Selçuk Ün. Sos. Bil. Ens. Der. 2019; (Prof. Dr. Fuat Sezgin Özel Sayısı): 296-308
- Uluslararası İlişkiler / Araştırma -

Gelenekselden Dijitale Siber İstihbarat ve Rus Dış Politikası

Demet Şefika MANGIR[*]
Sevda Nur KÜÇÜKKIRLI[**]

ÖZ

Uluslararası sistemin egemen devletleri çıkarları gereği, askeri, güvenlik, ekonomik ve ticari faaliyetler içerisinde karşılıklı işbirliğini sürdürebildikleri gibi, çatışan çıkarları doğrultusunda rekabetçi politikalar izleyebilmektedirler. Bu bağlamda çıkar eksenli amaçlar doğrultusunda farklı birçok yol ve yönteme de başvurmaktadırlar. Bunlardan biri de istihbarattır. İstihbarat ülkelerin "gizli" yollar ile bazı bilgilere ulaşma ve bu bilgileri devletin yararına olacak şekilde kullanma, gizleme ya da engelleye yönelik olarak taktik içerikli işlenmiş bilgi olarak özetlenebilir. Devletler ve devlet-dışı aktörler istihbarat kavramını çok uzun yıllardan beri kullanmaktadır. Günümüzde CIA (Central Intelligence Agency), FSB (Federal Security Service), MOSSAD (The Institute for Intelligence and Special Positions) gibi istihbarat servisleri ve arkalarında ABD (Amerika Birleşik Devletleri), Rusya, İsrail gibi küresel etkileri tartışılmaz ülkelerin bu servisleri kullanarak pek çok alanda devletlerin çıkarlarına uygun politikaların oluşturulması için araştırmalar yaptıkları ve çeşitli araçlarla bilgi topladıkları bilinmektedir. Sovyetler Birliği'nin halefi olarak uluslararası sistemde yerini alan Rusya, yakın çevre doktrini kapsamında eski Sovyet sınırlarında önemli bir aktör olduğunu, özellikle eski KGB (Komitet Gosudarstvennoy Bezopasnosti) ajanı Vladimir Putin'in iktidara gelmesiyle birlikte değişimin ve dönüşümün kapılarını aralayacağının sinyallerini vermiştir. Realist paradigmadan bakıldığında anarşik ve çıkar temelli bir dünyada yürütülen ilişkiler, menfaatleri öncelemekte ve devletlerin ve devlet-dışı aktörlerin muhatapları karşısında bir adım önde olma isteği istihbaratın gerekliliğini kendi içinde meşrulaştırmaktadır. Bu nedenle Rusya'nın hem iç politikada hem de dış politikada etkin olmasında, ekonomik, toplumsal ve siyasal açılardan istihbarat servislerinin nasıl bir rol oynadığı merak konusudur. Günümüzde istihbarat yöntemleri eski geleneksel yöntemlerini devam ettirmekle birlikte, teknolojik gelişim ve dijitalleşen dünya ile kullanılan teknik donanımlar bilgiyi ülkelerin elini daha da güçlendiren bir işlev görmektedir. Dolayısıyla çalışmada, uluslararası sistemin önemli aktörlerinden Rusya'nın dış politikasında, geleneksel istihbarattan siber istihbarata verilerin işlevinin ve etki alanının dijitalleşmeyle nasıl bir boyut kazandığı irdelenmektedir. Bu doğrultuda, literatür taraması ile elde edilen verilerden yola çıkılarak, kuramsal çerçevede istihbarat kavramı sorgulanarak Rus dış politikasında geleneksel istihbarattan dijital istihbarata geçiş süreci ve bunun politik eksendeki yansımaları analiz edilmeye çalışılacaktır.

Anahtar Kelimeler: İstihbarat, Dijitalleşme, Siber İstihbarat, Rus Dış Politikası.

Cyber Intelligence in Russian Foreign Policy

ABSTRACT

The sovereign states of the international system can continue their mutual cooperation in military, security, economic and commercial activities as well as pursue competitive policies in line with their conflicting interests. In this context, they apply to many different ways and methods for interest-oriented purposes. One of them is intelligence. Intelligence can be summarized as tactical information for countries to access certain information through "confidential" means and to use, conceal or block this information for the benefit of the state. States and non-state actors have been using the concept of intelligence for many years. Today, it is known that intelligence services such as CIA (Central Intelligence Agency), FSB (Federal Security Service), MOSSAD (The Institute for Intelligence and Special Positions) and the countries whose global influences such as the USA(United States of America), Russia and Israel are indisputable are conducting researches and collecting information by means of these services in order to formulate policies that are in the interests of the states. Russia, which took its place in the international system as the successor of the Soviet Union, signaled that it was an important actor within the borders of the former Soviet Union, especially with the arrival of the former KGB agent Vladimir Putin to open the doors of change and transformation. From the realist paradigm, relations in an anarchic and interest-based world prioritize interests, and the desire to be one step ahead of the interlocutors of states and non-state actors justifies the necessity of intelligence in itself. Therefore, the role of intelligence services in economic, social and political aspects plays an important role in Russia's effectiveness in both domestic and foreign policy. Today, although intelligence methods continue their old traditional methods, they are inadequate in technological development and digitalizing world. Therefore, the study examines how the function and domain of data from traditional intelligence to cyber intelligence has gained a dimension in the foreign policy of Russia, one of the important actors of the international system. In this direction, based on the data obtained from literature review, the concept of intelligence is questioned in the theoretical framework and the process of transition from traditional intelligence to digital intelligence in Russian foreign policy and its reflections on political axis will be analyzed.

Keywords: Intelligence, Digitalization, Cyber Intelligence, Russian Foreign Policy.

[*] Dr. Öğr. Üyesi, Selçuk Üniversitesi, orcid no: 0000-0002-2542-8551, demetacar@selcuk.edu.tr.

[**] Yüksek Lisans Öğrencisi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Uluslararası İlişkiler Bilim Dalı, orcid no: 0000-0001-6306-7016, sevdanurkkirli@gmail.com

Makalenin Gönderim Tarihi: 18.11.2019; Makalenin Kabul Tarihi: 28.12.2019

1. Giriş

İstihbarat kelime anlamı olarak, *"bilgi toplama, haber alma"* (tdk.gov.tr) anlamında dilimize Arapçadan geçmiş bir sözcüktür. Devletlerin, uluslararası sistemin aktörlerine dair bilgi toplaması durumu olarak da tanımlanan (dictionary.cambridge.org) istihbarat, ABD'nin 1947 yılında yayınladığı *Ulusal Güvenlik Eylem Planında* da, yabancı hükümetlerin veya bunların unsurlarının, yabancı kuruluşların veya yabancı kişilerin kapasiteleri, niyetleri veya faaliyetleriyle ilgili bilgi olarak tanımlanmıştır (Warner, 2002; 15). 2013 yılında ABD, İstihbarat Reformu ve Terörle Mücadele Yasası'nda, *"ülkenin insanlarına, mülküne veya çıkarlarına yönelik tehditleri engellemek; kitle imha silahlarının geliştirilmesi, yaygınlaştırılması veya kullanılmasını önlemek ulusal veya uluslararası güvenliği sağlamak adına bilgi toplama süreci"* olarak istihbarat kavramını yeniden tanımlamıştır. Bu bağlamda, istihbarat politika kararlarına, askeri eylemlere, uluslararası müzakerelere ve yabancı ülkeler düzeyindeki temaslara dayandırılmıştır. Dolayısıyla etkili bir istihbarat programının oluşturulması, en küçük birimden en büyük birime kadar uyumlu, hızlı ve etkin bir şekilde karar alınması gerektiğinin önemi vurgulanmıştır (USANI, 2013; 1-4).

İstihbarat, üst düzey merkezler tarafından yönetilen çalışmaların amaca ulaşabilmesi için, mevcut imkânların ötesine geçip yeni stratejiler ve yollar kullanmayı gerektirmektedir. Bu süreçte tüm istihbaratlar, bilgiler üzerine kuruludur, ancak her bilgi bir istihbarat sağlamamaktadır. Çoğu zaman istihbarat ile bilgi birbirleri yerine kullanılmakla birlikte, istihbarat analitik bir sürecin ürünüdür ve bazı aşamalardan geçmesi gerekmektedir. Bu nedenle, bilgi toplanacak alanın belirlenmesi, bilginin toplanması, işlenmesi, analiz edilmesi ve sonrasında bilginin yayılması ve geri bildirimin sağlanması amaçlanmaktadır (Pace, 2018; 2). Toplanılan istihbarat bilgileri pek çok alanda kullanılmakta ve devletler için hayati önem taşımaktadır. Bu bağlamda istihbarat bilgileri; daha önce yapılan anlaşmaların durumunu ve yaptırımların gidişatını izlemede, askeri operasyonları desteklemekte, savunma ve güvenlik politikalarının kapsamını ve etkisini arttırmakta ayrıca ekonomi alanı da başta olmak üzere devlet mekanizmasını doğrudan etkileyecek pek çok konunun karara bağlanmasında kullanılmaktadır (Johnson, 2007; 125-127).

