Güvenlik Bilimleri Dergisi / Journal of Security Sciences

Jandarma ve Sahil Güvenlik Akademisi
Güvenlik Bilimleri Enstitüsü
Güvenlik Bilimleri Dergisi, Mayıs 2022,Cilt:11, Sayı:1, 223-240
doi:10.28956/gbd.1015517

Gendarmerie and Coast Guard Academy
Institute of Security Sciences
Journal of Security Sciences, May 2022,Volume:11, Issue:1, 223-240
doi:10.28956/gbd.1015517

Makale Türü ve Başlığı / Article Type and Title
Derleme/ Review Article
Yeni Nesil Savaş ve Siber İstihbarat
Next Generation War and Cyber Intelligence

Yazar(lar) / Writer(s)
Hasan Alpay KARASOY. Doç. Dr., Selçuk Üniversitesi İktisadi ve İdari Bilimler Fakültesi Kamu Yönetimi Bölümü, dr.alpaykarasoy@gmail.com, ORCID: https://orcid.org/0000-0002-3813-2960,

Bilgilendirme / Acknowledgement:
-Yazarlar aşağıdaki bilgilendirmeleri yapmaktadırlar:
-Makalemizde etik kurulu izni ve/veya yasal/özel izin alınmasını gerektiren bir durum yoktur.
-Bu makalede araştırma ve yayın etiğine uyulmuştur.

Bu makale Turnitin tarafından kontrol edilmiştir.
This article was checked by Turnitin.

Makale Geliş Tarihi / First Received :27.10.2021
Makale Kabul Tarihi / Accepted :03.03.2022

Atıf Bilgisi / Citation:
Karasoy H. A. (2022). Yeni nesil savaş ve siber istihbarat. *Güvenlik Bilimleri Dergisi, 11(1), ss 223-240, doi:10.28956/gbd.1015517*

YENİ NESİL SAVAŞ VE SİBER İSTİHBARAT

Öz

Toplumun yapısını ve işleyişini değiştiren makine çağı, insan çatışmasının doğasını da değiştirmiştir. Bu değişim, akademisyenler tarafından farklı incelemelere konu olmuş ve savaşın doğasındaki değişim "Yeni Savaş" veya "Dördüncü Nesil Savaş" şeklinde isimlendirilmiştir. Farklı isimlerle anılmakla birlikte savaşın bu yeni şeklini açıklamada kullanılan kavramların ortak noktası; savaşın taraflarının, savaşta kullanılan silahların ve savaşın gerçekleştiği alanın artık eskisinden farklı olduğudur. Savaşın doğasındaki bu değişim, devletin ve askerî gücün merkezde yer aldığı geleneksel güvenlik anlayışını da değiştirmiş ve güvenlik, kamu hizmetlerinin sunumu noktasında kritik hâle gelen bütün altyapıları kapsamaya başlamıştır. Öte yandan savaş ve güvenlik denilince akla gelen bir üçüncü kavram da istihbarat olmaktadır. Çünkü savaşta rakibe üstünlük sağlamanın, barış zamanlarında ise ulusal güvenliği temin etmenin en önemli yolu istihbarat faaliyetleri ile gerçekleşmektedir. Buradan hareketle bu çalışmanın konusunu savaş, güvenlik ve istihbarat oluşturmaktadır. Savaşın ve istihbaratın dönüşümünü, günümüz çatışma ortamının özelliklerini, bu çatışma ortamında siber güvenliğin yerini ve siber güvenliğin sağlanmasına yönelik bir faaliyet olarak siber istihbaratın önemini incelemek ise çalışmanın amacıdır. Betimleyici analiz yöntemine dayanan çalışma sonucunda ulaşılan bulgular; günümüzde güvenliğin kapsamında meydana gelen genişlemenin istihbaratın da kapsamını genişlettiğini, siber istihbarat faaliyetlerinin bankacılık ve kamu hizmetlerinin sunumu noktasında yoğunlaştığını, dolayısıyla da bu alanlarda siber tehdit istihbaratı faaliyetlerine ağırlık verilmesi gerektiğini göstermektedir.

Anahtar Kelimeler*: Savaş, Yeni Nesil Savaş, İstihbarat, Siber Güvenlik, Siber İstihbarat.*

NEXT GENERATION WAR AND CYBER INTELLIGENCE

Abstract

The machine age having changed both the structure and function of the society, has also changed the nature of human conflict. This change has been examined by academics within the subject of different studies and the change in nature of war has been named as "new war" or "Fourth Generation War". Although there are different names, the common point in all definitions is that the sides of war, the weapons used in the war and the area where the war take place are different now from the old ones. Changing nature of war has also changed the classical security understanding, in which the state and military power are at the center, and security has become to include all critical infrastructures. On the other hand, when talking about war and security, intelligence comes to mind firstly because intelligence activities are the most important way to gain the upper hand over the opponent in war and ensure national security in times of peace. Thus, the subject of this study is war, security and intelligence. The aim of this study is to examine the transformation of war and intelligence, the characteristics of today's conflict environment, the place of cyber security in this environment and the importance of cyber intelligence as an activity for providing cyber security. This study based on descriptive analysis method. Findings indicate that extension of public security led to extension of intelligence, cyber intelligence activities are focused on the provision of banking and public services, and therefore, cyber threat intelligence activities should be focused on in these areas.

Keywords*: War, Next Generation War, Intelligence, Cyber Security, Cyber Intelligence*

GİRİŞ

İstihbarat genel olarak, "yabancı ülkeler, düşman veya potansiyel düşman kuvvetler ve unsurlar ile fiilî veya potansiyel operasyon alanları ile ilgili mevcut bilgilerin toplanması, işlenmesi, entegrasyonu, değerlendirilmesi, analizi ve yorumlanmasından kaynaklanan ürün" olarak tanımlanabilir (Felix, 2018: 7). Savaş ve istihbarat birbirleriyle oldukça yakın ilişkisi bulunan kadim olgulardır. İktisat biliminde tamamlayıcı mallar olarak adlandırılan ve biri olmadan diğerinin tek başına pek bir anlam ifade etmediği şeklindeki anlayış; savaş ve istihbarat için de geçerlidir denilebilir. Çünkü istihbaratın özünde mücadele, yani savaş vardır. İstihbarat olmadan bir savaştan başarı ile çıkılması düşünülemez.

