Harbin Beşinci Boyutunun Yeni Gereksinimi: Siber İstihbarat

The New Requirement for the Fifth Dimension of the War: Cyber Intelligence

Gökhan BAYRAKTAR*

Öz

Bir disiplin haline getirilmesinden bu yana yaklaşık yarım yüzyıl geçmiş olan istihbarat kavramı, yapıları ve faaliyet alanları tehdit algılamalarındaki değişime paralel olarak sürekli değişmiştir. Siber uzayda yaşanan gelişmeler sayesinde geleneksel istihbarat giderek yerini spesifik istihbarat alanlarına bırakırken, söz konusu gelişmeler harp ortamına da farklı bir bakış açısı getirmiştir. Devletlerin kritik sektörlerinin bilgi altyapılarını hedef alan siber savaş, başta modern ülkeler olmak üzere siber bağımlılıkları yüksek olan devletlerin ulusal güvenlikleri için gerçek bir tehdit oluşturmaktadır. Siber savaşın asimetrik özelliği nedeniyle bireylerden karmaşık ulusal organizasyonlara kadar geniş bir yelpazede olan tehdidin kaynağının tespit edilememesi, çok düşük maliyetlerle büyük etkiler oluşturması ve konvansiyonel silahlara başvurmadan sadece görünmeyen saldırıların kullanılmaya başlanması, siber savaşın önemini daha da arttırmakta ve bu tehdide karşı siber istihbarat kavramına olan gereksinimi ön plana çıkarmaktadır. Bu çalışmada uluslararası ilişkilerde sınırları tanımlanamayan siber uzayda icra edilecek siber savaşların devletlerin ulusal güvenliklerini tehdit eden yeni bir savaş çeşidi olduğunu açıklamak, siber savaşlarda inisiyatifi kazanabilmek ve tehditle ilgili değerlendirmeler yapabilmek için önem arz eden siber

* Hv. İsth. Kur. Bnb., Genelkurmay Başkanlığı, E-posta: gokhanbayraktar@hotmail.com

istihbarat kavramı ile faaliyet alanlarını tanımlamak ve yöntemlerini ortaya koymak amaçlanmıştır.

Anahtar Kelimeler: *Siber Uzay, Siber Tehdit, Siber Güvenlik, Siber Savaş, İstihbarat.*

Abstract

The structure and operational domain of intelligence concept have been evolving continuously in parallel to the change in threat perceptions since it became a discipline more than half a century back. All these developments brought a new approach to the area of war. Indeed, specific intelligence started to dominate the field in comparison to conventional intelligence due to the quick progress in cyber space. Cyber attacks, which usually target the information systems of the governments' critical departments, are great threat especially for the nations, which are heavily dependent to cyber space. The importance of cyber attacks rise day by day because, most of the time, detecting the source of the attack is a challenging task that might be initiated through a wide spectrum profiles ranging from simple individuals to complex organizations. Moreover, these attacks make a great impact despite their low cost. Furthermore, they are initiated through invisible methods where conventional weapons are not even utilized. Hence, the concept of cyber intelligence looms large against this threat. This paper strives to explain that cyber attacks can be classified as a new type of war, because it threatens national securities and happens in cyber space that does not have any defined borders in international relations. In addition to the above, this study defines cyber intelligence concept and its operational domain as well as it puts forth the methodology for consideration in order to gain the initiative in cyber attacks and to make analysis on the threat.

Key Words: *Cyber Space, Cyber Threat, Cyber Security, Cyber War, Intelligence.*

1. Giriş

İstihbarat, bilgi toplayıp analizler yaparak, karar vericilerin önünü aydınlatmak olarak tanımlanırken, bir yandan da karar

vericilerin belirlediği politikalar doğrultusunda psikolojik harekât, propaganda gibi yöntemler kullanarak toplumların algılarını yönetmek olarak ifade edilebilir. Askerî açıdan bir disiplin haline getirilmesinden bu yana yaklaşık yarım yüzyıl geçmiş olan istihbaratın hedefleri, çalışma metotları ve kullandığı araçlar konjonktürel olarak sürekli değişmiştir. İki kutuplu bir dengenin yaşandığı Soğuk Savaş döneminde, ulusal gücün askerî güç ile eşdeğer tutulmasıyla istihbarat, düşmanın imkân ve kabiliyetlerini keşfetmek, harp silah ve araçlarını belirlemek olarak algılanmıştır. Bu bağlamda, askerî güç öncelikli hedef hâline gelmiştir.[1]

Soğuk Savaş döneminin iki kutuplu yaklaşımının sona ermesi ile beraber gerek düşman tanımlarındaki gerekse dünyadaki güvenlik ve tehdit algılamalarında önemli değişimler yaşanmıştır.[2] Diğer taraftan bilgi teknolojilerindeki gelişmeler sayesinde geleneksel istihbarat giderek yerini spesifik istihbarata bırakmıştır. Bu hızlı değişim süreci neticesinde istihbarat yapı ve algıları da büyük ölçüde sorgulanmaya başlanmış ve değişime zorlanmıştır.[3] Bu sayede istihbarat disiplini, bir yandan yeni tehditler ile beraber yeni ilgi alanları kazanırken, diğer yandan gelişen teknoloji sayesinde haber alma yöntem ve vasıtalarına yenileri eklenmiştir.

Günümüz harekât ortamında, orduların operasyonel üstünlüklerine bakılırken veya kuvvet mukayeseleri yapılırken, harp silah araçları ve komuta-kontrol sistemlerinin yanı sıra elektronik harp kabiliyetleri ile görüntü alma, uzaktan algılama gibi İstihbarat Gözetleme Keşif fonksiyonlarının ve uzayın daha etkin kullanımının çok önemli olduğu görülmektedir.[4] Devletler tarafından tüm bu yeni yetenek kazanım çabalarına rağmen harp öncesi dönem, kriz dönemi ve düşük yoğunluklu

[1] Mesut Hakkı Caşın, "Soğuk Savaş Sonrası Askerî Stratejik İstihbaratın Yeni Vizyonu", ***Avrasya Dosyası***, 2002, Cilt:8, Sayı:2, 254-294, s. 275.

[2] Atilla Sandıklı ve Bilgehan Emeklier, "Güvenlik Yaklaşımlarında Değişim ve Dönüşüm", Atilla Sandıklı (ed.), ***Teoriler Işığında Güvenlik, Savaş, Barış ve Çatışma Çözümleri,*** Bilgesam Yayınları, 2012, 3-70, s. 25.

[3] İhsan Bal, ***Alaca Karanlıkta Terör ile Mücadele ve Komplo Teorileri***, USAK Yayınları, Ankara, 2006, s. 65-66.

[4] Hakan Canlı ve Ahmet Kandakoğlu, "Hava Gücü Mukayesesi İçin Bulanık AHP Modeli", ***Havacılık ve Uzay Teknolojileri Dergisi,*** 2007, Cilt:3, Sayı:1, 71-82, s. 76.

çatışma zamanlarında konvansiyonel silahlara başvurmadan, görünmeyen saldırı ve savunma sistemi olarak siber uzayın kullanılmaya başlandığı görülmektedir.

Siber uzayda yaşanan gelişmeler harekât ortamına farklı bir mekân boyutu eklemiş ve harplerin icra edildiği kara, deniz ve hava gibi fiziksel mekânlardan farklı olarak bütün bu boyutlarda icra edilen harekâtları doğrudan etkileyen yeni bir boyut kazandırmıştır.[5] Harbin bu boyutunda kazanılan başarıların kuvvet çarpanı etkisi oluşturduğu ve daha harp başlamadan veyahut kriz döneminde stratejik seviyede uygulanan siber saldırılar sayesinde düşmanın harp etme azim ve kararının kırılabileceği görülmektedir. Hatta siber uzay barış döneminden itibaren düşmanın imkân ve kabiliyetlerini geliştirecek yeteneklerine yapılacak saldırılar ile tehdidin daha oluşmadan yok edilmesine imkân sağlayabilmektedir. Tüm bu gelişmeler gelecekte siber savaşın önemini daha da arttırmakta ve bu tehdide karşı siber istihbarat kavramına olan gereksinimi ön plana çıkarmaktadır.