Geleneksel istihbaratta bir bilginin istihbarat haline gelebilmesi için gereken bu süreçleri yerine getirebilmek uzun bir zamana yayılmakta ve karmaşık süreçleri içermektedir. Ancak teknolojik gelişmelerle birlikte, dünya zaman içerisinde yaşadığı değişimler nedeniyle adeta "küçülmüş" ve bilgi toplamak daha kolay bir hale gelmiştir. Bu bağlamda istihbarat çalışmaları da yeni düzene adapte olmak için kendisini güncellemiş, dijital istihbarat, siber istihbarat gibi yeni kavramları metodolojisi içerisine dâhil etmek durumunda kalmıştır.

Bilgi çağı, insanoğluna yeni fırsatlar sunmakta, bilgi toplama sürecini hızlı ve daha basit hale getirmektedir. Bu süreç istihbarat servislerinin gelişimi açısından olumlu karşılansa da, karşı taraf için bir dezavantaj konumundadır. Bütün verileri elinde toplayabilen ve güvenlik açıkları olmakla birlikte bu bilgilerin korunmasını sağlayabilen siber alan ve siber istihbarat çalışmaları son yılların trend konularından olmuştur. Bu bağlamda Rusya da teknolojik değişim ve gelişimlerle, güvenli bilginin sağlanması ve kullanılması açısından gerekli alt yapı ve donanımlarını oluşturmuştur. Siber güvenliğe çok önem veren Rusya aynı zamanda siber gücünü de sürekli olarak üst düzeyde tutan bir devlettir. İstihbarat konusundaki uzun geçmişi de düşünüldüğünde, Rusya'nın siber istihbarat alanında önemli bir rol alması kaçınılmazdır. Dolayısıyla, Rus dış politikası iç veya dış unsurlara göre belirlense de siber alandan alınan istihbaratlar da dış politikayı şekillendirmede etkin bir silah olarak kullanılmaktadır. Bu çerçevede istihbarat nedir nasıl yapılır gibi sorulara cevap verildikten sonra geleneksel yöntemlerden dijitale ve siber istihbarata giden süreç irdelenecek ve bu süreçte Rus dış politikasının temel argümanları çerçevesinde nasıl bir yol ve yöntem izlediği üzerinde durulacaktır.

2. Kuramsal Çerçeve; İstihbarat Nedir?

On beşinci yüzyıldan bu yana bilgi ve haber amaçlı kullanılan istihbarat, on dokuzuncu yüzyılda kurumsallaşmıştır. İstihbarat çoğunlukla savaşların bir parçası olarak, askeri konulara ve olaylara yönelik bilgi edinme işlevini yerine getirmektedir. Savaş dışı dönemlerde de diplomasinin bir aracı olarak müzakerelerde önemli bir unsur olmuştur. İstihbarat kelimesi, etimolojik olarak Arapça "istihbar" kelimesinden aktarılan ve İngilizcede "intelligence" kelimesi ile haber ve bilgi almanın dışında zeka, anlayış gibi kavramları da vurgulayarak, bilginin elde edilmesinden öte bilginin analiz edilmesini içermektedir

(Özdağ, 2014; 19). Bu nedenle bilginin istihbarat niteliğinde olması için, akla dayalı bilimsel bir süreçten geçmesi ve analiz edilmesi gerekmektedir.

Tarihsel süreç içerisinde büyük bir ivme kazanan istihbarat, modern devletin önemli bir parçasıdır ve hükümetin başarısı ve başarısızlığında önemli bir faktör olmuştur. Bu nedenle devletlerin büyük bir çoğunluğu kalıcı bir kurumsallaşmaya gitmiş ve büyük kaynaklar olmasa da ciddi miktarlarda bu yapıya yatırım yapmışlardır. Buna paralel olarak özellikle, ABD ve Kanada'daki üniversitelerde ve kolejlerde "istihbarat çalışmaları" adı altında tarih ve siyaset bilimi derslerinin alt biriminde akademik kurslar açılmıştır (Spracher, 2009; 44).

İstihbarat amaçlı farklı araçlar ve yöntemlerle toplanan veriler, ülkelerin dış politikaya yönelik eylemlerini desteklemeye yardımcı olmaktadır. II. Dünya Savaşı'ndan bu yana geleneksel çizgide devam eden istihbarat araçları son yıllarda değişen ve gelişen teknolojik gelişmelerle birlikte önemli ölçüde değişmiştir. Bu bağlamda istihbarat servislerinin en bilinen yöntemi insan temelli istihbarat yöntemidir. Bu yöntemin dışında teknik temelli (sinyal istihbaratı, ölçüm ve imza istihbaratı (Major, 1995; 11), coğrafi istihbarat ve siber istihbarat (Katz ve Banaski, 2018; 60) gibi) istihbarat yöntemleri günümüzde daha hızlı, daha kesin ve daha işlevsel yöntemler olarak kullanılmaktadır.

En yaygın olarak kullanılan yöntem insan temelli istihbarattır (HUMINT). Kökleri antik dünyaya kadar uzanan yöntem, II. Dünya Savaşı ve Soğuk Savaş döneminin ilk yıllarında kritik bilgiler elde etmek, düşman eylemlerini önlemek ve dost kuvvetlerin askeri, siyasi ve ekonomik avantajlar kazanmasına yardımcı olmak için hemen hemen bütün toplumlar tarafından kullanılmıştır. Yabancı bir ülkenin amaçlarını, kapasitelerini, gücünü, eğilimlerini, taktiklerini, ekipmanlarını ve yeteneklerini öğrenmek ve kendi ülkesine iletmek için insanlardan veya kurumlardan bilgi toplayan kişiler (casuslar)(United States Army,, 2016; 362) aracılığıyla, kişilerarası iletişim, sorgulama, gizli fotoğraf, belge ve diğer materyallerle veriler elde edilmektedir (NATO, 2008; 130; CIA, 2010). 1950'lerde geliştirilen yeni teknolojilerle, hava ve uydu araçlarıyla verilerin elde edilmesi daha da kolaylaşmış ve zamanla insan temelli istihbarat yönteminin etkisi azalmıştır. İstihbaratın teknik temelleri günümüzde daha etkin bir şekilde kullanılmaktadır.

Teknik istihbarat (TECHINT); sinyallerle, fotoğraflarla, uydularla, radarlarla ve çeşitli elektronik manyetik araçlarla yapılmaktadır (Özdağ, 2014; 124). Bu bağlamda sinyal istihbaratı ile elektromanyetik spektrum (dalga boyu ve frekans aralığı) kullanılarak, karşı tarafın niyetleri, eğilimleri ve yetenekleri öğrenilmektedir. Aslında, sinyallerin yakalanmasıyla yapılan istihbarat toplama işlemidir. Elektronik sinyalleri ifade eden sinyal istihbaratı, kendi içerisinde ikiye ayrılmaktadır (USMC, 2018; 9). Bunlardan ilki, iletişim istihbaratı bir diğeri de elektronik istihbarat sistemidir. Buna göre iletişim istihbaratı telefon görüşmeleri, kısa mesajlar ve çeşitli çevrimiçi etkileşimler dâhil olmak üzere kişilerin veya kurumların iletişiminden toplanan bilgilerdir. Bu bilgiler, iletimdeki frekans ve diğer teknik detaylar dikkate alınarak toplanmaktadır (Gökduman, 2018; 4). Elektronik istihbarat ise doğrudan iletişimde yer almayan bilgileri, yayılan radyo frekansları ile radar sistemleri yoluyla elde etmeyi ve gerektiğinde erken uyarı sağlamayı içermektedir. Elektronik istihbarat sayesinde ülkelerin savunması sağlanmakta, yabancı füzeler ve uzay araçları gibi pek çok bilgi elde edilmektedir (Bernard, 2009; 2).

Ölçüm ve imza istihbaratında (MIGINT), herhangi bir ayırt edici özelliği tanımlamak amacıyla belirli tekniklerden (metrik, açı, uzamsal, dalga boyu, zamana bağlılık, modülasyon, plazma ve hidro-manyetik) faydalanarak, verilerin nicel ve nitel analizleri ile elde edilen bilimsel ve teknik istihbarat bilgisi ifade edilmektedir. Böylece yabancı ülkelerdeki nükleer, kimyasal ve biyolojik özellikler, yayılan nükleer, termal ve elektromanyetik enerji, yansıyan veya yeniden düzenlenmiş radyo dalgaları, ışık ve ses doğrultusunda manyetik özellikli bilgiler elde edilmektedir. Ayrıca, gizli yer altı tesisleri, bulunması zor kimyasal ve biyolojik savaş sahalarındaki faaliyetleri izleyebilme gibi devletlerin elini güçlendirecek yeteneklere sahip olunmaktadır (Seng, 2007; 119).

İnsan temelli istihbarat yöntemleri ile birlikte kullanılan teknik istihbaratta, her türlü tehdit ve yabancı askeri teçhizat ile ilgili bilgi toplanmakta ve analiz edilmektedir. Küreselleşen dünyada istihbaratın tüm formları ve teknikleri, hızlanan iletişim teknolojisi ve çeşitli bilgi işlem ve ölçüm cihazları tarafından desteklenmektedir. Minyatür kameralar ve mikrofilmlerle gizli belgelerin fotoğraflanması ve filmlerin gizlemesi kolaylaşmıştır. Uyduların casusluk işlevinde kullanılması, bu yolla gizli askeri tesislerin tespit edilmesi gibi çalışmalar yapılmaktadır. Gizliliğin esas olduğu bu süreçte, telefonların kablo kullanılmadan

dinlenebilmesi, kapalı ortamlarda elektronik dinleme ve kayıt cihazları ile birlikte veri sağlanması ve karanlıkta fotoğraf çekebilme gibi imkânlar sağlanmaktadır (Fidan, 1999; 18). Dolayısıyla günümüzde, uydular, hava araçları, insansız hava araçları gibi teknik yöntemlerle, görüntü ve coğrafi bilgiler eşleştirilmekte ve konumsal verilere ulaşılmaktadır. Bu bağlamda coğrafi yöntemler de istatistiki verilere ulaşmada (haritalama ve ölçme teknolojileri ile grafik oluşturma, jeodezik gibi) etkili olmaktadır (Cardillo, 2018; 3).