Savaş olgusu, tarihi süreç içerisinde içinde bulunduğu dönemin şartlarına göre değişimler yaşamıştır. Özellikle Sanayi Devrimi'nden sonra makine çağı toplumun yapısını değiştirdiği gibi insan çatışmasının doğasını da değiştirmiştir. Bilim ve teknolojideki gelişmeler, Soğuk Savaş'ın sona ermesi, konvansiyonel çatışmaların maliyetli hâle gelmesi ve kamuoyunda sıcak çatışmalara yönelik isteksizliğin artması gibi faktörler, 21.yüzyıla gelinirken insan çatışmasının doğasını bir kez daha etkilemiştir. Savaşın değişen bu doğası farklı incelemelere konu olmuştur. Örneğin Kaldor ve Münkler, 21.yüzyılda savaşın değişen doğasını açıklamada "yeni savaşlar" şeklinde bir kavram üzerinde dururlarken, Lind ve arkadaşları da "Dördüncü Nesil Savaş" şeklinde bir yaklaşım geliştirmişlerdir (Eker, 2015: 33).

Bu çalışmada Lind ve arkadaşlarının yaptığı incelemeden hareketle savaş olgusundaki dönüşüm; birinci, ikinci, üçüncü nesil savaşlar şeklinde incelenecek, savaşın dördüncü nesli olarak ifade edilen 20.yüzyılın sonu ve 21.yüzyılın başındaki çatışmalar ise Yeni Nesil Savaş (YNS) başlığı altında ele alınacaktır. Lind ve Thiele (2016) tarafından yazılan "4th Generation Warfare Handbook" adlı kitabın tanıtım kısmında, Dördüncü Nesil Savaş'ın Yeni Nesil Savaş'ın bir doktrini olduğundan bahsetmeleri nedeniyle Yeni Nesil Savaş kavramını kullanmanın savaşın doğasındaki değişimi açıklamada daha kapsayıcı olacağı düşünülmüştür.

Savaş olgusunun dönüşümü, güvenlik olgusunun dönüşümünü de beraberinde getirmiştir. Siber alanın gündelik hayata her alanda dâhil olduğu günümüzde (2021) siber güvelik kavramı da güvenlik anlayışının merkezi hâline gelmiştir. Siber güvenliğin önemi şu örneklerle daha iyi anlaşılabilir: 2027 yılına kadar dünya lideri olmayı planlayan Çin, ordularını siber güvenlik okullarında yeniden eğitmeye başlamıştır (Firch, 2020). Haziran 2021'de gerçekleştirilen ABD başkanı Biden ile

Rusya Devlet Başkanı Putin arasındaki görüşmenin en önemli gündem maddelerinden bir tanesi de siber güvenlik olmuştur (VOA, 2021).

Bu verilerden hareketle bu çalışmanın konusunu savaş, güvenlik ve istihbarat oluşturmaktadır. Bilim ve teknolojide yaşanan gelişmelerin savaş ve istihbarat üzerindeki etkisini, YNS olarak adlandırılan günümüzün çatışma ortamında siber güvenliğin ve siber güvenliği sağlamaya dönük bir faaliyet olarak siber istihbaratın önemini incelemek ise çalışmanın amacıdır.

Betimleyici analiz yöntemine dayanan çalışmanın ilk bölümünde savaş ve istihbarat olgularının dönüşümü ve YNS kavramı incelenecektir. İkinci bölümde ise YNS ortamında siber güvenliğin, siber güvenliğin sağlanmasında ise siber istihbaratın önemi ele alınacaktır.

1. YENİ NESİL SAVAŞ: ÇATIŞMANIN VE ÇATIŞMA ORTAMININ DEĞİŞEN DOĞASINI AÇIKLAYICI BİR KAVRAM

İnsanlık tarihi kadar oldukça kadim bir geçmişi olan savaş olgusu, modern anlamda uluslararası ilişkilerin başlangıcı olan ve Avrupa'da Otuz Yıl Savaşları'nı bitiren Westphalia Antlaşması (1648) sonrasında ulus-devletin yaygınlaşması ile birlikte bir incelemeye tabi tutulmuştur (Lind, Nightengale, Schmitt, Sutton ve Wilson, 1989). Bu incelemeler arasında en çok bilinenlerden bir tanesi Lind ve arkadaşları tarafından yapılan incelemedir. Savaşın değişen doğasını kuşaklara ayırarak yapılan bu inceleme, bazı akademisyenler tarafından "yanıltıcı bir yapı dayattığı" (Jordan, Kiras, Lonsdale, Speller, Tuck ve Walton, 2016: 133) gerekçesiyle eleştirilse de, savaş olgusunun dönüşümünü açıklamada yararlı olduğu düşünülmektedir.

Savaş denilince akla ilk gelen kavramlardan bir tanesi ise istihbarattır. Savaş olgusunu inceleyen en eski askerî stratejistlerden olan ve "Savaş Sanatı" adlı klasiğin yazarı Sun Szu'dan beri istihbarat, bir çatışmada üstünlük sağlamanın en önemli aracı olarak değerlendirilmiştir. Bu nedenle çalışmanın bu bölümünde ilk olarak savaş ve istihbaratın YNS döneminden önceki evrimi üzerinde durulacaktır.

1.1. Savaş ve İstihbaratın Yeni Nesil Savaş Döneminden Önceki Evrimi

Yeni Nesil Savaş (YNS) dönemi öncesinde gerçekleşen savaşlar "birinci, ikinci ve üçüncü nesil savaş" başlıkları altında incelenecektir. Birinci nesil savaş, 1648 tarihli Westphalia Anlaşması ile başlayıp 19.yüzyılın ortalarına kadar geçen sürede savaşın doğasındaki hâkim anlayışı ifade eder (Yalçınkaya, 2019: 4). Birinci nesil savaşta; savaşın gerçekleştiği zaman, ortam, savaşın tarafları, savaşın başlangıç ve

bitiş tarihleri muayyendir. Ağızdan dolmalı tüfek ve yine ağızdan dolmalı sahra topları savaşın ana silahları olup savaştaki başlıca hedef, belirli bir bölgenin kontrolünü ele geçirmek veya elde tutmaktır (Gürcan, 2011: 149).