Bu makaledeki amacımız; uluslararası ilişkilerde sınırları tanımlanamayan siber uzayda icra edilecek siber savaşların devletlerin ulusal güvenliklerini tehdit eden yeni bir savaş çeşidi olduğunu açıklamak ve siber savaşlarda inisiyatifi kazanabilmek ve tehditle ilgili değerlendirmeler yapabilmek için önem arz eden siber istihbarat kavramını tanımlamak ve yöntemlerini ortaya koymaktır. Bu çalışma; güvenlik ve tehdit algılamalarındaki değişime paralele olarak istihbarat disiplinin konjonktürel olarak değişimini inceleyip, siber tehditlerin ve etkilerinin yaşandığı siber savaşlarda spesifik bir istihbarat alanı olarak ihtiyaç haline gelen siber istihbaratın gereksinimlerini belirterek, siber istihbaratın yöntemleri üzerine bir çıkarımla sonlandırılacaktır.

2. İstihbarat Kavramı ve Teori Sorunsalı

Arapça kökenli bir kelime olan istihbarat, "haber alma" anlamındadır. Türk Dil Kurumu Sözlüğü ise "haber alma" tanımının

[5] Cengiz Özteke, "Cyber-A New War Domain", ***Defence Turkey,*** 2013, Vol.8, No.48, 8-9, p. 8.

yanında "yeni öğrenilen bilgiler, haberler, bilgi toplama" olarak tanımlamaktadır.[6] Bal, "eldeki verilerin en iyi şekilde kullanılması ve bilginin gücü"[7] tanımlamasında ise yalnızca haber alma faaliyetine değil, elde edilen verilerin başarılı bir şekilde kullanılması ve bilginin güce dönüştürülmesine vurgu yapmaktadır. Tezsever ise istihbaratı "işleme tabi kılınan değerlendirilmiş bilgi"[8] diye tanımlayarak elde edilen haber ve bilgilerin istihbarat hâline dönüşebilmesi için belli işlemlere tabi tutulması gerektiğine dikkat çekmektedir.

İnsanoğlu merak ve korku duygusunun sonucu olarak gelecekte nelerin olabileceğini bilmek ve mümkünse bunu yönlendirebilmek için çeşitli yöntemler geliştirmiştir. Özellikle savaş alanlarında, düşman niyetlerini öğrenme çabalarıyla desteklenen bu yöntemler, istihbaratın bir disiplin haline gelmesine neden olmuştur. İstihbaratın kavramsallaştırılmasıyla ilgili çalışmaların realist bir bakış açısına sahip Sun Tzu ile başladığı düşünülmektedir. Sun Tzu, devletlerin güvende olmasını savaş sanatına hâkim olmalarına bağlamış ve tüm savaşların aldatmacalara dayalı olduğunu vurgulayarak istihbarata da özel bir önem vermiştir.[9] Ancak Sun Tzu'nun istihbarat kavramı, doğal olarak, askerî istihbarat ile sınırlı kalınmıştır. İstihbaratın faaliyet alanlarının belirlenmesinde ise, Machiavelli'nin görüşlerinin önemli bir yeri bulunmaktadır. Machiavelli'nin görüşleri istihbarat dünyasının bir parçası olan örtülü operasyonların mantığının temeli olarak algılanabilir. Devletin varlığını sürdürme amacını, diğer tüm amaçların üzerinde tutan Machiavelli,[10] prensine hitaben yazdığı eserinde; herkesin zaten kötü olduğu bir ortamda, başkaları kendisine kötülük yapmadan, ahlaki değerlere bağlı kalmaksızın amacına ulaşmakta her yolu meşru

[6] ***Türkçe Sözlük-Türk Dil Kurumu***, Cilt:1, Türk Tarih Kurumu Basımevi, Ankara, 1998, s. 1107.
[7] Bal, a.g.e., s. 67.
[8] Serhat Tezsever, ***Milli Güvenliğimiz İçerisinde İstihbarat-Türkiye Cumhuriyeti ve İstihbarat Olgusu***, İ.U.Basımevi, İstanbul, 1999, s. 106.
[9] Sun-Tzu, ***Savaş Sanatı***, çev. Adil Demir, Kastaş Yayınları, İstanbul, 2001, s. 43-45.
[10] Tayyarı Arı, ***Uluslararası İlişkiler Teorileri; Çatışma, Hegemonya, İşbirliği***, Alfa Yayınları, İstanbul, 2004, s. 180.

görmekte ve amaç kazanmak olduğunda gayri ahlaki yollar ile aldatmalara başvurmayı alkışlanabilir bir tavır olarak kabul etmektedir.[11]

Devleti uluslararası ilişkilerin temel aktörü olarak kabul eden realistler için önemli olan devletin çıkarlarının korunup korunmadığıdır.[12] Güç unsuruna odaklanan gerek realist, gerekse günümüzdeki devamı olan neo-realistler, istihbarat kavramını genel olarak ihmal etmiştir.[13] Bu nedenle istihbaratın bir disiplin olarak kabul edilmesinden bu yana yaklaşık yarım yüzyıl geçmesine rağmen, istihbarat kavramının ve faaliyetlerinin tanımlamasında yaşanan zorluklar, istihbarat teorisine ulaşamamanın temel sorun alanını oluşturmaktadır.

Scott ve Jakson, istihbarat konusunda yapılan çalışmalardaki farklılıkları üç ana başlık altında toplamaktadır. Buna göre ilk yaklaşımda istihbarat, savaşta ve barışta politika yapıcılar tarafından verilen kararlara açıklık getirebilmek amacıyla yeni bilgilerin elde edilmesi için bir araçtır. Bu yaklaşımı paylaşan araştırmacılar istihbarat toplama sürecine, istihbarat kaynaklarına ve karar verme zinciri boyunca istihbaratın doğru kullanımına özel önem verirler. İkinci yaklaşım, istihbarat sürecindeki hataları ve başarıları açıklamak için genel bir model oluşturmaya çalışmaktadır. Bu görüşü paylaşan araştırmacılar çoğunlukla analiz ve karar seviyesiyle ilgilenirler. Üçüncü yaklaşım ise, istihbaratın devletin bir kontrol mekanizması olarak politik fonksiyonuna odaklanır.[14] Fakat bu gruplandırma istihbaratın ne olduğu ve ne yapması gerektiği konusuna yeterli bir açıklık getirememiş; istihbarat dış politikada karar verme sürecinin bir basamağı, iç politikada ise devletin kontrol mekanizması düzeyine indirgenmiştir.

İstihbarat teori arayışlarına tarihsel bir bakış açısı ile yaklaşan Kahn ise teorisinde istihbaratın geçmişi, bugünü ve geleceği ile

[11] Deniz Ülke Arıboğan, ***Kabileden Küreselleşmeye Uluslararası İlişkiler Düşüncesi***, Sarmal Yayınevi, İstanbul, 1998, s. 78-90.
[12] Arı, a.g.e., s. 163-165.
[13] Len Scott and Peter Jackson, "The Study of Intelligence in Theory and Practice", ***Intelligence and National Security***, 2004, Vol.19, No.2, 139-169, p. 143.
[14] Scott and Jackson, a.g.m., p. 143.

ilgilenerek onun günümüzdeki önem seviyesine nasıl yükseldiğini ve çözümsüz ana sorunlarını belirlemeyi hedef almaktadır. Kahn, teorisinde, tarihsel süreç içerisinde istihbaratı yalnızca askerî yönden ele alarak, modern istihbaratın savunmanın belirleyici unsuru olduğunu ve saldırıda ise belli şartlara bağlı olduğunu savunmaktadır.[15] Kahn'ın istihbarat teorisinin en önemli eksikliği; sivil istihbarat organizasyonlarını görmezden gelmesi ve istihbaratı karar için sağlanan bilgi desteği olarak kavramsallaştırmasıdır.

Johnson ise istihbarat kavramının üç farklı boyutuna vurgu yaparak istihbarat faaliyetlerinin planlama/yönlendirme, toplama, işlem, üretim/analiz ve dağıtım diye sıralanabilecek istihbarat akışını açıklayan basamaklar etrafında inşa edilebileceğini, dış ülkelerdeki olayların gizli yollardan manipülasyonunu (örtülü operasyonlar) ve dış istihbarat örgütlerinin engellenmesi ve karşı korunması gerektiğini savunmuştur.[16] Johnson'un kurmaya çalıştığı teori, istihbaratı politika sürecinde yalnızca bilgi sağlayıcı olmaktan çıkartmakta; yabancı istihbarat örgütlerinin faaliyetlerine engel olmayı da istihbaratın görevleri arasına sokmaktadır.