Sonuç olarak, istihbarat amaca uygun olarak çeşitli yöntemler kullanmıştır. Bu yöntemlerle elde edilen veriler, olayların değişimi ya da dönüşümüne oranla esneklik sağlayabilecek sonuçları da beraberinde getirmiştir. Yani sadece aktüel tehditlerle değil fırsatları da göz önünde bulundurmanın ve geleceğe de yön vermenin çabası içerisinde bilginin doğru analiz edilmesi ve amacına uygun kullanılması gerekmektedir. Bu bağlamda sürekli yenilikçilik gerektiren istihbarat, gazeteler, dergiler, konuşmalar, radyo istasyonları, sosyal paylaşım siteleri ve hükümet raporlarını içeren kamuya açık bilgi kaynaklarını da kullanmaktadır.

Dijitalleşme ile birlikte istihbarat yöntemleri çeşitlenirken, alanı, kapsamı ve etkisi de genişlemektedir. Bu çerçevede, haber ve bilgi ajansları, kültürel-diplomatik değişimler ve sosyalleşme ile elde edilen bilgi çoğu zaman güdülenmiş olmasına rağmen, internet ve bilgi iletişim teknolojilerine dayalı olarak daha fazla kitleyi etkilemektedir. Bilginin dijitalleşmesi literatüre siber istihbarat kavramını katmaktadır (Ünver, 2018; 14). Dijital bilginin kendine siber alanda yer bulması ile istihbaratta geleneksel yöntemlerin ötesinde hız-kesinlik-doğruluk ilkeleri siber alana taşınmıştır.

3. Gelenekselden Dijitale Siber İstihbarat

Geleneksel istihbaratta, insan temelli yöntemlerle yapılan bilgi toplama, işleme ve kullanma süreci, dijital istihbaratla teknik boyutun daha da işlevselleştiği mekanik bir yapıya dönüşmüştür. Dijital istihbarat (DNINT), bilgiye erişmede ve bilgiyi işlemede, iç ağlardan, güvenlik cihazlarından, sosyal medya platformlarından kısacası networklardan faydalanmaktadır. Bir yerden bir yere bilgi aktarımında kullanılan ağlar vasıtasıyla hızlı ve etkin bir şekilde bilgiye erişim sağlanmaktadır. Dijital istihbarat, bilişim teknolojilerinin gücünü bugünün dünyasına uygun bir şekilde uyarlayarak istihbarat için yeni bir kanal yaratmaktadır (Mithas ve McFarlan, 2017; 9).

Dijital istihbarat, politika yapıcılar olarak devlet ve devlet dışı aktörelerin yanı sıra uluslararası toplumun dinamiklere göre dünyayı etkilemektedir. Örneğin iş dünyası ve ekonomik veriler devletlerin ekonomi politikalarında, birbirlerine karşı uygulayacakları yatırımları ve yaptırımları yönlendirebilecek etkiye sahiptir. Bu noktada, web siteleri veya mobil uygulamalarının kullanımları ile toplanan veriler işleme süreçlerine gerek kalmadan tek bir dijital dosya ile hem ekonominin aktörleri için hem de istihbarat kurumları için hızlı ve etkin bir şekilde kullanılacaktır (Manasia vd, 2018; 7901).

Dijital teknolojilerle ilgili yeni bilgi ve becerileri edinme ve uygulama kabiliyetini sağlayan dijital istihbarat, bugün yeni bir istihbarat alanı yaratmış ve kendi içerisinde de alt dallar oluşturmuştur. Bunlardan birisi de sosyal medya istihbaratıdır. Son yıllarda dijital araçlara yapılan erişimin giderek artması, insanların en önemli bilgilerini başka platformlara daha bilinen adıyla "bulutlara" yüklemesi gibi pek çok gelişme sosyal medya istihbaratının doğmasında etkili olmuştur (simonwaller.com).

İnternet ve mobil teknolojiler sosyal medyanın yükselişinin ardındaki temel güç olmuştur, bilgi yayma, içerik oluşturma ve etkileşimli iletişim için yeni platformlar sağlayan sosyal medya dünya genelinde milyonlarca kullanıcıya ulaşmaktadır. Örneğin şu an dünya genelinde 4,393,684,400 kişi interneti kullanmakta ve bu sayı her salisede katlanarak artmaktadır (internetlivestats, 2019). Bu sayılar aslında kullanıcı sayısı kadar, dijital bilgi üretilmekte ve işlenmekte olduğunu göstermektedir.

Bu bağlamda sosyal medya, bilgi ekosisteminin kritik bir parçasıdır. Bu nedenle sosyal medya platformları ve uygulamaları, kullanıcılara, tüketicilere, seçmenlere, işletmelere, hükümetlere ve aynı zamanda kar amacı gütmeyen kuruluşlara, yaşamın her kesiminden herkese sağladığı erişim ile eşi benzeri görülmemiş bir bilgi yığını oluşturmaktadır. Dolayısıyla politikacılar, siyasi partiler ve hükümetler için de sosyal medya, politikalar ve siyasi konular hakkında kamuoyunu ölçmenin yanı sıra tüm bilgilere ulaşabileceği veri tabanını temsil etmektedir. Bu açıdan sosyal medya istihbaratı da, çeşitli gereksinimlerle belirli sosyal medya verilerini toplama, izleme, analiz etme, gözetleme ve görselleştirme için bilişim araçlarını geliştirmek ve değerlendirmekle ilgilenmektedir.

Sosyal medya istihbaratı, verilerin uygulama yöneticileri ile paylaşılması, devletin bu bilgilere erişiminin sağlanması ve kişilerin zayıf yönlerini kullanarak onların kişisel ve özel bilgilerine erişimin sağlanması yolu ile veri toplamaktadır (Zeng vd. 2011; 14). Bu bağlamda sosyal medya istihbarat işlevini sosyal mühendislik yoluyla daha etkin hale getirmektedir. Sosyal mühendislik insanların zaaflarından faydalanarak bilgi toplamayı amaçlayan, kasıtlı olarak insanları manipüle ederek aldatıcı tekniklerin kullanılması sonucu bilginin sömürülmesi sürecini ifade etmektedir (Barbosa, 2019; 4205). Sosyal Mühendislik, kötü amaçlı kişilerin karşı tarafı ikna ve kandırma yolu ile bazı bilgileri elde ederek güvenlik duvarlarını aşmayı ve ya da kişilerin kendi rızaları ile dijital ortama kaydettikleri bilgileri kullanarak amaçlarını gerçekleştirmelerini anlatan bir kavramdır (Shetty, 2011; 3).

Dijital istihbarat, geleneksel bilgi toplama yöntemlerine nazaran hem daha çok veri elde edilmesine sağlamakta hem de daha kolay erişim sağlamaktadır. Dijital yöntemlerle bilgileri işlemek daha basitleşmiş ve bilgiyi yayma sürecinde de büyük bir hız elde edilmiştir. Ancak bilgiyi analiz etmede ve bilgiyi istihbarat haline dönüştürme de insan temelli yöntemlerin gerekliliği de gözden kaçırılmaması gereken bir durumdur. Burada insan temelli yöntemlerle, potansiyel bir tehdidin nasıl araştırılacağı, bir saldırıyı engellemek için hangi önlemlerin alınacağı, güvenlik kontrollerinin nasıl güçlendirileceği veya ek güvenlik kaynaklarına ne kadar yatırım yapılması gerektiği gibi pek çok analiz sorusuna cevap aranmaktadır. Dolayısıyla geleneksel ve dijital istihbarat birbirini tamamlayıcı bir etkiye sahip olmakla birlikte dijital istihbarat geleneksel istihbaratın yöntemlerini daha efektif hale getirmiştir (Pace, 2018; 3-8). Böylece bugün sosyal medya platformları sayesinde dünyanın diğer ucunda olan bir gelişmeyi oturduğumuz yerden öğrenmek mümkün hale gelmiştir.

İnternet, istihbaratın elini güçlendirmede önemli bir kaynaktır. Özellikle son yıllarda yaşanan gelişmelerin dinamik etkileşimi sayesinde, dijital istihbarat araçlarının geliştiğini görmek mümkündür. İnternetin ve dijital verilerin kamu, kurumsal ve devlet tarafından kullanımının artmasıyla daha önce eşi benzeri görülmemiş bir bilgi kaynağı oluşturulmuştur. Dijital ortamda yer alan pek çok program, bireylerin etkinliklerinin, hareketlerinin ve bilgilerinin takip edilmesini sağlamaktadır. Dolayısıyla teknolojik gelişmeler ve popüler uygulamalar, bilgiye ulaşmak için yeni fırsatları mümkün kılmakta, istihbarat elde etmek için dijital verilerin daha ustaca kullanılmasının geliştirilmesine katkı sağlamaktadır (Omand, 2015; 2).