İstihbarat açısından bakıldığında ise birinci nesil savaş döneminin istihbarat anlayışının "insan kaynaklı istihbarat" veya başka bir ifadeyle "ajanlık-casusluk" olduğu görülecektir. İnsan kaynaklı istihbarat, insan unsurunu kullanarak istihbarat toplamak anlamına gelmektedir. Tıpkı savaş gibi istihbaratın da oldukça eski bir geçmişi vardır. İnsan toplulukları, kabileler ve ilerleyen zamanlarda ise devletler, düşmanlarının veya rakiplerinin kendileri hakkındaki düşünce ve faaliyetlerini öğrenmek ve kendi çıkarlarını korumak için nasıl hareket edeceklerini bilmek istemişlerdir (Hitz, 2010: 258). Bu bilginin odak noktasında ise askerî konular yer almaktaydı. Dolayısıyla istihbarat denilince kaynak açısından insan, konu açısından ise askerî bilgiler önce gelmektedir.

Modern anlamda uluslararası ilişkilerin başlamasından önce de bir devletin başka bir devlette bulundurduğu elçilikler istihbarat toplamak amacıyla kullanılırdı. Yakın, bu durumu şu şekilde ifade etmektedir:

> *"XV. yüzyılda ilk defa İtalyanlar, daimi elçilikler ihdası suretiyle istihbaratta ileri bir adım atmışlardır. Venedikli elçiler yazdıkları raporlarda, müşahade ve kanaatlerini değerli bir şekilde belirtmişler, askerî istihbarata hizmet etmişlerdir. Bu elçiler yalnız müşahade ile yetinmemişler, devamlı surette çalışacak olan istihbarat şebekeleri kurmanın temelini de atmışlardır"* (Yakın, 1969: 12).

Casusluk, istihbarat toplamanın en kadim yöntemidir. 19.yüzyılın sonu ve 20.yüzyılın başlarında da İngiltere ve diğer sömürgeci güçler, imparatorluklarını savunmak için casusluğu kullanmışlardır (Hitz, 2010: 259). İnsan kaynaklı istihbarat, günümüzde teknolojinin bu denli geliştiği bir ortamda bile müstesna yerini korumaktadır.

Elektrik, demiryolu ulaşımı, kitle üretimi ve fabrikalar yoluyla insan yaşamını değiştiren Sanayi Devrimi'nin insan çatışmasının doğasını da değiştirmesi neticesinde ikinci nesil savaşların perdesi açılmıştır. İkinci nesil savaş, Sanayi Devrimi'nin bir ürünü olan makineli tüfek, uzun menzilli toplar, buharlı deniz gücü ve Birinci Dünya Savaşı'nın başlamasından sonra yaygın olarak kullanılan uçak ve denizaltı gibi araçların kullanılması ile ifade edilir (Gürcan, 2011: 150).

İkinci nesil savaş olarak adlandırılan dönem (19.yüzyılın ortalarından Birinci Dünya Savaşı'nın sonuna kadar geçen süre), aynı zamanda uçak, telgraf, telefon ve telsiz haberleşmesi gibi iletişim ve ulaşım alanında önemli icatların kullanılmaya başladığı bir döneme tekabül etmektedir. Bu yeni icatlar, hem asli amaçları olan eksende kullanıldığı gibi, aynı zamanda birer istihbarat toplama aracı olarak da kullanılmaya başlanmıştır.

Teknolojinin gelişimi ile birlikte telsiz iletişiminin kullanılmaya başlanması "sinyal istihbaratı" olarak adlandırılan yeni bir istihbarat türünün ortaya çıkmasını sağlamıştır. Sinyal istihbaratı, sinyal olarak adlandırılan elektromanyetik dalgaların yakalanması ve bunlardan istihbarat elde edilmesine verilen isimdir. Birinci Dünya Savaşı yılları, telsiz iletişiminin yaygın olarak kullanıldığı, dolayısıyla da sinyal istihbaratından istifade edildiği bir zaman dilimidir.

Sinyal istihbaratının Birinci Dünya Savaşı yıllarında olgunlaşması Ferris'in şu ifadelerinden de anlaşılabilir: 1913 yılında (yani savaş başlamadan bir yıl önce) dünyada yaklaşık 100 kod kırıcı vardı. 1917-1918 yıllarında yaklaşık 2500 İngiliz, 2500 Fransız, 2000 Alman, 1000 İtalyan, 1000 Amerikalı ve 1000 Rus personel radyo sinyallerini dinleme ve kod çözme işinde çalışmıştır (Ferris, 2010: 159). Özellikle Birinci Dünya Savaşı'nın başlangıç yıllarına tekabül eden Ağustos-Eylül 1914 yıllarında sinyal istihbarat teşkilatları mantar gibi çoğalmıştır. Sinyal istihbaratının Birinci Dünya Savaşı'ndaki ilk ve en önemli getirilerinden bir tanesi, Almanların kendilerinden iki kat daha büyük Rus ordusu karşısında kazandığı zaferde görülmüştür. Rus ordusu devasa yapısına rağmen ilkel bir iletişim yöntemi kullanıyordu ve gönderilen telsiz mesajları şifresizdi. Telsiz haberleşmesini dinleyen Almanlar, Rusların saldırı planları hakkında edindikleri bilgiler sayesinde Rus ordusunu Doğu cephesinde mağlup etmiştir.[1]

İkinci nesil savaş döneminin istihbarat anlamında bir diğer yeniliği "fotoğraf-görüntü istihbaratı"dır. Adından da anlaşılacağı üzere fotoğraf-görüntü istihbaratı, çekilen fotoğraflardan elde edilen bilgileri ifade eder. 19.yüzyılın sonlarından itibaren fotoğrafın yaygınlaşması fotoğraf istihbaratı çağını başlatmışsa da bu istihbarat türünün de yaygın olarak kullanımı Birinci Dünya Savaşı yıllarına rastlamaktadır. Özellikle havacılığın yaygınlaşması ile birlikte havadan gözetlemenin ve istihbarat amaçlı çekilen fotoğrafların sayısı artmıştır. Birinci Dünya Savaşı'nın başlangıcı olan Ağustos 1914'te İngiliz Kraliyet Uçuş

[1] Bu konuda daha fazla bilgi için "Sayılarla Birinci Dünya Savaşı" adlı belgesel serisinin "Savaşa Doğru" başlıklı birinci bölümüne bakılabilir.

Kolordusu, Belçika üzerinden ilerleyen Alman birliklerinin havadan gözetimini gerçekleştirmiştir. Kısa bir süre sonra keşif uçaklarına kameralar yerleştirilmiş ve havadan foto keşif dönemi başlamıştır (Shulsky ve Schmitt, 2002: 22-23).

