European Leadership Network.

[65] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on access to electronic data for the purpose of countering serious crime. (2019). https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019

[66] Bayraktar, G. (2015). *Siber savaş ve ulusal güvenlik stratejisi*. Yeni Yüzyıl Yayınları.

[67] Akkuş, B. (2017). *Özgürlük ve güven(siz)lik ikileminde siber uzay : yeni dünya için bir toplum sözleşmesi denemesi*. Milenyum Yayınları.

[68] HM Government. (2022b). UK government's global digital access programme (DAP) -Pillar 2 Trust & Resilience project summaries. https://assets.kpmg.com/content/dam/kpmg/uk/pdf/2022/12/fcdo-dap.pdf

[69] Mearsheimer, J. J. (2016). Yapısal realiizm. Tim Dunne, Milja Kurki, Steve Smith (ed), *Uluslararası ilişkiler teorileri disiplin ve çeşitlilik*, Özge Kelekçi (Çev.), Sakarya: Sakarya Üniversitesi Kültür Yayınları, 86-106.

[70] Nye, J. S. (2005). *Dünya siyasetinde başarının yolu yumuşak güç*. Rayhan İnan Aydın (Çev.), Ankara: Elips Kitap.