Bilgi çağı insanoğluna sağladığı avantajlar ile bugün yeni fırsatlar sunmuş ve yeni alanların ortaya çıkmasında etkili olmuştur. Bilgi toplama sürecinin bu kadar kolaylaşması istihbarat servisleri için olumlu bir gelişme olsa da bu bilgileri içeren siber dünyanın ve o dünya içerisindeki bilgilerin korunması, siber koruma dâhilinde yapılan çalışmalar son yılların trend konularından olmuştur. Bu bağlamda, siber istihbarat (CYBINT); siber alanda yer alan bilgiyi toplama, analiz etme ve yayma ile ilgili olarak ele alınan bir kavramdır. Siber alan içerisinde yer alan bilgiler saniyeler içinde yüklendiği ve kimi zaman da değiştirildiği için siber istihbarat geniş ve aldatıcı özellikleri olan bir alt istihbarat dalıdır. Siber istihbarat bilgiye ulaşılmasını kolaylaştırdığı gibi bilginin korunmasını sağlayan her türlü güvenlik kontrolünü de kırabilecek bir yapıya sahiptir. Örneğin, kötü niyetler ile oluşturulan bir solucan, dünyanın her yerindeki binlerce bilgisayara saatler, dakikalar veya hatta saniyeler içinde yayılabilir ve bilgi güvenliğini alt üst edebilir (Alsmadi, 2019; 91).

Geleneksel istihbarat yöntemlerinin dijitalleşmesiyle literatüre giren siber istihbarat, uluslararası ilişkilerin tüm aktörlerinin, insanların, ekonomik amaçları olan kurum ve kuruluşların ve daha pek çok öznenin siber alandaki yeteneklerini, niyetlerini ve faaliyetlerini değerlendiren ve bu yetenekler doğrultusunda bilgi elde etme süreçlerini içeren bir kavramdır (Akyeşilmen, 2018; 231). Bir başka tanımla siber istihbarat, yetenekleri, niyetleri ve karar vermeyi geliştiren, hedeflenen bölgelerdeki faaliyetleri belirlemek, izlemek ve tahmin etmek için bilgi edinme ve analiz etme yöntemidir (Ettinger, 2019; 3). Dolayısıyla siber istihbarat, dış aktörlerin ülke içindeki amaçlarını anlama, ülke çıkarları gereğince başka ülkelerden bilgi toplama, yerel değişiklikleri ve şüpheli etkileşimleri tespit etme gibi pek çok konuda politika yapıcıların elini güçlendirmektedir. Elde edilen veriler doğrultusunda olası saldırganların motivasyonları, dilleri, organizasyonları ve sosyal davranışları anlaşılmakta ve bu kişilere ve kurumlara ait siber profiller oluşturulmaktadır. Böylece potansiyel tehdit içeren oluşumlar tespit edilip devletlerin siber alanda daha proaktif politikalar yürütmesine zemin hazırlanmaktadır (INSA, 2015; 2).

Geleneksel istihbarat sürecinin siber istihbaratta uyarlanması ve siber uzayın doğasına uygun olarak tasarlanması gerekmektedir. Bu bağlamda siber istihbarat döngüsü geleneksel istihbarat ile karşılaştırılarak bir dizi süreç uyarlanmıştır. Buna göre siber istihbarat döngüsünün başlangıcını, siber istihbarat çalışmalarını, gerekliliklerini ve ihtiyaçlarını belirlemek ve sonrasında bu amaçların gerçekleşebilmesi için yapılacak işlemleri içeren, *planlama ve yönlendirme* aşaması oluşturmaktadır. Daha sonra veri ve bilgi toplamak için gereken ortam, güvenlik duvarı kayıtları, izinsiz giriş tespiti sistemi kayıtları gibi, siber güvenlik önlemleri de dikkate alınarak gerçekleşen *bilgi toplama* aşaması başlamaktadır. Bu doğrultuda siber alanda bilgi toplamanın pek çok yolu bulunsa da en sık kullanılan yöntemler şunlardır: Şebekelerden veya bilgi sistemlerinden toplanan verileri içeren *pasif bilgi toplama*, diğer ağlardan veya düşman olarak görülen bilgi sistemlerinden paylaşılan bilgiler doğrultusunda toplanan verileri içeren *karışık bilgi toplama* ve son olarak dış ağlardan veya rakiplerin etkisi altındaki bilgi sistemlerinden elde edilen verileri içeren *aktif bilgi toplama* sistemleridir (Vardangalos, 2016; 5).

Makineler tarafından toplanan bilgilerin insan tarafından okunabilir bilgilere dönüştürülmesi ve ayrıştırılması için gereken aşama ise *bilgiyi işleme ve kullanma* aşaması olarak adlandırılmıştır. Bir kaynaktan toplanan değerlendirilmemiş verilere *ham veriler* denmekte ve bu veri türü, işlenmesi ve analiz edilmesi için ekstra zaman gerektiren bir veri türü olarak sistem içerisinde yerini almaktadır. Seçilmiş ham verileri içeren başka bir analist tarafından işlenen ve analiz edilen veriler *analiz verileri* olarak adlandırılmaktadır. Verilerin, görev ve işlemlerini tamamlamak için gerekli olan aşamaya gelmesi ve yaymaya hazır bilgilerin bir rapor haline gelmeye hazırlanması aşamasına gelmesiyle ortaya çıkan veri türü *üretim verileri* türüne geçmektedir. İşlenen bilgiler neticesinde üretilen tüm raporların, başta belirlenen istihbarat ihtiyacını veya amacını karşılamasına yönelik *analiz ve yorumlama* aşaması bilgiyi işlemeden sonra gelmektedir. Son olarak istihbarat isteyen kurumlara kaliteli bilgiyi ulaştırmayı içeren *bilgiyi yayma ve birleştirme* adımı gelmektedir(Vardangalos, 2016; 7). Bu süreçler sonunda toplanan istihbarat bilgileri devletlerin iç ve dış politikalarını şekillendirmede aktif bir rol oynamaktadır.

Geleneksel istihbaratta bilgiye erişim uzun süreler alsa da günümüzde siber istihbaratta kullanılan teknoloji ile daha kısa sürede veri elde edilmektedir. Siber alanda, verilerin analizi ve yorumlanması oldukça zor bir süreci içermekle birlikte oluşan veri setleri ile daha efektif bilgilerin kapısı aralanmakta bu doğrultuda geleneksel istihbarata nazaran daha fazla sonuç veren bir istihbarat yapısı oluşmaktadır. Dolayısıyla, analiz edilen verilerle büyük felaketlerin önlenmesi, ülke çıkarlarına yönelik olası tehditlere önceden önlem alınabilmesi gibi öngörülü bir yaklaşım oluşturulmaktadır (Murray, 2016; 92).

Siber istihbaratın istenilen çıktıları verebilmesi için teknik, bilişim, analitik, iletişim ve örgütsel yeterliliklerinin olması gerekmektedir. Teknik yeterliliklerle, bilgi ve iletişim teknolojisinin, donanım ve yazılım (özellikle siber güvenlikle ilgili olarak) açısından anlaşılır olması gerekmektedir. Bilişim (bilgi yönetimi) yeterlilikleri ise; bilgi toplama ve planlama için bilgi yönetimi doğrultusunda karmaşık veri ve bilgi analizini ve sunumunu toplamak ve bunları destekleyecek araçları kullanmayı ifade etmektedir. Analitik yeterlilikler, eleştirel ve sistematik düşünme, akıl yürütme ve mantık, problem çözme ve karar verme gibi çeşitli kaynaklardan gelen verilerin ve bilgilerin karmaşık analizi için gerekli olan yeteneği içermektedir. İletişim ve organizasyon yeterlilikleri ise, fikirlerin ve akıl yürütmenin açıkça ifade edilmesinin yanı sıra, bireyin fikirlerini yazılı, sözlü sunum ve görsel gösterme ile proje yönetimi becerilerinin etkili bir şekilde iletilmesini vurgulamaktadır. Son olarak örgütsel yetenekler; karmaşık sorunları analiz etmek, belirli hedeflere ulaşmak için kaynakları, süreçleri ve sonuçları planlamak, düzenlemek, değerlendirmek, yaymak ve kontrol etmek için gerekli proje yönetimi becerilerinin olması gerektiğini içermektedir (INSA, 2015; 7).

Siber istihbarat çalışmaları bilgi toplama amacı ile yapılmakla birlikte siber saldırılarla caydırıcılık işlevini de yerine getirmektedir. Siber alanda güçlü olan devletler kendi istediklerine ulaşabilmek için diğer devletlerin sistemlerinin yürüdüğü önemli platformlara saldırabilmekte, kritik altyapıları hedef alarak karşıdaki devlette bir caydırıcılık yapmayı hedeflemektedir (Keleştemur, 2019; 7). Bu bağlamda siber saldırılar içinde caydırıcılığa yönelik yapılan en ünlü saldırılardan birisi Estonya'ya yönelik DDoS saldırılarıdır. Mayıs 2007'de gerçekleşen olayda Estonya'nın Rusya için önemi olan bir asker heykelini kaldırmak istemesi, Rus hükümetinin DDOS saldırılarıyla yanıt bulmuştur. Ülkenin cumhurbaşkanlığı sarayı, parlamentosu, hemen hemen tüm hükümet siteleri, siyasi partilerin sosyal ağları, medya ve iletişim şirketlerinin yanı sıra iki büyük banka bu saldırılardan doğrudan etkilenmiştir (Guinchard, 2011; 76).