İkinci nesil savaş döneminin istihbarat alanındaki yeniliklerinden bir tanesi de "iletişim istihbaratı"dır. İletişim istihbaratı, sinyal istihbaratının bir alt disiplini olup basit bir ifadeyle, kablolu veya kablosuz iletişim verilerinin, hedeflenen alıcılar haricindeki kişiler tarafından istihbarat elde etmek amacıyla kullanılması olarak tanımlanabilir. İkinci nesil savaş ve bu dönemin istihbarat anlayışı genel olarak bu şekilde ifade edilebilir.

Üçüncü nesil savaş kavramı, İkinci Dünya Savaşı ve sonrasındaki dönemin savaş anlayışını ifade etmektedir. Bu dönemin savaş anlayışında, Birinci Dünya Savaşı'na hâkim olan siper savaşları artık yer almamaktadır. Siper savaşlarını sonlandıran unsur ise tanklar olmuştur. Dolayısıyla üçüncü nesil savaş, tankların ve hava kuvvetlerinin yoğun olarak kullanıldığı, hız ve manevra kabiliyetinin ön plana çıktığı, gayrinizami savaş taktik ve tekniklerinin sıklıkla kullanılmaya başlandığı bir dönemi ifade etmektedir (Şenol, 2018: 186).

Üçüncü nesil savaş döneminde de insan kaynaklı istihbarat, havacılığın ve fotoğrafçılığın gelişmesi ile fotoğraf-görüntü istihbaratı, iletişim istihbaratı ve sinyal istihbaratı yoğun olarak kullanılmıştır. İkinci Dünya Savaşı yıllarında İngiltere, fotoğraf-görüntü istihbaratını sadece düşman silahlı kuvvetlerinin konuşlanmasını veya hareketlerini izlemek için değil, aynı zamanda önemli teknolojik gelişmelerden haberdar olmak için de kullanmıştır. Bu sayede İngiltere, Almanlar tarafından geliştirilen ve ilk balistik füze olma özelliği taşıyan V1 ve V2 füzeleri ile ilgili gelişmeler gibi yeni teknolojik faaliyetlerden haberdar olmuştur (Shulsky ve Schmitt, 2002: 22).

İletişim istihbaratı noktasında da İkinci Dünya Savaşı yıllarında önemli olaylara tanık olunmuştur. Örneğin, Haziran 1942'de, Hawaii'de bulunan Amerikalı istihbarat teknisyenleri, Japon donanmasına ait şifreli haberleşmeleri elde edip kırmayı başarmışlardı. Bu sayede ABD donanması, Japonya'nın Midway adasına saldırma planını önceden öğrenebilmiştir. Bu hayati istihbaratı iyi değerlendiren ABD'li Amiral Chester Nimitz, Japon donanmasını pusuya düşürerek, donanmanın büyük ölçekli operasyonlar düzenleme yeteneğine önemli ölçüde zarar vermiştir (Shulsky ve Schmitt, 2002: 28).

İkinci Dünya Savaşı'nın ardından başlayan ve 1990'lı yıllara kadar devam eden Soğuk Savaş döneminde gerçekleştirilen uydu teknolojisi, hem sinyal istihbaratı

hem de fotoğraf-görüntü istihbaratı elde etmek noktasında önemli bir işlev görmüştür. Yine ilk olarak 1970'lerde ABD Savunma İstihbarat Ajansı tarafından geliştirilen ve sabit veya hareketli hedeflerin ayırt edici özelliklerini belirlemek amacıyla kullanılan "ölçüm ve iz istihbaratı" da üçüncü nesil savaş döneminde kullanılan istihbarat kaynaklarından bazılarıdır (Richelson, 2007: 111-112).

Bilim ve teknolojide yaşanan gelişmeler, Soğuk Savaş'ın sona ermesi ve konvansiyonel savaşların maliyetinin artması gibi etkenler 1990'lı yıllardan itibaren savaşın doğasını etkilemiş ve Yeni Nesil Savaş olarak adlandırılan yeni bir çatışma türüne zemin hazırlamıştır. Bu yeni çatışma türü aşağıdaki başlık altında incelenecektir:

1.2. Genel Bakış Açısıyla Yeni Nesil Savaş

Yeni Nesil Savaş (YNS) kavramını anlamak için belirli bir tanım yapmaktan ziyade YNS'nin gerçekleştiği ortamı, YNS'nin başlıca özelliklerini ve YNS'nin amacını bilmek yararlı olacaktır.

YNS ortamı ile ilgili kesin bilgiler vermek zor olsa da günümüz perspektifinden bakıldığı zaman şunlar söylenebilir (Jordan, vd., 2016: 439):

- Milisler, isyancılar ve teröristler gibi devlet dışı aktörler güçlenmiş ve kamu güvenliğine yönelik yeni tehditler belirmiştir,
- Yaşanan terör saldırıları ve askerî operasyonlar, medyanın etkisi ile geniş kesimlere ulaşabilmektedir,
- İnternet ve kitle iletişim araçlarının öneminin artması neticesinde algı ve propaganda faaliyetleri yaygınlık kazanmıştır,
- Gündelik hayatın hemen her alanının internette dâhil olması neticesinde siber uzayın önemi artmıştır.

Birinci, ikinci ve üçüncü nesil savaşların aksine YNS'de amaç; belirli bir bölgeyi savunmak veya işgal etmek değildir. YNS'de amaç; karşı tarafın istikrarsızlığıdır. Bu istikrarsızlık; sosyal, siyasi, idari ve ekonomik alanları kapsayabilir. Örneğin, 11 Eylül saldırılarının amacının, ABD'nin ekonomik sistemini çökertmek olduğu belirtilmiştir (Anderson, 2013). Dolayısıyla YNS'de amaç; rakibin saldırı karşısında mukavemet etme yeteneğini zayıflatmak, rakibin siyasi idaresi ile kamu bürokrasisini işlemez hale getirmek ve vatandaşların kamu güvenliğini sağlama noktasında devletine olan inancını zayıflatmaktır.