Bu teoriler ışığında istihbarat kavramı, elde edilen bilgileri sistematik olarak tasniflemek, bilimsel ve istatistikî yöntemleri kullanmak suretiyle analiz etmek ve elde edilen ürünleri kıymetlendirerek istihbarat üretmek olarak tanımlamak mümkündür. İstihbaratın faaliyet alanları ise devletin kontrol fonksiyonundan ötürü tehdidin seviyesine göre yakın ve uzak tehlikelerin engellenmesi amacıyla karar vericilere bilgi desteği sağlamak, propaganda, psikolojik harekât gibi örtülü operasyon yöntemleri ile olayları yönetmek ve son olarak düşmanın veya muhtemel düşmanın istihbarat faaliyetlerini engellemek olarak ifade edilebilir. Böylece istihbarat, hem muhtemel risk ve fırsatları önceden değerlendirerek politika yapıcıların elini kuvvetlendirmekte,

[15] David Kahn, "İstihbaratın Tarihsel Teorisi", ***Avrasya Dosyası***, 2002, Cilt:8, Sayı:2, 5-20, s. 5-7.
[16] Loch K. Johnson, "Bricks and Mortar for a Theory of Intelligence", ***Compative Strategy***, 2003, Vol.22, 1-28, p. 2.

hem de alınan kararlar doğrultusunda, çeşitli yöntemler kullanarak uluslararası ortamı yönetmeye çalışmaktadır. Bu tanımlama ile istihbarat, yalnızca bilgi toplamak ve bilgileri analiz ederek karar vericilere destek sağlamak suretiyle pasif bir çerçeveye hapsedilmeyerek aktif bir konuma gelmektedir.

3. İstihbaratın Tarihsel Analizi

Canlıların yaşama savaşları, onları gelecek kararlarıyla ilgi olarak içgüdüsel de olsa analizler yapmaya zorlamıştır. Zamanla insanların topluluk hâlinde yaşamaya başlamaları, toplumlar arası mücadeleleri de beraberinde getirmiştir. İnsanların doğasında var olan ve yaşam mücadelesinin bir parçası olan istihbarat, zamanla toplumların yaşam mücadelesinin de aracı olmuştur. Fakat toplumlar kendilerine yönelecek olan tehditleri önceden haber almak için çeşitli yöntemler geliştirseler de tam olarak istihbaratın önemi anlaşılamamıştır. Sanayi devriminin sunduğu yenilikler neticesinde, orduların sahip olduğu harp silah ve araçlarının sayısı, menzili, teknik özellikleri gibi birçok konu harplerde belirleyici rol oynamaya başlamış ve savaşın gidişatını etkileyecek duruma gelmiştir. Düşman hakkında bilinmesi gerekenlerin artmasıyla istihbarat yeni hedefler kazanmış ve bu sayede istihbarata verilen önem de artmaya başlamıştır.[17]

Birinci Dünya Savaşı esnasında, orduların harekâtını kolaylaştıran telsizler, aynı zamanda düşmanın kulağı hâline gelmiş, telsiz dinlemeleri ile elde edilen bilgiler, komutanlara zaferler kazandırmıştır.[18] Ayrıca savaş boyunca ilk kez kullanılan balonlardan bir keşif aracı olarak faydalanılırken, harp meydanlarında boy gösteren uçaklar orduların ileri hatlarını gözetleyen haberciler haline gelmiştir.[19] İkinci Dünya Savaşı'nda ise radarın savaş alanında kullanılmasıyla istihbarat faaliyetlerinde önemli bir gelişme yaşanmıştır. Aynı

[17] Kahn, a.g.m., s. 7-8.
[18] National Security Agency (NSA) Resmî İnternet Sitesi, *"World War I Radio Intercept Site Exhibit"*, http://www.nsa.gov/museum/museu00012.cfm.
[19] Pamela Feltus, *"Aerial Reconnaissance in World War I"* http://www.centennialofflight.gov/essay/Air_Power/WWI-reconnaissance/AP2.htm (Erişim Tarihi: 01.02.2013).

zamanda İkinci Dünya Savaşı, muhabere şifrelemesi ve bu şifrelerin kırılması mücadelesi hâline dönüşürken, diğer taraftan uçakların gövdelerine yerleştirilen kameralar sayesinde çekilen fotoğraflar, planlayıcılar için eşsiz bir kaynak teşkil etmiştir.[20]

Doğduğu günden bu yana askerlerin elinde şekillenen istihbarat, Soğuk Savaş döneminde de ilgi alanına yine askerî güçleri yerleştirmiştir. Askerî gücün, büyük ölçüde millî güç ile eşdeğer tutulduğu Soğuk Savaş döneminde, devletler arasındaki rekabetin uluslararası sistemin temel belirleyicisi olması nedeniyle güvenlik kavramı da bu parametreler çerçevesinde ele alınmış ve devletler ait oldukları blokların askerî şemsiyesi altında güvenliklerini tesis etmişlerdir.[21] Güvenliğin konvansiyonel güçlerin mücadelesine bağlı olması nedeniyle bu dönemde de istihbarat, güvenlik odaklı bir faaliyet olarak algılanmış ve konvansiyonel harplerin ihtiyaçlarını karşılayacak şekilde yürütülmüştür.

Soğuk Savaş döneminin sona ermesiyle beraber dünya dengelerinde yaşanan büyük değişim, istihbarat anlayışına ve dolayısıyla faaliyetlerine de etki etmiştir. Bu dönemde kitle imha silahlarının yayılması, küresel terörizm, uluslararası örgütlü suçlar, etnik ve dinî çatışmalar, çevresel sorunlar gibi yeni tehditlerin ortaya çıkmasıyla istihbarat, yeni ilgi ve mücadele alanları kazanırken, diğer taraftan bilgi teknolojilerindeki gelişmelere paralel olarak küresel haber alma imkânları kazanmıştır. Bunların başında, uzayın kullanımı ve gözetleme-keşif sistemlerindeki yenilikler gelmektedir.[22] İstihbarat tarihi boyunca önemli bir yer tutan görüntü istihbaratı yeni platformlar elde etmiş, her hava koşulunda görev yapabilen, eş zamanlı görüntü iletebilen daha yüksek çözünürlüklü kamera sistemlerine kavuşmuştur.

[20] Gökhan Sarı, After Globalization Process New Horizons in Contemporary Strategic Intelligence, Yeditepe University Graduate Institute of Social Sciences, İstanbul, 2003, p. 36 (Yayınlanmamış Yüksek Lisans Tezi).

[21] Hasret Çomak, "Avrupa'da Güvenlik Yapılanmasının Yeni Parametreleri ve Türkiye'nin Konumu", ***Avrupa Araştırmaları Dergisi,*** 2006, Cilt:15, Sayı:1, 97-120, s. 100.

[22] Paul Todd and Jonathan Bloch, ***Küresel İstihbarat***, çev. Enver Günsel, Truva Yayınları, İstanbul, 2006, s. 60.

Teknolojideki hızlı ilerleme uydu resimlerini yalnızca stratejik bir değer olmaktan çıkarmış, taktik seviyeye de hizmet eder hâle getirmiştir.[23] Ayrıca günümüzde hayatın her geçen gün teknolojiye daha da bağımlı hâle gelmesi, küresel olarak bilgi toplayabilmek amacıyla Echelon ve PROMIS gibi sistemlerin doğmasına neden olmuştur.[24]

Konvansiyonel harplerin yerini asimetrik savaşlara bıraktığı günümüzde güvenlik algılamalarında önemli paradigma dönüşümleri yaşanmış ve bu dönüşüm esnasında ülkelerin güvenlik algılamalarında da önemli kaotik problemler görülmüştür.[25] Ulusal güvenlik yaklaşımları açısından, 11 Eylül saldırıları bu paradigma dönüşümünün tarihsel süreçte miat olarak kabul edildiği temel olaydır. Bunun üzerine ABD tarafından uygulamaya geçirilen "Protected War" Önleyici Savaş doktrini[26] ise bu paradigma dönüşümünün temel göstergesidir. ABD'nin 2002'de Afganistan'a yapmış olduğu "Enduring to Peace of Afganistan Operations" Barış İçin Özgürlük Harekâtı[27] ile 2003'te Irak'a yapmış olduğu "Enduring to Irak Operations" Irak'ın Özgürlüğü Harekâtı[28], her paradigma dönüşümünün sonrasında yaşanan kaos sürecini temsil etmekte olup, bu harekâtlardan elde edilen tecrübeler ile yeni güvenlik paradigması uluslararası sistem tarafından içselleştirilmiş ve uyum sağlanmaya çalışılmıştır.