Dolayısıyla, siber alanda bilgi toplamak kimi zaman kullanıcının öz iradesi ile yayınladığı bilgiler ve kandırma ile sosyal mühendislik doğrultusunda gerçekleşse de bazen de bu bilgi toplama işlemi siber saldırılar ile gerçekleşmektedir. Siber alanda bu saldırıların kim tarafından ne sıklıkla ve ne zaman yapıldığını anlamak çok zordur. Özellikle devletlerin istihbarat sağlamak için yapmış olduğu saldırıları tespit etmek neredeyse imkânsızdır. Zira bu uluslararası hukuk bakımından da açıkta kalan bir konuyu oluşturmaktadır. Siber saldırıların menşei ülkesi bilinse bile bunun bir yaptırımı veya geri dönüşümü olmalı mıdır gibi sorular uluslararası hukuk tarafından yeniçağın getirdiği sorunlar kategorisinde incelenmektedir.

Siber uzayda bir saldırının gerçekleşmesi için çeşitli yol ve yöntemler bulunmakta ve bu saldırılar da kötü niyetli veya iyi niyetli hackerler tarafından gerçekleştirilebilmektedir. Bu yöntemlerin bazılarından bahsetmek siber saldırılar ve siber istihbaratta bilgi toplanması aşamalarının daha iyi anlaşılmasını sağlamak için yol gösterici olacaktır. Veri sahteciliği, virüsler, solucanlar, casus yazılımlar(spyware), kötücül yazılımlar, mantık bombaları, phishing (oltalama), spam, sosyal mühendislik, zombileştirmek, DOS ve DDOS saldırıları, fidye yazılımları (ransomware) ve klavye takipçileri(key loggers) siber saldırıların başlıca yöntemlerini oluşturmaktadır (Akyeşilmen, 2018; 74-80). Tüm bu saldırılan hepsini açıklamak başka bir çalışmanın konusunu oluşturmaktadır. Ancak bu saldırı yöntemleri ile bilgi toplandığını bilmek siber istihbaratın sağlanması için kullanılan araçları içerdiğinden konunun daha da sağlam bir zemine oturmasını sağlayacaktır.

Birleşmiş Milletler 'in Bağımsızlık ve Egemenliğin korunması hakkındaki beyanına göre;

"*Hiçbir devlet veya devlet grubu, herhangi bir nedenle başka bir devletin iç veya dış işlerine doğrudan veya dolaylı olarak müdahale etme hakkına sahip değildir. Sonuç olarak, silahlı müdahale ve diğer tüm müdahale biçimleri ya da devlet kişiliğine ya da siyasi, ekonomik ve kültürel unsurlarına karşı tehdit girişimleri, uluslararası hukuka aykırıdır*" (UNGA, 1965).

Bu maddeden de anlaşılacağı üzere, silahlı müdahale ve diğer tüm müdahale biçimleri (siber saldırılar da dâhil olmak üzere); devlet kişiliğine ya da siyasi, ekonomik ve kültürel unsurlarına karşı tehdit girişimleri, uluslararası hukuka aykırıdır. Ancak siber istihbarat ve casusluk bu maddeye rağmen devam etmekte ve bugün pek çok devletin dış politikasını yönlendirmektedir. Bu bağlamda Rus dış politikasında istihbaratın ve siber istihbaratın yeri ve önemi irdelenecektir.

4. Tarihsel Çerçevede Rus İstihbaratı

Rusya'da ilk istihbarat faaliyeti Korkunç Ivan döneminde (1565-1572) Çar'a muhalif aristokratların topraklarını müsadere etmek amacıyla kurulmuş, Opriçnina adındaki gizli polis teşkilatıdır. Zaman içinde sürekli olarak devam eden Rus istihbarat faaliyetleri genellikle rejime karşı muhalifleri denetleme ve baskılama amaçlı faaliyetlerdir. I. Dünya Savaşı sırasında gizli belgelerin yayınlanmasıyla yerini Cheka'ya bırakmıştır. Ekim Devrimi'nden sonra yönetimi ele geçiren Bolşevik Liderler emperyalist savaştan çekildiklerini açıklayarak Çarlık Yönetimi'nin dâhil olduğu bütün gizli anlaşmalarını dünya kamuoyuyla paylaşmıştır (Çamaş, 2018; 129).

1917 yılında ülkede başlayan isyanlar sonucunda II. Nicolas-Romanov hanedanlığı sona ermiş, 1917'de Ekim Devrimi sonrası Bolşevik iktidarı kurulmuş ve ülke iç savaşa sürüklenmiştir. Sovyetlerin ilk lideri Lenin, Rus istihbarat servisi Çeka'yı kurmuştur (Pringle, 2006; 8). Servis, Sovyet rejimi içindeki düşmanları hedef alan "devrimin kılıcı ve kalkanı" olarak adlandırılan bir yapıya sahip olmuştur. Kökenleri ve amaçları ne olursa olsun, Rusya'ya karşı her türlü devrim ve sabotaj eylemlerine son vermek servisin temel görevi olmuş ve bu durumdan dolayı pek çok tutuklama ve suikast gerçekleştirilmiştir (Alphahistory, 2019). Çeka kurumsal yapılanmasını genişleterek faaliyetlerine devam etmiş, sahip olduğu büyük casus ağı ile ordu ve istihbarat alanında büyük bir etki yaramıştır. Bu etki Rus istihbarat servisinin konjonktürel şartlara uygun olarak tarihsel süreç içerisinde çeşitli isimlerle (NKGB ve NKVD, MGB, MVD gibi) kendini revize etmesine ve dış politika sürecinde devletlerin ulusal çıkarları için önemli bir rol oynadıklarını ortaya koymuştur. Bu bağlamda, 1954 yılında Bakanlar Kuruluna bağlı olarak KGB (Devlet Güvenlik Komitesi) kurulmuş, Küba Füze Krizi'nin çözümünde, 1968'de Prag Baharı'nda, 1979' da Afganistan müdahalesinde önemli bir rol oynamıştır (Zickel, 1991; 403-407). Bu bağlamda, KGB Sovyetlerin güvenliğinden sorumlu, casusluk, gizli eylem, karşı istihbarat, sınır koruma ve nüfus kontrolü ile birlikte, yasaların ve idari önlemlerin tamamını kapsayan bir sorumluluk içerisinde hareket etmiştir (Polgar, 1989; 1-3). GRU (Glavnoye Razvedyvatel'noye Upravleniye) ise, Sovyet döneminde askeri istihbarat alanı ile ilgili bir birim olarak hizmet etmiş ve bugün de Rus istihbaratının önemli bir parçasıdır. GRU'nun agresif ve risk alma

kültürü, askeri geçmişini ve önemli elektronik, uydu ve savaş alanı keşif yeteneklerini ve Spetsnaz'ı (özel kuvvetler) içeren geniş portföyünü yansıtmaktadır. Genelkurmay Başkanlığı'nın bir parçası olmasına rağmen, bir dereceye kadar operasyonel özerkliğe sahiptir ve başkanı doğrudan cumhurbaşkanını bilgilendirmektedir (Galeotti, 2016; 2).

Soğuk Savaş'ın sona ermesiyle KGB'de işlevini tamamlamış yerini FSB (Federal Güvenlik Servisi) ye bırakmıştır (Andrew ve Gordijewski, 1991; 1). FSB, Rus İstihbarat Servisi (SluzhbaVneshney Razvedki/ SVR) ve GRU sahip oldukları siber kapasiteleri bağlamında Rusya'nın siber savunma ve saldırı kapasitesinde önemli bir rol oynamaktadırlar. Bu bağlamda, SVR KGB'nin uzantısı olarak Rusya'nın dış istihbarat faaliyetlerini yürütmektedir. SVR, GRU ile birlikte askeri alandan, ekonomiye ve siyasete ilişkin tüm verilerin elde edilmesinden iletişim, bilim ve teknoloji konularına uzanan geniş bir alanda istihbarat toplamaktadır (Darıcılı ve Özdal, 2017; 126).

Rusya, 1995 yılında hem içerde Çeçenistan ile yaşadığı sorunlar hem de uluslararası konjonktürel yapı gereği FSB'yi kurmuştur. FSB diğer istihbarat servislerine oranla karşı-istihbarat ve terörle mücadele konusunda daha fazla ekonomik destek almış ve büyük bir sorumluluğa sahip olmuştur. İstihbarat faaliyetlerini sürdüren Rusya, 1999 yılında casusluk yaptığı gerekçesiyle ABD' li bir diplomatını sınır dışı etmiş, buna karşılık Rus diplomat Stansilav Gusev, ABD Dışişleri Bakanlığının ofisine casus dinleme aracı olan "böcekleri" yerleştirdiği gerekçesiyle ABD tarafından sınır dışı edilmiştir (IOSS, 2017:12).