YNS'nin başlıca özellikleri ise şu şekilde sıralanabilir:

- Konvansiyonel savaşlarda devlet, savaşın başlıca aktörüydü. YNS ortamında ise devlet bu özelliğini yitirmiştir (Lind, 2004: 13).
- Konvansiyonel savaşlarda savaş ve barış zamanları belirgindi ve savaşlar genellikle bir devletin başka bir devlete savaş ilan etmesi ile başlardı. YNS ortamında ise savaş ve barış arasındaki ayrım belirsizleşmiştir. Savaş ve barış arasındaki ayrıma mukabil olarak zafer olgusu da muğlak hâle gelmiştir (Gürcan, 2011: 168).
- Konvansiyonel savaşlarda sivil-asker arasındaki ayrım ve savaş alanı kavramları belirgindi. YNS ortamında ise bu kavramlar belirsizleşmiştir (Johnson, 2019). Yani YNS ortamında savaşın muhatabı sadece askerler olmadığı gibi savaş alanı sadece belirli bir cephe ile sınırlı olmayıp ülkenin kritik altyapı sistemleri gibi alanlar da olabilir.
- Konvansiyonel savaş neticesinde meydana gelebilecek zararı tahmin etmek YNS ortamında gerçekleşecek bir çatışma neticesinde meydana gelebilecek zararı tahmin etmekten daha kolaydır (Johnson, 2019).
- YNS ortamında savaşta kullanılan silahlar da değişime uğramış, sadece ateşli silahlardan ziyade enerji, para, bilgi dezenformasyonu, propaganda ve siber saldırılar birer savaş silahı olarak kullanılmaya başlanmıştır (Johnson, 2019).

Özetle YNS ortamında savaşın tarafları, savaşın gerçekleştiği zaman ve zemin, savaşın başlangıç ve bitiş tarihi gibi kavramlar belirsizleşmiş; savaşta kullanılan silahlar ise değişmiştir. Siber yetenekler, nesnelerin interneti ağı, yapay zekâ ve büyük veri gibi bilgisayar alanındaki yeniliklerin (2018 itibarıyla) gelecek 20 yılın askerî teknolojisindeki en önemli alanlardan biri hâline geleceğini belirten O'Hanlon (2018)'un bu ifadesinden, karşı tarafa verdirilmek istenen zararlarda siber saldırıların önemli bir rol oynayacağı anlaşılmaktadır. Bu nedenle çalışmanın ikinci bölümünde YNS ortamında siber saldırıların gerçekleştiği alan olan siber uzayın güvenliği ve bu güvenliği tesis etmeye matuf uygulamalardan bir tanesi olan siber istihbarat konuları incelenecektir.

2. YENİ NESİL SAVAŞ ORTAMINDA SİBER GÜVENLİK

YNS ortamında mücadele, fiziki alanlardan sanal alanlara doğru kaymıştır denilebilir. Çünkü günümüzde güvenlik anlayışı, yukarıda YNS'nin özellikleri kısmında da bahsedildiği üzere, devlet merkezli ve sadece askerî tehditlere indirgenen bir yaklaşım olmaktan çıkmış ve güvenliğin gündemi siber alanın güvenliğine doğru kaymaya başlamıştır (Sertçelik, 2015). Siber güvenliğin önemi ve onu günümüz güvenlik anlayışının merkezine yerleştiren hususlar aşağıda incelenecektir:

2.1. Siber Güvenlik Kavramı ve Önemi

Uluslararası Telekomünikasyon Birliğinin yaptığı tanıma göre siber güvenlik, "*siber uzayda, kullanıcılar ve organizasyonların varlıklarını korumak amacı ile kullanılan politikalar, risk yönetimi yaklaşımları, araçlar, güvenlik kavramları, güvenlik önlemleri, uygulamalar, kurallar, eylemler, eğitimler ve teknolojilerin bütünü"* (Sertçelik, 2015: 27) şeklinde tanımlanmıştır. Günümüzde siber güvenlik kavramının üzerinde sıklıkla durulmasının ise birtakım nedenleri bulunmaktadır. Bu nedenlerden belli başlı olanları şu şekilde sıralanabilir:

- Yapılan araştırmalar, 2025 yılına kadar dünyanın sanal nüfusunun yeryüzü nüfusunu geçeceğini ve her bireyin bir şekilde sanal ortamda yer alacağını göstermektedir (Schmidt ve Cohen, 2014). Her bireyin sanal ortamda yer alması, bireylerin kişisel verilerinin de sanal ortamlarda bulunması anlamına gelmekte ve güvenlik açısından (kişisel verilerin üçüncü kişilerin eline geçmesi gibi) riskler oluşturmaktadır.
- Her bireyin sanal ortamda yer alacağı konusuna bir örnek olarak son yıllarda dünya genelinde kullanımı artan e-ticaret verilebilir. Özellikle Covid-19'un da etkisiyle 2020 yılında dünyada internet kullanan her 5 kişiden 4'ü e-ticareti deneyimlemiştir (Berktan, 2021). İnternet kullanıcılarının sayısının artmasının beraberinde getirdiği tehditlere örnek olarak da, 2020 yılında Danimarka'da yapılan bir araştırma sonucunda şirketlere karşı gerçekleştirilen en yaygın siber saldırının "kimlik avı" olması verilebilir (Johnson, 2021). Kimlik avı, bireyin kişisel bilgilerine yönelik bir saldırıdır ve doğrudan kullanıcı bilgilerini hedef almaktadır. Şirketlere yönelik bir siber saldırı, hem binlerce (belki de milyonlarca) kullanıcının bilgilerini tehlikeye atacak hem de şirket imajı için şirketin hanesine bir eksi not olarak geri dönecektir.
- Özel sektör için siber güvenliğin önemine değinmek gerekirse 2009 yılında 4 şirketten 1'inden daha azı (yani yüzde 25'ten daha azı) ticari faaliyetleri için internete bağımlıydı. 2019 yılı itibariyle 10 şirketten tamamı, ticari faaliyetleri için internete bağımlı hâle gelmiştir. Ayrıca, iş dünyası liderlerinin yüzde 90'ına göre, güvenilir bir dijital ekonomi, işletmelerin büyümesi için kritik öneme sahiptir (Accenture, 2019).
- Günümüzde bir devletin elektrik santrali ve telekomünikasyon altyapısı, ekonomi ve sağlık sistemi gibi alanlar (bunlara kritik altyapı denmektedir) doğrudan internete bağlı olan alanlardır ve siber tehditler karşısında hassastır. Bu gibi alanlara yapılacak bir siber saldırının maliyeti oldukça yüksek olacaktır (Firch, 2020).

- Ülkelerin kritik altyapılarının yanı sıra, siber alanın güvenliği günümüzde kamu hizmetlerinin dijitalleştiği bir ortamda kamu hizmetlerinin sunumu açısından da önem arz etmektedir. Türkiye özelinde bir değerlendirme yapmak gerekirse Türkiye'de e-devlet üzerinden hizmet veren kurum sayısının 646, sunulan toplam mobil hizmetin 2449 ve toplam hizmet sayısının 5231 olduğu ifade edilmektedir (Karasoy ve Babaoğlu, 2020: 124).