[23] David D. Deptula and R.Greg Brown, "A House Divided: The Indivisibility of Intelligence, Surveillance, and Reconnaissance", ***Air & Space Power Journal***, 2008, Vol.22, No.2, 5-15, p. 7.
[24] Markus G. Kuhn, ***Compromising Emanations: Eavesdropping Risks of Computer Display***, Cambridge University Press, Cambridge, 2003, p. 14.
[25] Alvin Toffler, ***Üçüncü Dalga***, çev. Selim Yeniçeri, Koridor Yayıncılık, İstanbul, 2012, s. 13-22.
[26] The National Security Strategy of The United States of America, The White House, Washington, 2002, p. 6.
[27] Anthony Burke, "Just war or ethical peace? Moral discourses of strategic violence after 9/11", ***International Affairs***, 2004, Vol.80, No.2, 329-353, p. 332.
[28] Steven Metz and John Robert Martin, ***Decisionmaking in Operation Iraqi Freedom: The Strategic Shift of 2007***, Strategic Studies Institute, Pennsylvania, 2010, p. 12.

Bilgi teknolojilerindeki gelişmeler ışığında siber uzayda yaşanan mücadele ve geçtiğimiz 10 yıl içerisinde yaşanan siber taarruz olayları dikkate alındığında ise yakın geleceğe yönelik yapılan stratejik öngörüde silahlı çatışmaların yaşandığı asimetrik savaşların yerini ağırlıklı olarak siber savaşlara bırakacağı ve siber taarruzların harbin diğer unsurlarını da doğrudan etkileyeceği bir paradigma dönüşümüne neden olacağı değerlendirilmektedir. Ülkelerin bütün kritik altyapıları her geçen gün uzaktan kontrol ve yönetim olarak SCADA sistemlerine ve bilgi sistemlerine emanet edildiği görülmekte ve bu yapıdaki ülkelerin sayısının ve bu sistemlere bağlılıklarının zamanla arttığı bilinmektedir.[29] Bu nedenle yakın gelecekte savaşların kaderini; klasik cephelerin yerine, siber savaşların belirleyeceği ve ülkelerin bilgi sistemlerinin güvenliği ülkelerin ağırlık merkezleri haline geleceği öngörülmektedir. Siber taarruzların ülkelerin güvenliklerine olan etkileri ve toplumlarda yaratmış olduğu korku ortamı ile siber savunma yöntemlerinin oluşturulmasında yaşanan zorluklar, siber savaşın güvenlik yaklaşımlarında meydana getirdiği paradigma dönüşümünden kaynaklanan kaos dönemini temsil etmektedir. ABD'nin siber taarruzları savaş sebebi olarak kabul etmesi ise siber savaşların topyekûn ülkeleri bir savaşa sürüklediğinin ve güvenlik algılamalarında bir paradigma dönüşümüne neden olduğunun kanıtıdır.[30]

Bilgi teknolojilerindeki gelişmeler istihbarat faaliyetlerine büyük kolaylıklar sağlarken, diğer taraftan siber uzayın etkin kullanımı büyük güvenlik açıklarını da beraberinde getirmiştir. Ancak bu açıklar her devlet için aynı sonuçları doğurmamaktadır. Bilgi üretebilen, ürettiği bilgiyi teknolojiye, teknolojiyi güce çevirebilen ülkeler, bu imkânlar sayesinde küresel haber alma ve kontrol yeteneğine sahip olmaktadır. Ayrıca bu teknolojileri ihraç ederek, söz konusu teknolojiye sahip olmayan ülkeleri kendilerine bağımlı kılabilmektedir. Böylece bilgiyi

[29] Cenk Ceylan, *"Siber Savunma İçin Karar Destek Sistemi ve İstihbarat Stratejisi",* http://www.bilgiguvenligi.gov.tr/siber-savunma/siber-savunma-icin-karar-destek-sistemi-ve-istihbarat-stratejisi.html (Erişim Tarihi: 16.01.2013)

[30] Julian E. Barnes, "Cyber Combat: Act of War", ***Wall Street Journal***, 31 May 2011.

üretemeyen ülkelerin ulusal istihbarat sistemleri de dışa bağımlı olmakta ve istihbarata karşı koyma faaliyetleri neredeyse imkânsız hâle gelmektedir. Öyle ki, istihbarat teşkilatları bu konuya ilgi duymakta hiç gecikmemiştir ve bunun sonucunda da siber istihbarat kavramı ortaya çıkmıştır.

4. Siber Ortamda İstihbarat Kavramı

Bilgi çağıyla birlikte geleneksel istihbarat giderek yerini teknik istihbarat, sinyal istihbarat, ölçüm ve iz istihbaratı gibi spesifik istihbarat alanlarına bırakmıştır.[31] İnternet ve bilgi sistemleri sayesinde istihbaratın ihtiyaç duyduğu personel ve malzemenin azalmasıyla birlikte bilginin maliyeti düşerken, aynı zamanda kaynaklardaki artış nedeniyle bilgilerin depolanması ve analiz edilmesi için bilgisayarlar istihbarat faaliyetlerinin vazgeçilmez bir parçası haline gelmiştir. Bilgi çağının getirileri yalnızca açık kaynakların artması ve bilgiye ulaşma maliyetinin azalması olmamış, aynı zamanda internete bağlı bilgisayarlara duyulan yüksek bağımlılığın yarattığı ortam da siber istihbaratı da beraberinde getirmiştir. Bu nedenle istihbarat servisleri, internetten yalnızca açık kaynaklardan yararlanmak için değil; aynı zamanda ağa bağlı bilgisayar sistemlerine gizlice girerek aleni olmayan bilgileri toplamak için de faydalanmaktadır.[32]

İstihbaratın faaliyet alanları; devletin kontrol fonksiyonundan ötürü tehdidin seviyesine göre yakın ve uzak tehlikelerin engellenmesi amacıyla karar vericilere bilgi desteği sağlamak, propaganda, psikolojik harekât gibi örtülü operasyon yöntemleri ile olayları yönetmek ve düşman veya muhtemel düşmanın istihbarat faaliyetlerini engellemek olduğu dikkate alındığında, siber uzayda bu amaçlı yapılan faaliyetler bütünü "siber istihbarat" olarak kavramsallaştırılabilir.

[31] Terry Roberts et. al., "Cyber Intelligence: Setting the Landscape for an Emerging Discipline", ***Intelligence and National Security Alliance***, 2011, Vol.9, 1-20, p. 1-3.
[32] James A. Lewis, *"Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats"*, http://www.csis.org/media/csis/pubs/021101_risks_of_cyberterror.pdf (Erişim Tarihi: 10.03.2013)

5. Siber İstihbarat Yöntemleri

Siber istihbaratın yöntemleri ülkeden ülkeye göre farklılık göstermekle birlikte, aynı zamanda bilgi teknolojilerin her geçen gün ilerlemesiyle beraber yeni yeni yöntemler keşfedilecek ve bu yöntemlere yönelik siber savunma taktikleri geliştirilecektir. Geleneksel istihbarat sistematik bir şekilde disiplinlerine, seviyelerine ve konularına göre sınıflandırılırken; siber istihbaratın faaliyet alanları geleneksel istihbarat ile aynı olmasına rağmen siber uzayın farklılığından ve gereksinimlerinden ötürü siber istihbarat faaliyetlerinin yöntemlerine göre tasniflenmesinin daha uygun ve anlaşılabilir olacağı değerlendirilmektedir. Girgin'e göre; siber istihbaratın iki yüzü vardır. Bunlardan ilki, bilgisayar yoluyla internet üzerinden pek çok bilgiye çok kısa sürede ulaşmak ve uygun görülen bilgileri yaymaktır. İkincisi, bilgisayarların çalışması sırasında bazı teknik oyunlarla hedef bilgisayardan bilgi kapmaktır.[33] Ancak bunlara açık kaynakların propaganda ve psikolojik harekât kapsamında kullanılmasıyla internet üzerinden yapılan haberleşmelerin dinlenmesini eklemek gerekir. Bu kapsamda siber istihbarat yöntemleri; Siber Elektronik İstihbarat, Siber Açık Kaynak İstihbaratı ve Sosyal Ağlara Dayalı Siber İstihbarat olmak üzere üç ana başlık altında incelenebilir.