Putin'in 2000 yılında iktidara gelmesiyle birlikte, Rus istihbarat servisi yeniden yapılandırılmış, birçok meslektaşı istihbarat ve ulusal güvenlik kurumlarında üst düzey görevlere atamıştır. Putin, Afganistan'ın işgalinde, Çeçenistan'ın kontrol edilmesinde, Ukrayna müdahalesinde ve Kırım ilhakında ve Suriye politikalarında istihbaratı çok aktif bir biçimde kullanmış ve yaptığı açıklamalarla (Pringle, 2013:23) .Rusya'nın eski güçlü günlerine ulaşmak için istihbaratın önemine dikkat çekmiştir (Smith, 2018; 10).

Sonuç olarak Rus istihbaratı küreselleşmenin de etkisiyle değişen, dönüşen ve gelişen teknolojiye adapte olmuş ve dünyadaki istihbarat faaliyetlerini siber alana taşımıştır. Rusya, siber alanda da güvenliğini sağlamak, sahip olduğu bilgiyi ve donanımı güvence altına almak ve korumak için siber güvenlik ve siber istihbarat alanlarında faaliyetlerine devam etmektedir (Craigen, vd. 2014; 15).

5. Rus Dış Politikasında Siber İstihbarat

Rusya'nın siber gücü dünyadaki diğer siber güçlerle yarışabilecek bir büyüklüğe sahiptir. Çin ve ABD ile birlikte Rusya, siber alanda istihbarat toplama, siber saldırılar gerçekleştirme ve siber güvenliği sağlama konusunda oldukça başarılıdır. Rusya, SSCB (Sovyet Sosyalist Cumhuriyetler Birliği) zamanında bile siber alanda istihbarat faaliyetlerini sürdüren ve bu konu ile ilgili pek çok önemli çalışmalar yapmış bir devlettir.

Rusya siber kelimesi yerine genellikle bilgi güvenliği ifadesini kullanmayı tercih etmektedir. Rusya Federasyonu yayınlamış olduğu Bilgi Güvenliği Doktrini'nde bu tutumunu belli etmiş doktrin içerisinde internet kelimesinden bahsetmemiştir. Rusya'nın bilgi kavramı için belirttiği hedefler, ulusun bilgi ve kültürünü korumak ve serbest bilgi akışını garanti etmeye yöneliktir. 2000'de kabul edilen Rus Bilgi Güvenliği Doktrini, bilgi güvenliğini; "bireyin, toplumun ve devletin sahip olduğu bilgilerin ve Rusya'nın ulusal çıkarlarının korunması" olarak açıklamıştır. Rusya'nın bilgi politikasının temel amacı, sosyal ve politik istikrarın sağlanmasına katkıda bulunmaktır. Rusya hükümeti, devlet bilgi politikasının dört temel hedefini olduğunu belirtmiş bunlar; Rus toplumu için bir değerler sistemi geliştirmek; devlet politikalarına yönelik kamu desteğini ulusal ve uluslararası kamuoyundan sağlamak; yıkıcı ideolojilere, dini aşırılığa, ulusal ve uluslararası seçim bölgelerinin devlet politikaları üzerindeki dezenformasyonuna karşı koymak; istikrar ve güvenliğin bozulmasının ve ulusal bilgi altyapısının (askeri, teknolojik ve politik yönleri dâhil) işleyişini korumayı hedeflemektir. Rusya bilgi güvenliğine verdiği bu önem nedeniyle siber güvenliğini güçlendirmek için hem ulusal hem de uluslararası boyutta pek çok çalışma yapmaktadır (Gady ve Austin, 2010; 5).

Siber güvenlik analisti Keir Giles tarafından hazırlanan ve Rus Savunma Bakanlığı tarafından 2011 yılında yayınlanan, Bilgi Çağında Rus Silahlı Kuvvetleri'nin Faaliyetlerine İlişkin Kavramsal Görüşler (Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space) adlı belge Rus ordusu ile ilişkilendirilmiştir. Belgede silahlı kuvvetlerin siber alanda da faaliyet göstermesi gerektiği vurgulanmıştır. Rus ordusunun karşı karşıya kaldığı bilgi tehditlerinin siber alanda ordu ile özleştirilmesi, Rusya'nın bu konuyu ne kadar dikkate aldığının bir kanıtı olarak

görülmektedir. Rusya Federasyon'u ayrıca bilgi güvenliğini de istihbarat servisleri ile birlikte sürdürmekte, dış istihbarat servisleri kullanılarak yürütülen yıkıcı operasyonların oluşmasının engellenmesi, Rusya'ya karşı yapılacak siber saldırılara karşı önlem alınması ve ülkenin siber güvenliğin temin edilmesi, istihbarat servislerinin görev kapsamına girmektedir (Darczewska, 2016; 8).

Rusya da teknolojik değişim ve gelişimlerle, güvenli bilginin sağlanması ve kullanılması açısından gerekli alt yapı ve donanımlarını oluşturmuştur. Siber güvenliğe çok önem veren Rusya aynı zamanda siber gücünü de sürekli olarak üst düzeyde tutan bir devlettir. İstihbarat konusundaki uzun geçmişi de düşünüldüğünde, Rusya'nın siber istihbarat alanında önemli bir rol alması kaçınılmazdır. Dolayısıyla, Rus dış politikası, iç veya dış unsurlara göre şekil alsa da siber alandan alınan istihbaratlar dış politikayı şekillendirmektedir. Bu bağlamda siber casusluğun ilk belgelenen vakası, *Cuckoo's Egg* dir. Bir KGB ajanı olan Markus Hess tarafından 1986'da Lawrence Berkeley Ulusal Laboratuvarı'nda gerçekleştirilmiştir. ABD'ye karşı bir dizi bilgisayar saldırısı gerçekleştiren Hess, ABD ile ilgili ekonomik, askeri, siyasi konuları içeren pek çok gizli bilgiye ulaşım sağlamış ve bu bilgeleri Soğuk Savaş'ın o çekişmeli dünyasında istihbarat olarak kullanmıştır. Bu olay siber casusluğun ilk belgelenen vakasıdır (Jupillat, 2016; 934).

Soğuk Savaş'ın sonlarına doğru Rus istihbaratının rakiplerine yönelik gerçekleştirmiş olduğu bir diğer saldırı da *Moonlight Maze* olarak adlandırılan siber saldırıdır. Başta ABD olmak üzere, İngiltere, Kanada, Brezilya ve Almanya gibi pek çok devlet Rus istihbarat faaliyetlerinin hedefi olmuş ABD Savunma ve Enerji Bakanlığı'na, NASA'ya ve üniversitelere ait binlerce gizli bilgiyi sağlayan Rusya bu alanda bir uyanışı başlatmıştır. O zamana kadar eşi benzeri görülmemiş bir ölçekte ve koordineli bir şekilde gerçekleşen bu saldırı siber alandaki bilgilerin güvenliğinin sağlanmasına yönelik olan inancı canlandırmıştır (Doman, 2019). Rusya için, siber çatışmalar bir düşmana karşı istenen hedeflere ulaşmak ve istihbarat elde etmek için kullanılacak bir güç politikası stratejisidir. Bu nedenle yapılan tüm saldırılar aslında dış politikanın şekillenmesinde etkili olmaktadır. Sovyetler Birliği döneminde gerçekleşmiş bu iki istihbarat temelli siber saldırı ile Soğuk Savaştaki en önemli rakiplerini egale etmek isten Ruslar siber alanda istihbarat sağlayarak bir adım öne geçmeyi hedeflemiştir.

Sovyet sonrası dönemde de istihbarata yönelik tutumunu değiştirmeyen Rusya yapmış olduğu siber müdahaleler ile kimi zaman bilgi toplamış kimi zaman da istihbaratın bir diğer amacı olan düşman devletlerin sistemlerini bozarak ilerleme stratejisini kullanmıştır. Estonya ve Gürcistan saldırıları bu duruma örnektir. Estonya'daki heykel krizi sonucunda iki haftalık bir saldırıya maruz kalınmış ve bu saldırı yaklaşık 750 milyon dolara mal olmuştur. Bu saldırıda, heykel krizinin ardında yatan sebep, Estonya'nın, 2007'ye kadar AB ve NATO'ya tam üyelik sürecini başlatmasıdır. Dolayısıyla Rus dış politikası ile çelişen bu durum hem Rusya'nın bölgedeki gücünü hem de dış politika hedeflerine ulaşmakta her türlü mekanizmayı kullanabileceğini göstermesi bakımında önemlidir. Bu doğrultuda Estonya saldırıları siber istihbarat ve dış politika ilişkisini iyi açıklamaktadır (Maness ve Valeriano, 2015; 113).

Rusya Yakın Çevre Doktirini kapsamında Avrasya coğrafyasındaki yayılmacı ve saldırgan tutumunu devam ettirerek bu coğrafyada siber saldırılarını bir güç unsuru olarak kullanmıştır. Gürcistan'da bulunan Güney Osetya bölgesinin bağımsızlık talebi sonucunda taraflar arasında ortaya çıkan savaşa Rusya'da dâhil olmuş karadan yürüttüğü bu savaşı siber alandan yaptığı saldırılar ile de desteklemiştir. Gürcistan'a ait tüm medya ve telekomünikasyon kanallarına erişimi engelleyen Rusya yaklaşık 5 gün içerisinde Gürcistan ordusunu yenip Güney Osetya'yı güvenli hale getirmiş ve bunu yaparken de yaptığı siber saldırılar ile dünyadaki diğer devletlerin haberi bile olmadan hedeflerine kolaylıkla ulaşmada bir avantaj sağlamıştır. Gürcistan'ın Bağımsız Devletler Topluluğu'na girmesini isteyen Rusya hem ayrılıkçı hareketleri destekleyerek hem de yürütülen savaşta rol alarak dış politika hedeflerine ulaşma doğrultusunda adım atmıştır (Popescu, 2018; 59).