Kamu hizmetlerinin dijital ortamlarda sunulur hâle gelmesi, devletin kritik altyapılarının internete bağlı olması, özel sektörün faaliyetlerini gerçekleştirmek için internete olan bağımlılığın artması ve ticaretin günümüzde giderek e-ticaret hâlini alması gibi faktörler siber güvenliğin önemini daha da artırmaktadır. Bu açıdan siber güvenliği tesis edici etkenler de daha önemli hâle gelmektedir. Bu etkenlerden bir tanesi olan siber istihbarat kavramı aşağıda ele alınacaktır:

2.2. Siber Güvenliğin Sağlanmasında Bir Etken Olarak Siber İstihbarat

İlk olarak belirtilmelidir ki, geleneksek güvenlik anlayışının istihbarat odaklı olması en iyi uygulama olarak kabul edildiği gibi (Crest, 2019: 6), güvenliğe yönelik tehditlerin çok aktörlü ve çok faktörlü hâle geldiği YNS ortamında da istihbarat, güvenlik anlayışının merkezinde olmalıdır. Yukarıda da ifade edildiği gibi YNS ortamında siber alanın güvenliği, kamu ve özel sektörün faaliyet göstermesi için önem arz eden bir konudur. Siber istihbarat kavramı ve bu kavramın günümüze bakan yönüyle artan önemi aşağıda daha ayrıntılı olarak ele alınacaktır:

2.2.1. Siber İstihbarat Kavramı ve Önemi

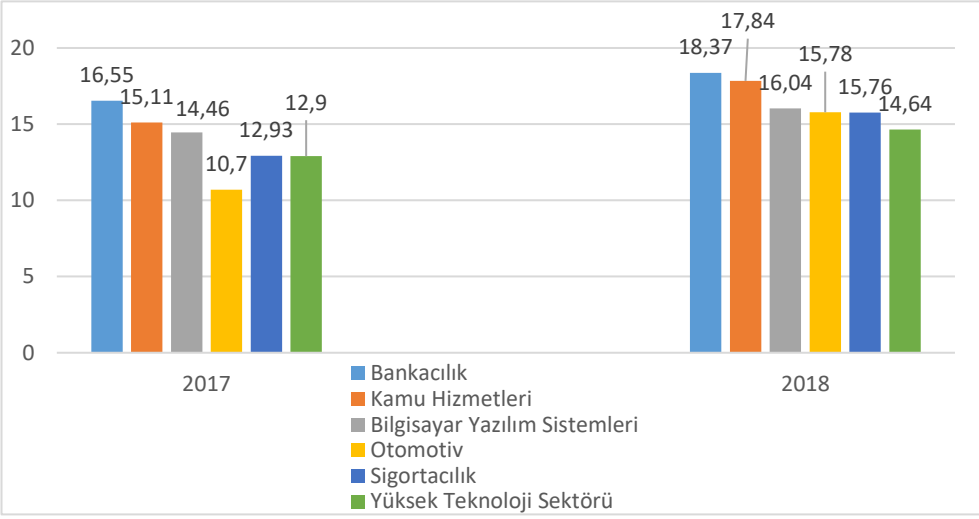
Siber istihbarat kısaca şu şekilde tanımlanabilir (Keleştemur, 2018: 27):

> *"bir ülkenin siber uzaydaki cihazları, enerji üreticileri, kabloları, internet servis sağlayıcıları, sunucuları vb. donanımlarla birlikte yazılımları ve bundan başka siber güvenlik, siber saldırı, siber istihbarat vb. faaliyetlerde bulunacak teknokratların, görevlilerin nitelik ve nicelik gibi özellikleriyle ilgili bilgi toplanması ve analiz edilmesidir."*

Daha genel bir ifadeyle siber istihbarat, siber alanda yer alan verilerden istihbarat oluşturma faaliyetidir. Bu faaliyet, hedefteki dijital cihaza izinsiz erişim sağlayarak cihazdaki bilgileri elde ederek casusluk faaliyeti yürütmek şeklinde olabileceği gibi, siber alanda açık kaynaklardan istihbarat toplamak şeklinde de olabilir. Bunun yanında siber istihbarat faaliyetleri, sadece bilgi elde

etmek amacıyla yapılmamakta, bir ülkenin kritik altyapılarına yönelik saldırılar şeklinde de yapılabilmektedir (Keleştemur, 2017: 76).

Günümüzde siber istihbarat; siber alanda yer alan bilgisayar sistemlerine yönelik saldırılar şeklinde gerçekleştirilebildiği gibi bir ülkenin bankacılık, enerji santralleri, kamu hizmetlerinin sunumu gibi kritik altyapılarına yönelik saldırılar şeklinde de gerçekleşebilmektedir. Aşağıdaki şekilde siber suçların sektörlere göre yıllık ortalama maliyeti gösterilmektedir. Bu şekil, siber istihbarat faaliyetlerinin en çok hangi sektörlerde gerçekleştiği noktasında bir fikir verecektir.



Şekil-1. 2017-2018 Yıllarında sektöre göre siber suçların yıllık maliyeti (Milyon Dolar), Kaynak: Accenture, 2019: 11

Yukarıdaki şekilde dikkat çeken ilk husus, bahsi geçen altı sektörde de siber suç maliyetinin 2018 yılında bir önceki yıla göre artmış olduğudur. İkinci olarak ise siber suçların öncelikli hedefinin bankacılık, kamu hizmetleri ve bilgisayar yazılım sistemleri gibi bir ülkenin kritik altyapısını hedef aldığıdır. Buradan; siber istihbarat faaliyetlerinin de öncelikli olarak bankacılık, kamu hizmetleri ve bilgisayar yazılım sistemleri gibi sektörde yoğunlaştığı yorumu yapılabilir.

Siber alan (başka bir ifadeyle siber uzay), gün geçtikçe genişleyen bir alan olup farklı tehdit türlerini (kimlik avı saldırısı, DDoS saldırısı gibi) bünyesinde barındırmaktadır. Bu nedenle siber istihbaratın bir diğer ayağını da siber alandaki bu tehditlere odaklanan siber tehdit istihbaratı oluşturmaktadır.