a. Siber Elektronik İstihbarat

Hükûmetler, bankalar veya şirketler gibi resmî ya da özel kurumlar iç işlemlerini kendi iç ağlarında, kendilerine has yazılımlarla gerçekleştirmekte ve tüm çalışmalarını, hizmetlerini, bilgilerini ve sırlarını bu iç ağ ile birbirlerine ulaştırmaktadır. Beraber iş yaptıkları veya bir şekilde iletişim halinde olmaları gereken dışarıdaki kuruluşlara bilgi göndermeleri veya almaları gerektiğinde ise internete açılan güvenli olduğuna inandıkları kapıları kullanmaktadırlar. Ancak bir kapı varsa, bu kapı her iki tarafa da açılıyor demektir. Bu güvenli kapıları açmak için hazırlanan çok özel yazılım ve donanımlar sayesinde

[33] Kemal Girgin, ***Uluslararası İlişkiler Modern İstihbarat ve Türkiye***, Okumuş Adam, İstanbul, 2003, s. 383.

istihbarat servisleri iç ağlara nüfuz edebilmektedir.[34] İstihbarat servisleri bu yöntem için kendi yetiştirdiği personelini kullanabileceği gibi aynı zamanda daha zahmetsiz bir yol olarak bilgisayar korsanlarını da kendi casusları ve haber toplama elemanları gibi kullanabilmektedirler. Nitekim 1986 ile 1989 yılları arasında Doğu Almanya'daki bilgisayar korsanları ABD, Batı Avrupa ve Japonya'daki birçok askerî, bilimsel ve endüstriyel kurumun bilgisayarlara girerek parola, yazılım ve diğer bilgileri çalmış ve Sovyet gizli servisine satmıştır.[35]

Siber elektronik istihbaratla ilgili genel kaygılardan biri de uzmanların sistem zayıflıklarından daha kolay yararlandıkları bir yöntem olan ve bilgisayar yazılımlarına dışarıdan hiçbir şekilde tespit edilemeyen gizli giriş şifrelerinin yerleştirilmesidir.[36] Bu konuda en büyük sansasyonu, bilgisayar donanım ve yazılım teknolojisinin lideri Microsoft firmasının geliştirdiği ve dünyanın her yerinde resmî ve özel kuruluşlar ile bireylerin çoğunluğunun bilgisayar sistemlerinde kullandığı, Windows işletim sistemi ile ilgili ortaya atılan iddialar yaratmıştır. Kanadalı bir araştırmacı olan Endrew Fernandez, Windows programı içerisinde Amerikan Ulusal Güvenlik Ajansı (National Security Agecy)'nın kısaltması "NSA" harfleri ile kodlanmış bir şifre keşfetmiştir. Bunun üzerine ABD istihbaratının dünyadaki haberleşmeyi izlemesini sağlayacak yazılım programları geliştirmek için Microsoft ile birlikte çalıştıkları iddia edilmiştir.[37] Bu gelişmeler üzerine Rusya, Çin ve Almanya Microsoft programlarının resmî kurumlar tarafından kullanılmaması hususunda ciddi tedbirler almıştır.[38]

[34] Nedret Ersanel, ***Siber İstihbarat***, ASAM, Ankara, 2001, s. 23.
[35] Anthony H. Cordesman and Justin G. Cordesman, "Cyber-Threats, Information Welfare, and Critical Infrastructure Protection: Defending the U.S. Homeland", ***Praeger, Connecticut***, 2001, 1-18, p. 18.
[36] Egmannt R. Koch and Jochen Sperber, ***Bilgi Mafyası***, çev. Kaan Ökten, Sarmal Yay., İstanbul, 1996, s. 23.
[37] Gürol Canbek ve Şeref Sağıroğlu, "Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma", ***Gazi Üniv. Müh. Mim. Fak. Der.***, 2007, Cilt:22, Sayı:1, 121-136, s. 126.
[38] Ersanel, 2001, a.g.e., s. 25-28.

İstihbarat teşkilatlarının bir diğer örtülü bilgi toplama aracı da bilgisayar yazılımlarıdır. Bu amaçla kullanılan yazılımların en önemlisi ve en çok sansasyon yaratanı ise PROMIS (Prosecutor's Management Information System) isimli programdır. 1982 yılında Inslaw şirketi tarafından ABD Adalet Bakanlığı savcıları için geliştirilen program, üreticisinin dahi haberi olmadan hükûmet tarafından çalınarak, birçok ülke istihbarat servisine satılmıştır.[39] 1990 yılında CIA tarafından kullanıldığının açıklanması üzerine Kanada, İtalya, Hollanda ve İsrail gizli servislerinin de programı kullandıkları ortaya çıkmıştır. Bu program, farklı veri tabanlarını kullanarak kişilerin elektronik ortamlarda bıraktıkları izleri toplamakta ve anlamlı bir şekilde birleştirmektedir. Telefon şirketi, elektrik şirketi, banka veya benzeri bir sistemden herhangi birine bu programa sahip bir bilgisayar ile sızılması yeterlidir. Program bir evde su tüketiminin artması veya telefon görüşmelerinin çoğalması durumunda, burada yaşayanların arttığı gibi mantıklı sonuçlar üreterek kullanıcıyı uyarabilmektedir.[40] Ya da bu programın satıldığı ülkelerdeki banka sistemlerinin istenildiği anda kilitleyebilecek ve kontrollü mali krizlere yol açabilecektir.[41] Ancak PROMIS programının çok konuşulan bir program olmasının asıl sebebi, çalındıktan sonra Amerikan istihbarat servisi tarafından bir "arka kapı" yerleştirilerek aralarında Türkiye'nin de bulunduğu[42] 40'tan fazla ülkeye satılmış olmasıdır.[43] Bu arka kapı sayesinde program, satıldığı ülkelerin gizli servislerine, banka ve finans kuruluşlarına ait bilgileri ABD istihbarat servisine göndermektedir.[44]

[39] Jerry Seper, "Software Likely in Hands of Terrorist (Promis/Inslaw)", ***Washington Times***, http://www.freerepublic.com/forum/a3b28933d7f22.htm (Erişim Tarihi: 22.04.2013)
[40] Ersanel, 2001, a.g.e., s. 34-35.
[41] Sait Yılmaz, ***21. Yüzyılda Güvenlik ve İstihbarat***, Alfa Yayınları, İstanbul, 2006, s. 618.
[42] Ersanel, 2001, a.g.e., s. 36.
[43] Ömer Özkaya, ***CIA Belgeleriyle Zihin Kontrol Operasyonları***, IQ Kültür Sanat Yayıncılık, İstanbul, 2003, s. 255.
[44] David Dastych, "Another Watergate? Promisgate: World's Longest Spy Scandal Still Glossed Over", ***Canada Free Press***, http://www.canadafreepress.com/

İstihbarat amaçlı olarak siber uzayda küresel bilgi toplanması için özel sistemler kurulmaktadır ve "Echelon" da bunların başında gelmektedir. "Küresel Denetleme" sistemi de denilen Echelon projesinin temeli UKUSA (United Kingdom, USA) isimli anlaşmaya dayanmakta olup ABD, İngiltere, Kanada, Avustralya ve Yeni Zelanda'nın ortaklığı ile yürütülmektedir.[45] Birçok NATO ülkesi de Echelon'a destek vermekte ve böylece sistemi kendi adına kullanabilmektedir.[46] Echelon sistemi, üye ülkelere ait beş ana stratejik uyduyu kullanmakta ve diğer amaçlı uydulardan da yardım almaktadır.[47] Faaliyete geçirildiği günden bu yana küresel olarak, belgegeçerleri, elektronik postaları (e-posta), telefon haberleşmelerini izleyebilme ve aynı zamanda nakledilen verileri de ele geçirebilme yeteneğine sahip olan sistem,[48] küresel haberleşmeleri dinleyebilmek için iki temel metot kullanmaktadır. Bunlardan ilki, uydu sinyalleri ve mikro dalga sinyallerin yakalanmasıdır. Böylece uydu üzerinden geçen iletişimin yakalanması sağlanır. Diğer bir metot da okyanus aşan kabloların dinlemeye alınmasıdır.[49] Sistem dünya genelindeki yoğun haberleşmeyi, istihbarat servisleri için hazırlanmış olan anahtar kelimeler vasıtasıyla takip etmekte ve sistem bu kelimeleri içeren görüşmeleri yakaladığında ilgili istihbarat servisini ikaz etmektedir.[50]

Son derece gelişmiş olan siber elektronik istihbarat yöntemlerinden bir diğeri de elektromanyetik dinlemelerdir. Bilgisayarın klavyesinden,

2006/dastych013106.htm (Erişim Tarihi: 21.04.2013)

[45] Girgin, a.g.e., s. 324.