Rusya'nın dış politikasında Ukrayna, hem barındırdığı Rus etnik nüfus hem de Karadeniz'in jeopolitiği dikkate alındığında önemli bir konumdadır. Özellikle NATO'nun genişlemesi, Gürcistan ve Ukrayna üzerinden Karadeniz'e yerleşmesi Rusya'nın ulusal çıkarları ve güvenliği için açıkça tehdit olarak algılanmıştır. Bu nedenle, Rusya'nın yayılmacı ve saldırgan tutumunda Ukrayna'nın hem içerden hem de dışardan Rus hegemonyası altına alınmak istenmesi görülmektedir. Bu bağlamda Rusya-Ukrayna ilişkileri, Rus diasporasını koruma endişesiyle hareket eden Rusya'nın Kırım ilhakı ile olumsuz bir sürece girmiştir. Rusya için Ukrayna, Avrasya'daki hâkimiyetinin önemli bir parçasıdır. Bu nedenle Rus dış politikası,

Gürcistan'da olduğu gibi Ukrayna'da da askeri, ekonomik, psikolojik yöntemlerini siber alana entegre etmiştir. Örneğin, Ukrayna parlamenterlerinin cep telefonlarına istihbarat amaçlı mesajlarla siber saldırılar düzenlenmiştir. Bunun dışında Ukrayna Güvenlik Servisi'nin Merkez Seçim Komisyonunun sistemlerinde seçim sonuçlarında toplanan verileri ele geçirmek üzere tasarlanan bir virüs bulunmuş ve Rus bilgisayar korsanlarının sonuçları sabote etmeye yönelik hedefleri olduğunu iddia edilmiştir. Bu durum Ukrayna seçimlerine yönelik kamuoyunu yönlendirmek amaçlı apaçık bir siber istihbarat çalışmasının yapıldığını göstermektedir (Maurer ve Janz, 2014; 3). Bu bağlamda, Genelkurmay Başkanı Valery Gerasimov'un, -Gerasimov Doktrini olarak bilinen-askeri niteliğe sahip olmayan yöntemlerin kullanılarak, daha az konvansiyonel güç ile sorunları çözme stratejisine uygun hareket edildiğini ve hedefe yönelik siber saldırılar ile avantaj sağlanmanın ve gerek altyapı gerekse ekonomik zararın beklenildiğinden daha etkili olduğu görülmüştür (Fridman, 2019; 102).

2016 yılında yapılan ABD seçimlerine Rusya'nın müdahale de bulunduğuna dair de pek çok haber çıkmış Rusya'nın kamuya açık medyayı ve daha pek çok sosyal medya uygulamasını provanda yapmak amacı ile kullandığı ABD'de bulunan pek çok tartışmayı özellikle rahatsız olan kesimlerin gündemine getirerek demokratik sürecin gidişatının yönlendirilmesinde etkili olmaya çalıştığı iddia edilmiştir (Galante ve Ee, 2018; 2).

Siber saldırıların nereden geldiğini bilmek elbette çok zordur. Saldırıların bir devlet boyutu bir de sivil boyutu olduğu düşünüldüğünde devlet düzeyinde yapılan bilgi toplama çalışmaları istihbarat için daha etkili olacaktır. Bunun farkında olan Rusya'da kendi istihbarat teşkilatının görevleri arasına siber alanda bilgi toplamak ve öz bilgileri koruma görevi vermiştir. Günümüz dünyasında yaşanan pek çok siber saldırı bulunmakta her gün bir başka siber saldırı haberi çıkmaktadır. Örneğin 2015 yılında çıkan bir haber: Rus istihbarat teşkilatının, Finlandiya'nın bilgisayar güvenlik şirketi olan F-Secure ile Çeçenya, Ukrayna, Gürcistan, Türkiye, Polonya ve ABD gibi ülkelere yönelik olarak gerçekleştirdiği iddia edilen siber istihbarat saldırılarından bahsetmiş, Rusya'nın dış politika amaçlarını daha da ilerletmek için bilgisayar korsanlarını aktif olarak kullandığını belirtmiştir. Bu haberin doğru olması durumunda Rusya'nın siber istihbarat faaliyetlerini ne derecede ilerlettiğini görmek mümkündür. Zira izlenen devletler Rus dış politikasında adı sık sık anılan devletlerdir ve toplanan bilgiler Rus dış politikasının şekillenmesinde etkili olmaktadır (CSRI, 2019).

Sonuç olarak Rusya'nın istihbarat faaliyetleri, Avrupa hükümetlerinden daha başarılı ve etkili olma, olası düşmanları dengesizleştirme, Rusya'nın ekonomik çıkarlarını geliştirme gibi birçok alana yönelik çalışmakta ve değişen ve gelişen teknolojik gelişmeler doğrultusunda siber istihbarat alanı da bu hedefleri gerçekleştirme doğrultusunda kullanılmaktadır. Siber alandan alınan pek çok bilgi bugün hem istihbarat toplanmasına yardımcı olmakta hem de dış politika kararlarının daha etkili olmasına katkı sağlamaktadır.

6. Sonuç ve Değerlendirmeler

Devletler uluslararası alanda epistemolojik ve ontolojik kaygılarla kendi çıkarlarını uluslararası topluma kabul ettirme amacıyla hareket etmektedirler. Bu doğrultuda devletlerin sert güç, yumuşak güç, diplomasi, uluslararası örgütler, ittifaklar, propaganda gibi pek çok yöntemle dış politikalarına yön verdikleri görülmektedir (Stanzel, 2018; 10). İstihbarat da bu yöntemlerden birisidir. Dolayısıyla istihbarat ile dış politika birbirine paralel hareket etmekte, bilginin elde edilmesi ve işlenmesi ve dış politika yapıcıları tarafından uygulanabilir olması devletlerin etkinliğini, gücünü ve uluslararası sistemdeki konumunu etkileyecektir (Bimfort, 1995;76).

Devletlerin ve devlet dışı aktörlerin istihbarat çalışmalarının amacına ulaşabilmesi için mevcut imkânların ötesine geçip, yeni stratejiler ve yöntemler kullanmak istihbarat çalışmalarına yeni bir boyut kazandıracaktır. Bu süreç dijitalleşen bilginin daha etkin, daha hızlı ve daha kesin verilerle analiz sürecinin tamamlanmasına ve elde edilen sonuçların uygulanabilirliği imkân verecektir. Böylece devletlerin ulusal güvenlik ve çıkarlara yönelik etkili sonuçlar alınabilinecektir. Bu doğrultuda Rusya, tarihi boyunca istihbarat kavramına önem vermiştir. Güvenlik paranoyası içinde olan Rusya, istihbarat faaliyetlerini aktif bir biçimde kullanmış/maktadır.

Küresel yeni büyük oyunda geri kalmamak için her alanda istihbarat çalışmalarını sürdüren Rusya, Çin, Hindistan, Pakistan, İran gibi nükleer güçlerle işbirliği içerisinde uluslararası sistemin çok kutupluluğundan

yana tavır sergilemekte, ABD'nin tek kutuplu hegemonyasına karşı durmaktadır. Dolayısıyla Rusya büyük güç olabilme hedefine ulaşabilmek için siber güvenliğin sağlanması için siber istihbarat faaliyetlerini güncelleyerek her ortama adapte olmak koşuluyla diğerlerinden hep bir adım önde olabilmek için çalışmalarını sürdürecektir.

Kaynakça

Akyeşilmen, Nezir. Disiplinlerarası Bir Yaklaşım ile Siber Politika ve Siber Güvenlik, Ankara, Orion Kitabevi, 2018.

The Cheka. alphahistory.com, [Online] Available at: <https://alphahistory.com/russianrevolution/cheka>, [Erişim tarihi: 06.06.2019].

Alsmadi, Izzat. The NICE Cyber Security Framework: Cyber Security Intelligence and Analytics, Swetzerland, Springer, 2019.

Andrew, Christopher. Oleg, Gordijewski. KGB, Przelozyl Rafal Brzeski Dom Wydawniczy Bellona Warszawa,1999.

İnternet Live Stats. internetlivestats.com, [Online] Available at: <https://www.internetlivestats.com/>, [Erişim tarihi: 02.11.2019].

Barbosa H., Breda, F. ve Morais T. (2017). *"Social Engineering And Cyber Security"*, Conference: International Technology, Education and Development Conference, INTED.

Bimfort, M. T. (1995). "*A Definition of Intelligence*", Study of Intelligence, 2 (4): 75-78.

Cardillo, R. (2018). "*Geospatıal-Intelligence (Geoınt) Basıc Doctrıne*", Natıonal System For Geospatial Intelligence, Publication 1.0, s. 18-142.

CIA. (2010). INTelligence: Human Intelligence, cia.gov, [Online] Available at: <https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-human-intelligence.html>, [Erişim tarihi: 08.11.2019].