2.2.2. Siber Tehdit İstihbaratı

İstihbarat kavramının geçmişi eski olsa da, siber tehdit istihbaratının oldukça yakın bir geçmişi vardır. Siber tehdit istihbaratı, bir tehdit aktörünün amaçlarını, hedeflerini ve saldırı davranışlarını anlamak için toplanan, işlenen ve analiz edilen verilerden oluşur (Baker, 2021). Siber tehdit istihbaratını önemli kılan unsurlar ise kısaca şu şekilde özetlenebilir:

Siber tehdit istihbaratı bilinmeyene ışık tutarak güvenlik personelinin daha iyi karar vermesine yardımcı olur. Saldırganların güdülerini, taktiklerini ve tekniklerini ortaya çıkararak siber güvenlik paydaşlarını güçlendirir. Ayrıca güvenlik personelinin, tehdit aktörünün karar verme sürecini daha iyi anlamasına yardımcı olur (Baker, 2021).

Siber tehdit istihbaratı, güvenlik kuruluşlarının siber saldırıları gerçekçi, çağdaş ve doğru bir biçimde önleme, tespit etme ve bunlara yanıt verme yeteneğini geliştirmesini sağlar. Bir güvenlik kuruluşu siber saldırıların hangi varlıkları, nerede, ne zaman, nasıl ve neden hedef alacağı gibi önemli soruları nasıl yanıtlayacağını bildiğinde kendisini savunmak için önemli bir fırsat elde etmiş olur (Crest, 2019: 7).

Kısaca siber tehdit istihbaratı; mevcut veya ortaya çıkabilecek siber tehditlere karşı hızlı yanıt verilmesine yardımcı olabilecek, ihtiyaca dayalı, doğru ve eyleme geçirilebilir istihbarat elde edilmesine yardımcı olur. Günümüzde güvenlik kuruluşları için siber tehdit istihbaratına sahip olmak önemli bir güvelik bileşeni hâline gelmiştir (Wilson, 2015: 13).

Siber tehdit istihbaratı stratejik, taktik ve operasyonel olmak üzere üç boyutta gerçekleşir. Bir örgütün yöneticileri için en üst düzey analizi sağlayan stratejik tehdit istihbaratında amaç, siber tehditler arasındaki daha geniş eğilimleri anlamak ve dikkate almaktır. Taktik tehdit istihbaratı ise internet ortamında yaşanan olağandışı veri trafiği, dosya indirme ve oturum açma etkinliklerine odaklanır. Operasyonel tehdit istihbaratı, belirli siber saldırılar hakkında, saldırının ne zaman, nasıl ve kimler tarafından başlatıldığını araştırarak saldırı hakkında parçalardan bütüne ulaşmayı amaçlar (Baker, 2021).

SONUÇ

İstihbarat ve savaş tarih boyunca birbirini etkileyen ve bir arada olan iki kavram olmuştur. Savaş ve istihbarat arasında bir ilişki bulunduğu gibi savaş ve teknoloji, ayrıca istihbarat ve teknoloji arasında da bir ilişki vardır. Burada savaş ve istihbarat

kavramlarını bağımlı değişken, teknolojiyi ise bağımsız değişken olarak düşünmek mümkündür. Dolayısıyla savaş ve istihbaratı ortak bir payda altında toplamak gerekirse bu paydanın teknoloji olduğu söylenebilir.

İnsan kaynaklı istihbarat olarak başlayan istihbarat faaliyetleri, teknolojinin gelişmesi ile birlikte iletişim istihbaratı, sinyal istihbaratı ve fotoğraf-görüntü istihbaratı şeklinde farklı kaynaklardan beslenmeye başlamıştır. Savaşın birinci, ikinci ve üçüncü nesilleri geride kalmıştır ancak, savaşın bu kuşaklarında kullanılmaya başlayan istihbarat faaliyetleri, teknolojideki gelişimlere ayak uydurarak kullanılmaya devam etmektedir.

Soğuk Savaş'ın sona ermesi, bilgi iletişim teknolojilerinde yaşanan gelişmeler ve bu kapsamda siber alana olan bağımlılığın artması, konvansiyonel savaşları daha maliyetli hâle gelmesi ve kamuoyunun sıcak bir çatışmaya karşı tavır alması gibi durumlar, insan çatışmasının doğasını da değiştirmiş ve Yeni Nesil Savaş dönemini açmıştır. Yeni Nesil Savaş ile amaçlanan hususlara bakılırsa örneğin rakip ülkenin ekonomik sistemine zarar vermek, siyasi irade ile kamu bürokrasisi arasındaki bağlantıyı etkilemek, bilgi dezenformasyonu yoluyla kamuoyunu etkilemek ve halkın gözünde devletin meşruiyetini sorgulanır hâle getirmek gibi amaçların hepsinin siber alan kullanılarak gerçekleştirilebileceği görülecektir. Bu nedenle Yeni Nesil Savaş ortamında güvenlik anlayışının siber güvenliğe doğru kaydığı görülmektedir.

Günümüzde kamu hizmetlerinin sunumunda, ticari faaliyetlerde, bankacılık sektöründe, sağlık sisteminde ve daha birçok alandaki faaliyetler siber alan üzerinden yapılmaktadır. Bu durum da siber alanın güvenliğini daha önemli hâle getirmektedir. Bu güvenliği sağlayıcı etkenlerden bir tanesi olarak siber istihbarat ön plana çıkmaktadır. Siber istihbarat kısaca, siber alana bağlı olan cihazlardan veri elde etmek şeklinde tanımlanabilir. Günümüzde eğitim, sağlık, bankacılık, ticaret, askerî güvenlik sistemleri ve kentlerin güvenliğini takip etmek amacıyla kullanılan sokak kameraları gibi birçok sektör ve cihaz siber alanda faaliyet göstermektedir. Bu kapsamda, günümüzde siber istihbaratın yapılamadığı herhangi bir alan yoktur. Çalışma kapsamında da ifade edildiği gibi, siber saldırıların sektöre göre yıllık maliyetine bakıldığı zaman bankacılık ve kamu hizmetlerinin ilk sırada yer aldığı görülmüştür. Buradan hareketle, siber tehditler karşısında daha etkili kararlar vermeye yardımcı olan siber tehdit istihbaratı faaliyetlerinin de bu alanlarda yoğunlaştırılması gerekmektedir.

Siber istihbaratın kapsamının genişlemesi, beraberinde oldukça yüksek bir veri yükünü de getirmektedir. Bu veri yükünün analiz edilmesi ve değerlendirilmesi çoğu durumda insan kapasitesini aşan boyuttadır. Bu nedenle siber güvenliğin sağlanmasında ve siber istihbarat faaliyetlerinde, yapay zekâ gibi teknolojilerden yararlanılması önem taşımaktadır.