[46] Nedret Ersanel, ***Siber İstihbarat Küresel ve Nano Casusluğun Anatomisi***, Hayykitap, İstanbul, 2005, s. 101.

[47] Yılmaz, 2006, a.g.e., s. 628-629.

[48] Enis Coşkun, ***Küresel Gözaltı Elektronik Gizli Dinleme ve Görüntüleme***, Ümit Yayıncılık, Ankara, 2000, s. 97.

[49] "Eavesdropping 101: What Can The NSA Do?", ***American Civil Liberties Union***, http://www.aclu.org/safefree/nsaspying/23989res20060131.html#echelon (Erişim Tarihi: 22.04.2013)

[50] Jeffrey Richelson, "Desperately Seeking Signals", ***Bulletin of the Atomic Scientists***, 2000, Vol.56, No.2, 47-51, p. 49.

ekranından, modem kablosundan ve diğer birçok bileşeninden yayılan elektromanyetik dalgalar; klavyede basılan tuşlar, ekrandaki görüntü ve modemle bilgisayar arasında geçen bilgileri de taşırlar. Yeterli donanıma sahip herhangi biri bu elektromanyetik dalgaları bir veya iki kilometreye varabilen bir mesafeden kaydedebilir ve ekrandaki görüntüyü, klavyede basılan tuşları veya modemden geçen bilgileri elektromanyetik ışınımı işleyerek tekrar oluşturabilir. Bu yönteme karşı Elektromanyetik Salınım Standardı "Transient ElectroMagnetic Pulse Standard-TEMPEST" adı verilen, elektronik aygıtların elektromanyetik ışınım düzeylerinin azami sınırlarını ve zırhlama metotlarını belirleyen bir standart oluşturulmuştur. TEMPEST güvenliği, haberleşme sistemlerinden, bilgi işlem donanımından, elektronik cihazlardan salınan elektromanyetik dalgalardan yetkisiz kişilerin bilgi çıkarmalarını engelleyici güvenlik önlemleri olarak ifade edilebilir.[51]

Siber elektronik istihbaratın bir diğer aracı da internetten sürekli istifade eden hemen herkesin kullandığı e-posta servisidir. E-posta yoluyla dolaşan ve bulaşan virüsler, spamlar ve üçüncü şahıslara mesajı ileten snifferlar gibi zararlı yazılımlar gönderilebilmektedir.[52] Birçok kurum ve firma, e-posta güvenliğini yetkisiz kullanıcıların müdahalesini engelleyen, "firewall" adı verilen koruma tedbirleri ile sağlamaktadır. Ancak iyi bir koruma sağlayan "firewall" sistemi e-postaların içeriğini kontrol etmediğinden, e-postalar sayesinde sisteme zararlı yazılımları yerleştirmek mümkün olabilmektedir. Gönderinin ya da alanın haberi olmadan e-postanın bir kopyası istihbarat servisleri tarafından ele geçirilebilmekte ve iletişim izlenebilmektedir.[53]

b. Siber Açık Kaynak İstihbaratı

İnternetin yaygınlaşması, uydu yayınlarının artması ve özel

[51] "Elektromanyetik Dinleme ve Güvenlik (EDG)", ***Olympos Security***, http://www.olympos.org/article/articleview/278/1/10/elektromanyetik_dinleme_ve_guvenlik_edg (Erişim Tarihi: 22.04.2013)

[52] Mustafa Ünver vd., ***Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler***, Bilgi Teknolojileri ve İletişim Kurumu, Ankara, 2009, s. 9.

[53] Ersanel, 2001, a.g.e., s. 29-30.

kanalların çoğalması bilgi ihtiyacımızı karşılayan muazzam kaynaklar sunmaktadır. Medyadaki bu hızlı gelişim, istihbarat servislerinin değerlendirmelerinde medyayı haber kaynağı olarak kullanmalarına da neden olmaktadır. Güvenlik algılamalarında düşman ve muhtemel düşmanın sahip olduğu harp silah ve araçlarının sayısı, menzili ve teknik özelliklerinin önemli olduğu dönemlerde, istihbarat ihtiyaçları ağırlıklı olarak ajanlar ve casuslar gibi unsurların yoğun çabaları ile karşılanmaya çalışırken, günümüzde istihbarat servisleri açık kaynak istihbaratına çok daha fazla ağırlık vermektedir. Dünyadaki gelişmelerle ilgili bilgilerin çok önemli bir çoğunluğu zahmetsiz ve kısa bir zamanda açık kaynaklardan elde edilebilmektedir.[54]

Medyanın istihbarat örgütleri için önemli bilgiler sunmasının yanında; istihbarat örgütlerinin belli çıkarlar için medyayı kullanması da son zamanlarda sık rastlanan bir yöntem olarak göze çarpmaktadır. Medya toplum üzerinde değişik algılama tarzları oluşturma gücüne sahiptir.[55] İstihbarat servisleri ise medyanın ürünlerini yönlendirmek suretiyle medyanın oluşturduğu algılamayı örtülü olarak yönetmektedir. Böylece ustalıkla hazırlanmış psikolojik harekât ve propaganda faaliyetlerini yeni medya unsurları ile kolayca halka enjekte edilebilmektedir.[56] Fakat siber uzayın sınırsız yapısı düşünüldüğünde yeni medya unsurlarını sansürlemek hemen hemen imkânsız bir hâle gelmiştir. Herhangi bir muhabirin dizüstü bilgisayarı ve cep telefonu ile internete bağlanması ve çektiği görüntüleri istediği yere anında göndermesi mümkün hâle gelmiştir. Ayrıca açık toplumlarda basın özgürlüğü ve haber alma özgürlüğü gibi temel haklara verilen önem sayesinde, basının açıkça sansür edilmesi de hukuksal açıdan

[54] Joseph M. Mazzafro, ***Cyber Intelligence: Setting The Landscape For An Emerging Discipline***, Intelligence and National Security Alliance (INSA), Arlington, 2011, p. 15.
[55] Matthew M. Harley, "For and From Cyberspace Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance", ***Air & Space Power Journal,*** 2012, 12-33, p. 13.
[56] Mehmet Nesip Öğün ve Adem Kaya, "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", ***Güvenlik Stratejileri Dergisi***, 2013, Cilt:9, Sayı:18, 145-181, s. 161.

engellenmektedir. Bu nedenle yeni medya unsurlarının, siber istihbaratın propaganda, psikolojik harekât gibi örtülü operasyon yöntemleri ile olayları yönetme faaliyet alanı kapsamında kullanımında, "özgürlük ile güvenlik" arasındaki dengenin gözetilmesi gerekmektedir.

11 Eylül saldırılarında, uçakların İkiz Kulelere çarpma görüntüleri eş zamanlı olarak dünya kamuoyunca da izlenmiştir. Bu saldırılar medyanın yardımıyla Irak'ın işgali için uygun ortam oluşturulmasında kullanılmıştır. Gerek ABD'de gerekse İngiltere'de işgali haklı kılabilmek için, istihbarat servislerinin elde ettiği bilgiler medya aracılığı ile kamuoyuna sunulmuş, istihbarat tarihinde daha önce sistematik olarak kullanımı olmayan "istihbarat bilgilerinin kamuya açık kullanımı" gündeme girmiştir.[57] Ancak bu uygulama 2003 yazında İngiltere'de Tony Blair hükûmetini ve İngiliz Müşterek İstihbarat Komitesini (JIC-Joint Intelligence Committee) ciddi politik tartışmaların odağı hâline getirmiştir. Irak'taki kitle imha silahları ile ilgili hazırlanan ve medya aracılığıyla kamuya açık şekilde sunulan istihbarat raporunun doğruları yansıtmadığı, hükûmetin Saddam Hüseyin rejimine karşı olan tutumuna destek sağlamak amacıyla politikleştirildiği ve amacın Irak'a karşı girişilecek bir harekât için kamuoyu desteği oluşturmak olduğu anlaşılmıştır.[58] İstihbarat böylece politika yapıcılara rehberlik yapmak dışında, açık bir şekilde hükûmet politikasına kamu desteğini sağlamak için kullanılmıştır.

c. Sosyal Ağlara Dayalı Siber İstihbarat (Sosyal Mühendislik)

Neredeyse tüm cihazların internete bağlandığı günümüzde, insanların bilgiye daha kolay erişmesiyle bilgi toplama işlemi, klasik medya unsurlarının takip edilmesi suretiyle gerçekleştirilen haber toplama faaliyetine yeni bir boyut katmış ve internette yapılan "sanal sörf" dahi istihbarat faaliyetinin konusu haline gelmiştir.[59] Her bilgiyi, kişiyi, kurumu, internete çekme stratejisi, istihbarat unsurlarına

[57] Barbara Starr, "Pentagon Sites: Journalism or Propaganda", ***CNN News***, 05 February 2005.
[58] Scott and Jackson, a.g.m., p. 150-151.
[59] Ersanel, 2001, a.g.e., s. 21-22.

muazzam bir gözetim imkânı sağlamaktadır. Bu nedenle bilginin toplanması, stratejik olarak tasnifi, sosyal mühendislik olarak kullanılması için özel amaçlı olarak oluşturulmuş ücretsiz internet blogları ve arkadaşlık siteleri, istihbaratta öne geçmek isteyen devletler tarafından örtülü olarak finanse edilmektedir.