Craigen, D., Thibault, N. ve Purse, R. (2014). "*Defining Cybersecurity, Technology Innovation*", Management Review, 4 (10): 13-21.

Russian State in Cyber Spy Claims (2015). csri.info, [Online] Available at: <http://www.csri.info/russian-state-in-cyber-spy-claims/>, [Erişim tarihi: 03.11.2019]

Çamaş, T. (2018). "*Opriçnina Teşkilatı ve Rus Merkezileşmesine Etkileri*", Vakanüvis-Uluslararası Tarih Araştırmaları Dergisi, 3 (2): 112-136.

Darczewska, Jolanta. Russia's Armed Forces on the Information War Front. Strategic Documents, Warsaw, Centre for Eastern Studies, 2016.

Darıcılı, A. B. ve Özdal, B. (2017). *"Rusya Federasyonu'nun Siber Güvenlik Kapasitesini Oluşturan Enstrümanların Analizi"* Bilig, sayı: 83, s. 121-146.

Doman, C. (2016). The first cyber espionage attacks: How Operation Moonlight Maze made history, [Online] Available at: <https://medium.com/@chris_doman/the-first-sophistiated-cyber-attacks-how-operation-moonlight-maze-made-history-2adb12cc43f7>, [Erişim Tarihi: 03.11.2019].

Ettinger, Jared. (2019). Cyber Intelligence Tradecraft Report the State of Cyber Intelligence Practices in the United States, Rapor, Carnegie Mellon University Software Engineering Institute, United States.

Fidan, H. (1999). "*Intelligence and foreign policy; A comparison of British, American and Turkish intelligence systems*", Yayımlanmamış yüksek lisans tezi, Bilkent Universitesi Ekonomi ve Sosyal Bilimler Enstitüsü Uluslararası İlişkiler Anabilim Dalı.

Fridman, O. (2019). "*On 'Gerasimov Doctrine': Why the West Fails to Beat Russia to the Punch"*. Prism, 8 (2): 101-112.

Gady, Franz Stefan ve Austin, Greg, Russia, The United States, and Cyber Diplomacy, Opening the Doors, New York, EastWestInstitute, 2010.

Galante, Laura ve Shaun, Ee. Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents, Washington, Atlantic Council, 2018.

Galeotti, M. (2016). *"Putin's Hydra: Inside Russia's Intelligence Services"*, ECFR/169, www.ecfr.eu, [Erişim tarihi: 21.11.2019].

Gökduman, Mert., "*Sinyal İstihbaratı*", Rapor, Ankara, Teknolojik Düşünce Merkezi Analizi, Ankara, 2018.

Guinchard, A. (2011). "*Between Hype and Understatement: Reassessing Cyber Risks As A Security Strategy*", Journal of Strategic Security, 4(2): 75-96.

INSA. (2015). "*Cyber Intelligence: Preparing Today's Talent for Tomorrow's Threats"*, Intelligence and National Security Alliance: Cyber Intelligence Task Force, September 2015, s. 2-17.

IOSS, Inteagency Opsec Support Staff. Intelligence Threat Handbook, Operations Security Information Series, United States, 1996.

Johnson, Loch K. Strategic Intelligence: Understanding the Hidden Side of Government, London, Preager Security International, 2007.

Jupillat, Nicolas. (2016). "*From the Cuckoo's Egg to Global Surveillance: Cyber Espionage that Becomes Prohibited Intervention*", NCJ Int'l L:42, 933.

Katz, Rebecca. Jim, Banaski. Essentials of Public Health Preparedness and Emergency Management, Burlington, Jones & Bartleed, 2018.

Keleştemur, Atalay, "Siber İstihbarat Tanımı ve Faaliyet Alanı", [Online] Available at: <https://www.academia.edu/30032177/Siber_%C4%B0stihbarat_Tan%C4%B1m%C4%B1_ve_Faaliyet_Alan%C4%B1>, [Erişim tarihi: 03.10.2019].

Major, George J. The Nature of Future: Intelligence Organizations:, Kansas, School of Advanced Mılıtary Studıes Monograph Approval 1995.

Manasia, L. ve.Andrei, P. Ianoş, M.G. (2018). "*Memories from the future: Is digital intelligence what matters in the forthcoming society*?", 10th International Conference on Education and New Learning Technologies.

Maness, Ryan C. ve Brandon Valeriano, Russia's Coercive Diplomacy Energy, Cyber, and Maritime Policy as New Sources of Power, New York, Palgrave Macmıllan, 2015.

Maurer, T., Janz, S. (2014). *"The Russia-Ukraine Conflict: Cyber and Information Warfare in a Regional Context"*, ISN ETH Zurich, [Online] Available at: <https://www.files.ethz.ch/isn/187945/ISN_184345_en.pdf>, [Erişim tarihi: ?]

Mithas, S. ve McFarlan, F. W. (2017). *"What is Digital Intelligence?,"* IEEE IT Professional, 19 (4): 3-6

Murray, M. (2016). "*Big Data And İntelligence: Applications, Human Capital, And Education*", Journal of Strategic Security, 9 (2): 92-121.

North Atlantıc Treaty Organızatıon (NATO):Standardızatıon Agency (NSA). Nato Glossary of Terms and Definitions, 2008.

Omand, D. (2015). "*Understanding Digital İntelligence and the Norms That Might Govern İt"*, International Governance Innovation and Chatham House. Oxford English Dictionary. [Online] Available at: <https://dictionary.cambridge.org/tr/s%C3%B6zl%C3%BCk/ingilizce/intelligence?q=%09intelligence>, [Erişim tarihi: 23.05.2019].

Pace, Chris. The Threat Intelligence Handbook: A Practical Guide for Security Teams to Unlocking the Power of Intelligence, Annapolis, CyberEdge Group, 2018.

Polgar, Thomas. The KGB an Instrument of Soviet Power, The İntelligence Profession Series:3, The Association of Former Intelligence Officers (AFIO), Virgina, 1989.

Popescu, Nicu ve Secrieru, Stanislav. Hacks, Leaks and Disruptions Russian Cyber Strategies, Paris, Chaillot Papers, 2018.

Pringle, Robert W. Historical Dictionary of Russian and Soviet Intelligence, Historical Dictionaries of Intelligence and Counterintelligence, No. 5, United States, Scarecrow Press, 2006.

Richard L. Bernard. Electronic Intelligence (ELINT) at NSA, Cryptologic History National Security Agency, USA, 2009.

Seng, Aaron Chia Eng. (2007). "MASINT: "*The Intelligence of the Future*", DSTA Horizons, s. 108-120.

Shetty, Dinesh. Social Engineering: The-Human-Factor, [Online] Available at: <https://www.exploitdb.com/docs/english/18135-social-engineering---the-human-factor.pdf>, [Erişim tarihi:14.11.2019].

Smith, Ben. (2018). Russian İntelligence Services and Special Forces, Briefing Paper, Number CBP 8430, 30 Ekim.

Spracher, William C. National Security İntelligence Professional Education: A Map Of US Civilian University Programs and Competencies, The George Washington University, 2009.

Stanzel, V. New Realities in Foreign Affairs: Diplomacy in the 21 st Century, German Institute for International and Security Affairs SWP Research Paper 11, 2018.

Türk Dil Kurumu. [Online] Mevcut: <http://www.tdk.gov.tr/index.php?option=com_gts&kelime=istihbarat>, [Erişim tarihi: 23.05.2019].

UNGA, Unıted Natıons General Assembly. (1965). Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, A/RES/20/2131.

United States Army (2016). Human Intelligence Collector Operations, Washington, [Online] Available at: <http://fas.org/irp/doddir/army/fm2-22-3.pdf> [Erişim tarihi: 08.11.2019]

United States Marine Corps (USMC). Signals Intelligence, Washington, Department of The Navy, 2018.

United States of America, Office of the Director of Natioal İntelligence (USANI). (2013). *"U.S National İntelligence: An Owerview"*, Taslak, Washington.

Ümit, Özdağ. İstihbarat Teorisi, Ankara, Kripto Yayınları, 2014.

Ünver, A. (2018). Digital Open Source Intelligence and International Security: A Primer, EDAM Cyber Governance and Digital Democracy, [Online] Available at: <https://edam.org.tr/en/digital-open-source-intelligence-and-international-security-a-primer/>, [Erişim tarihi: 19.11.2019].

Vardangaos, G. (2016). "*Cyber-İntelligence and Cyber Counterintelligence (CCI): General Definitions and Principles*", International Strategic Analyses (KEDISA), Research Paper No.1. [Online] Available at: <https://kedisa.gr/wp-content/uploads/2016/07/Cyber-intelligence-and-Cyber-Counterintelligence-CCI-General-definitions-and-principles-2.pdf>, [Erişim tarihi: 14.11.2019].

Waller, Simon. What is Digital Intelligence?, [Online] Available at: https://www.simonwaller.com.au/digital-intelligence/ [Erişim Tarihi: 02.11.2019].

Warner, Michael. (2002). "*Wanted: A Defmition of Intelligence*", Studies in Intelligence, 46 (3): 15-22.

Zeng, D. D., Chen, H., Lusch, R. ve Li, S. (2011). "*Social Media Analytics and Intelligence*", Intelligent Systems, 25(6): 13 – 16.

Zickel, Raymond E. Soviet Union a Country Story, Washington, D.C., Federal Research Division Librarary of Congrees, 1991.