Belirtilmesi gereken bir diğer önemli nokta da teknolojinin gelişmesine rağmen istihbarat faaliyetlerinde insan unsurunun öneminin azalmadığı, aksine daha da arttığıdır. Siber güvenliğin sağlanması noktasında en önemli eksikliklerden bir tanesi olarak yeterli güvenlik uzmanının eksikliğinden şikâyet edilmektedir. Bu nedenle siber istihbarat alanında da yetkin ve çağın gerektirdiği niteliklere sahip personel yetiştirilmesine önem verilmelidir.

KAYNAKÇA

Accenture. (2019). Ninth annual cost of cybercrime study. Erişim Tarihi 4 Eylül 2021, https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf

Anderson, G. (2013). The end of the peace of westphalia: fourth generation warfare. Erişim Tarihi: 20 Eylül 2021, https://smallwarsjournal.com/jrnl/art/the-end-of-the-peace-of-westphalia-fourth-generation-warfare

Baker, K. (2021). What is cyber threat ıntelligence. Erşim Tarihi: 25 Ağustos 2021, https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/

Berktan, H. (2021). Küresel e-ticaret pazarı %14 artışla 4,9 trilyon dolara koşuyor. Erşim Tarihi: 5 Eylül 2021, Bloomberg HT: https://www.bloomberght.com/kuresel-e-ticaret-pazari-14-artisla-4-9-trilyon-dolara-kosuyor-2282063

Crest. (2019). What is cyber threat ıntelligence and how ıs ıt used? Erişim Tarihi: 25 Ağustos 2021, https://www.crest-approved.org/wp-content/uploads/CREST-Cyber-Threat-Intelligence.pdf

Eker, S. (2015). Savaş olgusunun dönüşümü: Yeni savaşlar ve Suriye örneği. Türkiye Ortadoğu Çalışmaları Dergisi, *2*(1), 31-66.

Felix, M. T. (2018). Unıfied cyber threat ıntelligence. Universidade De Lisboa Faculdade De Ciencias Departamento De Informatica Mestrado Em Informatica, Lizbon.

Ferris, J. (2010). Signals intelligence in war and power politics, 1914–2010. L. K. Johnson (Ed.), The Oxford handbook of national security ıntelligence (ss. 155-171). Oxford University Press.

Firch, J. (2020). 10 Cyber security trends you can't ignore in 2021. Erşiim Tarihi: 5 Eylül 2021, https://purplesec.us/cyber-security-trends-2021/

Gürcan, M. (2011). Bir önceki savaş için hazırlanmak: değişen küresel güvenlik ortamının geleneksel savaş olgusuna etkisi. Bilge Strateji, 3(5), 127-178.

Hitz, F. P. (2010). Human Source Intelligence. L. K. Johnson (Ed.), The oxford handbook of national security ıntelligence (ss. 257-274). Oxford University Press.

Johnson, A. (2019, Şubat 19). A fourth service for the fourth generation of warfare. Erişim Tarihi: 5 Ekim 2021, Wavell Room: https://wavellroom.com/2019/02/19/a-fourth-service-for-the-fourth-generation-of-warfare/

Johnson, J. (2021). What are the greatest cyber/information security threats to your organization? Erişim Tarihi: 5 Eylül 2021, https://www.statista.com/statistics/871608/future-cybersecurity-threats-according-to-companies-in-norway-and-denmark/

Jordan, D., Kıras, J., Lonsdale, D., Speller, I., Tuck, C., ve Walton, C. D. (2016). Understanding modern warfare (2. Basım). Cambridge: Cambridge University Press.

Karasoy, H. A., ve Babaoğlu, P. (2020, Sonbahar). Türkiye'de elektronik devletten dijital devlete doğru. KSBD, 12(23), 115-134.

Keleştemur, A. (2018). Siber istihbaratın kamu güvenliği için rolü ve önemi. (Yayımlanmamış Yüksek Lisasn Tezi). İstanbul Gedik Üniversitesi, İstanbul.

Lind, W. S. (2004, Eylül-Ekim). Understanding fourth generation war. Military Review, 12-16.

Lind, W. S., Nightengale, K., Smitt, J., Sutton, J. W., ve Wilson, G. I. (1989, Ekim). The changing face of war: Into the fourth generation. Marine Corps Gazette, 22-26.

Lind, W. S., ve Thiele, G. A. (2016). 4th generation warfare handbook. Castalia House.

O'Hanlon, M. E. (2018). Forecasting change in military technology 2020-2040, Erişim Tarihi: 8 Aralık 2021, https://www.brookings.edu/research/forecasting-change-in-military-technology-2020-2040/

Richelson, J. T. (2007). The Technical Collection of Intelligence. L. K. Johnson (Ed.), Handbook of ıntelligence studies (ss. 105-117). New York: Routlege.

Schmidt, E., ve Cohen, J. (2014). Yeni dijital çağ. (Ü. Şensoy, Çev.) İstanbul: Optimist Yayınları.

Sertçelik, A. (2015). Siber olaylar ekseninde siber güvenliği anlamak. Medeniyet Araştırmaları Dergisi, *2*(3), 25-42.

Shulsky, A. N., ve Schmitt, G. J. (2002). Silent warfare understanding the world of ıntelligence (3. Basım). Potomac Books Inc.

Şenol, M. (2018). Hibrit savaş kapsamında siber savaş ve siber caydırıcılık. Ş. Sağıroğlu, ve M. Alkan (Ed.), Siber güvenlik ve savunma (ss. 181-221). Ankara: Grafiker Yayınları.

VOA. (2021). Biden ve Putin ilk kez yüz yüze görüştü. Erişim Tarihi: 8 Ekim 2021, https://www.amerikaninsesi.com/a/biden-ve-putin-ilk-kez-yuz-yuze-gorustu/5931386.html

Wilson, C. E. (2015, June). Cybersecurity in the 21st century: applying cyber threat ıntelligence. The Colloquium for Information System Security Education (CISSE) Proceedings of the 19th Annual Conference, 1-19.

Yakın, A. (1969). İstihbarat, casusluk ve casuslukla mücadele. Ankara: Dışişleri Akademisi Yayınları, Sayı 3.

Yalçınkaya, H. (2019). Savaşın değişimi ve kuramsal tartışmalar. Güvenlik Yazıları Serisi, (46), 1-8. doi:10.13140/RG.2.2.14764.21128