Sosyal mühendislik; bilgi güvenliği sistemlerindeki en zayıf halkanın insan olduğu varsayımına dayanır. Sosyal mühendislik alanında, analizci, insanların eğilimlerinden ve kişisel ilişkilerden faydalanarak gizli bilgilere erişmeye çalışmaktadır.[60] Bu yöntemde analizci insanların siber ortamda paylaştığı herkesin ulaşabileceği kişisel verileri, tek başlarına bir gizlilik içermemesine rağmen, farklı kaynaklardan temin ederek sistematik olarak birleştirilmekte ve gizlilik içeren veya önem arz eden bilgi haline dönüştürmektedir. Sosyal mühendisliğin ilgi alanı herkesin kullanabileceği iki yönlü iletişim sunan sosyal paylaşım siteleridir. Sosyal paylaşım sitelerinin en bilinenlerinden bir tanesi olan Facebook'un başka insanları tanımak, kendi görüşlerini anlatmak ve başkalarının nasıl düşündüğünü anlamak üzere üç temel işlevi bulunmaktadır.[61] Facebook sosyal paylaşım sitesinin dünya genelinde bir milyara yakın internet kullanıcısı bulunmaktadır.[62] Bu durum söz konusu sosyal paylaşım sitelerinin dünya çağında ne kadar yayın olarak kullanıldığının ve etkili olduğunun bir göstergesidir.

Facebook sosyal paylaşım sitesinin örtülü kullanım alanlarından biri de siyasi amaçlı olarak sosyal hareketleri eyleme geçirme özelliğidir.[63] 2011 yılının ilk aylarında Orta Doğu ve Kuzey Afrika'da

---

[60] Ülkü Arslan Aydın ve Cüneyt Acartürk, *"Kullanılabilir Güvenlik ve Grafik Parolalar",* http://inet-tr.org.tr/inetconf16/bildiri/28.pdf (Erişim Tarihi: 27.04.2013)

[61] Lee Hudson Teslik*, "New Media Tools and Public Diplomacy, Interviewee: Elliot Schrage, VP of Global Communications, Marketing, and Public Policy, Facebook, Interviewer",* http://www.cfr.org/public-diplomacy/new-media-tools-public-diplomacy/p19300 (Erişim Tarihi: 27.04.2013)

[62] "Facebook Statistics", ***Socialbakers***, http://www.socialbakers.com/countries/continents (Erişim Tarihi: 27.04.2013)

[63] Sait Yılmaz, *"Batı İstihbaratı ve Sosyal Medya"*, **USAM**, http://usam.aydin.edu.tr/analiz/guvenlik_isthbrt.pdf (Erişim Tarihi: 10.12.2012)

başlayan ve Arap Baharı olarak adlandırılan halk hareketlerinin örgütlenme ve iletişim aracı olarak sosyal medyayı kullanmaları neticesinde, yaşanan halk hareketlerine "sosyal medya devrimi" gibi tanımlamalar yapılmıştır.[64] Arap Baharı'ndaki halk hareketlerindeki sosyal medyanın etkisi, Arap coğrafyasında çıkarları olan devlet ve örgütler tarafından organize edilmiş olabileceği unutulmamalıdır. Böylece sosyal ağlara dayalı siber istihbarat ile sosyal medya, sosyal mühendislik kapsamında kullanımının yanı sıra, psikolojik harekât veya propaganda gibi örtülü operasyonlar amacıyla da kullanılabilmektedir.

6. Sonuç

Günümüzde, bilgi, belirleyici bir güç hâline gelmiştir. İstihbaratın amacı ise bilgiyi yani gücü elde etmektir. Bir disiplin haline getirilmesinden bu yana yaklaşık yarım yüzyıl geçmiş olan istihbarat kavramı, yapıları ve faaliyet alanları, tehdit algılamalarındaki değişime paralel olarak sürekli değişmiştir. İstihbarat ilk günden itibaren haber toplayabilmek için içinde bulunduğu dönemin en üst teknolojisini kullanmaktadır. Bu nedenle istihbarat, bilgi teknolojilerinin sunduğu imkânlardan sonuna kadar yararlanmaya ihtiyaç duymakta ve siber uzayı etkili bir şekilde kullanmaya başladığı görülmektedir. Siber uzay sayesinde, istihbarat bir taraftan yeni yetenekler kazanırken, bir taraftan da yeni mücadele alanları ile karşı karşıya kalmaktadır.

Siber uzayda yaşanan gelişmeler harekât ortamına farklı bir mekân boyutu eklemiş ve harplerin icra edildiği kara, deniz ve hava gibi fiziksel mekânlardan farklı olarak bütün bu boyutlarda icra edilen harekâtları doğrudan etkileyen yeni bir boyut kazandırmıştır. Harbin bu boyutunda kazanılan başarıların kuvvet çarpanı etkisi oluşturduğu ve daha harp başlamadan veyahut kriz döneminde stratejik seviyede uygulanan siber saldırılar sayesinde düşmanın harp etme azim ve kararının kırabileceği görülmektedir. Hatta siber uzay barış döneminden

[64] Mehmet E. Babacan vd., "Sosyal Medya ve Arap Baharı", ***Sakarya Üniversitesi Sosyal Bilgiler Enstitüsü Akademik İncelemeler Dergisi,*** 2011, Cilt:6, Sayı:2, 63-91, s. 63-65.

itibaren düşmanın imkân ve kabiliyetlerini geliştirecek yeteneklerine yapılacak saldırılar ile tehdidin daha oluşmadan yok edilmesine imkân sağlayabilmektedir.

Önümüzdeki dönemde savaşların kaderini klasik cephelerin yerine, asimetrik bir etki oluşturan ve harbin beşinci boyutu olarak kabul edilen siber uzayda yaşanan savaşlar belirleyecektir. Siber kabiliyetler sayesinde, bilgi teknolojilerine daha fazla bağımlı hale gelen devletlerin kritik altyapıları, ağırlık merkezleri haline gelecektir. Devletlerin, askerî üsleri, okyanuslardaki donanmaları veya yüksek teknolojiye sahip havacılık imkânları ile uzaydaki uydu yetenekleri kadar siber taarruz kabiliyetlerini de geliştirmeleri gerekecektir. Son 10 yıl içerisinde dünyanın çeşitli yerlerinde gerçekleştirilen siber taarruz olayları, devletlerin bu alanda kendi yeteneklerini geliştirmelerinin ve teşkilatlanmalarının zorunluluğunu ortaya koymuştur. Bu kapsamda siber tehditlerin her geçen gün geliştirilmesi ve siber taarruz yöntemlerinin tam olarak belirlenememesi, siber savunma alanında alınacak tedbirleri zorlaştırmaktadır. Tüm bu gelişmeler geleceğin harp ortamında siber savaşların önemini göstermekte ve siber savaşların başta modern devletler olmak üzere bilgi teknolojilerine bağımlılıkları yüksek olan devletlerin ulusal güvenliği için gerçek bir tehdit oluşturduğunu ortaya koymaktadır.

Ulusal güvenliği tehdit eden siber savaşlarda inisiyatifi kazanmak ve siber uzayda bulunan tehditlere yönelik doğru değerlendirmeler yapabilmek açısından gereksinim duyulan siber istihbarat kavramı ve siber istihbaratın faaliyet alanları bu çalışmada ortaya konulmuştur. Bu kavram ortaya konulurken istihbaratın temel faaliyet alanları üzerinden bir çıkarımda bulunulmuştur. İstihbaratın faaliyet alanları devletin kontrol fonksiyonundan ötürü tehdidin seviyesine göre yakın ve uzak tehlikelerin engellenmesi amacıyla karar vericilere bilgi desteği sağlamak, propaganda, psikolojik harekât gibi örtülü operasyon yöntemleri ile olayları yönetmek ve düşman veya muhtemel düşmanın istihbarat faaliyetlerini engellemek olduğu dikkate alındığında, siber istihbarat siber uzayda bu amaçla yapılan faaliyetler bütünü olarak tanımlanmıştır. Böylece siber istihbarat, hem muhtemel risk ve fırsatları önceden değerlendirerek, karar vericilerin elini

kuvvetlendirmekte hem de ulusal çıkarlar doğrultusunda, çeşitli yöntemler kullanarak siber uzayın etkin kullanımını sağlamaktadır.

Siber istihbaratın yöntemleri bir taraftan kazanılan yetenekler doğrultusunda ülkeden ülkeye göre farklılıklar gösterirken, bir taraftan da bilgi teknolojilerin her geçen gün ilerlemesi sayesinde yeni yeni yöntemler keşfedilmektedir. Bununla beraber bu yöntemlere yönelik yeni siber savunma taktikleri de geliştirilmektedir. Bu çalışmada, istihbaratın ana fonksiyonları siber uzayla ilişkilendirilerek, siber istihbaratın temel yöntemleri üzerine bir çıkarımda bulunulmuştur. Siber istihbarat yöntemleri sistematik olarak siber uzayda bulunan aleni olmayan elektronik bilgilerin toplanmasını, değiştirilmesini ve engellenmesini içeren Siber Elektronik İstihbarat, medyanın sunduğu bilgi akışından açık kaynak olarak yararlanan ve medyanın toplumları yönlendirebilme yeteneğinden faydalanan Siber Açık Kaynak İstihbaratı ve sosyal mühendislik faaliyetlerini kapsayan Sosyal Ağlara Dayalı Siber İstihbarat olmak üzere üç ana başlık altında kategorize edilmiştir.

Ulusal güvenliğine yönelik siber tehditlerle mücadele ederken, taktik seviyeden stratejik seviyeye kadarki karar alıcılar açısından siber istihbarat anahtar niteliği taşımaktadır. Siber istihbarat öncelikle devletlerin maruz kalabilecekleri siber tehditlere karşı durumsal farkındalıklarını arttıracaktır. Etkili bir siber istihbarat ile siber tehditlerin oluşturacağı riskler azalacak, siber saldırıların etkilerini azaltacak yetenekler geliştirilebilecek ve inşa edilecek siber güvenlik yapılanmasında doğru ve zamanında bilgilendirilmiş istihbarat ile verimli ve maliyet etkin kararlar alınabilecektir. Siber savaşların kaçınılmaz olduğu önümüzdeki dönemde, karar vericiler tarafından siber istihbarata gerekli önem gösterilmeli; devletlerin istihbarat servisleri, siber istihbaratın yöntemlerini etkin olarak hayata geçirilebilmek için ihtiyaç duyulan teşkilatlanmayı yapmalı ve gelecekte yaşanacak siber savaşlarda, siber istihbarat aktif rol oynamalıdır.

Summary

Today, information becomes a determining power. The objective of intelligence is to get the information, or in other words, the power.

Intelligence concept, which has become a discipline for half a century, finds itself in a continuous evolution along with its structure and operational area in parallel to threat perceptions. Intelligence always benefits from latest modern technology to collect information. Thus, it needs to utilize completely from the opportunities and potentials of information technology. Moreover, it is observed that it begins to manage the cyber space effectively.

Developments happened in cyber space added another space dimension to the operations environment, which is not only distinct from physical locations such as land, air and sea where wars are executed, but also has a direct impact to all of them as a new dimension. It is also noted that enemy loses its ambition and determination to combat because of the success in this dimension through creating a force multiplier due to the cyber attacks done in crisis period at strategic level or prior to start of the war. Furthermore, it provides opportunity to clear the threat before it is formed, thanks to the attacks initiated from cyber space during peace period to the portions where enemy is able to develop its ability and facilities.

In near future, destiny of the wars will be determined through cyber attacks, rather than classical front line operations. In addition, information system security of governments is the center of gravity. Nations should develop and focus on cyber attack abilities as well, in addition to the concentration given the satellites, modern high tech air force, navy and military bases. Cyber attacks done from various different points during the last decade revealed that nations are obliged to develop their talents in this field and organized systematically. In this respect, it also makes taking precautions so difficult to have the necessary defense against the cyber attacks because of being unable to define attack methods exactly and having continuous development in cyber threats. All these developments increase the importance of cyber war. Requirement for a cyber intelligence concept is at the core of discussions against this threat in terms of cyber space threat analysis.

Intelligence activities are supporting governments through providing information to decision makers in order to prevent close and remote threats depending on the threat level due to government

monitoring function; managing the events through covered operation methods such as propaganda and psychological operation; and to impede existing and potential enemies' intelligence activities. Hence, cyber intelligence is defined as the all activities done in cyber space for the above-mentioned purposes. The methods used in cyber intelligence differ among the countries. Moreover, cyber defense tactics are developed thanks to the new discoveries based on advances in technology. In this respect, cyber intelligence methods are classified systematically in three main titles: cyber electronic intelligence, cyber open source intelligence and cyber intelligence based on social networks. It is obvious that cyber wars are inevitable in the near future. Hence, decision makers show sufficient attention to cyber intelligence. Additionally, intelligence agencies should establish the required organization to initiate the effective methods of cyber intelligence. Finally, the last but not the least one is the requirement of active role of intelligence services in cyber intelligence in future cyber wars.

KAYNAKLAR

Kitaplar

ARI, Tayyar. ***Uluslararası İlişkiler Teorileri; Çatışma, Hegemonya, İşbirliği***, Alfa Yayınları, İstanbul, 2004.

ARIBOĞAN, Deniz Ülke. ***Kabileden Küreselleşmeye Uluslararası İlişkiler Düşüncesi***, Sarmal Yayınevi, İstanbul, 1998.

BAL, İhsan. ***Alaca Karanlıkta Terör ile Mücadele ve Komplo Teorileri***, USAK Yayınları, Ankara, 2006.

COŞKUN, Enis. ***Küresel Gözaltı Elektronik Gizli Dinleme ve Görüntüleme***, Ümit Yayıncılık, Ankara, 2000.

ERSANEL, Nedret. ***Siber İstihbarat***, ASAM, Ankara, 2001.

ERSANEL, Nedret. ***Siber İstihbarat Küresel ve Nano Casusluğun Anatomisi***, Hayykitap, İstanbul, 2005.

GİRGİN, Kemal. ***Uluslararası İlişkiler Modern İstihbarat ve Türkiye***, Okumuş Adam, İstanbul, 2003.

KOCH, Egmannt R. and Jochen SPERBER. ***Bilgi Mafyası***, Çev. Kaan Ökten, Sarmal Yay., İstanbul, 1996.
KUHN, Markus G. ***Compromising Emanations: Eavesdropping Risks of Computer Display***, Cambridge University Press, Cambridge, 2003.
MAZZAFRO, Joseph M. ***Cyber Intelligence: Setting The Landscape For An Emerging Discipline***, Intelligence and National Security Alliance (INSA), Arlington, 2011.
METZ, Steven and John Robert Martin. ***Decisionmaking in Operation Iraqi Freedom: The Strategic Shift of 2007***, Strategic Studies Institute, Pennsylvania, 2010.
ÖZKAYA, Ömer. **CIA Belgeleriyle Zihin Kontrol Operasyonları**, IQ Kültür Sanat Yayıncılık, İstanbul, 2003.
SARI, Gökhan. After Globalization Process New Horizons in Contemporary Strategic Intelligence, Yeditepe University Graduate Institute of Social Sciences, İstanbul, 2003 (Yayınlanmamış Yüksek Lisans Tezi).
SUN-TZU. ***Savaş Sanatı***, Çev. Adil Demir, Kastaş Yayınları, İstanbul, 2001.
TEZSEVER, Serhat. ***Millî Güvenliğimiz İçerisinde İstihbarat-Türkiye Cumhuriyeti ve İstihbarat Olgusu***, İ.U.Basımevi, İstanbul, 1999.
TODD, Paul and Jonathan Bloch. ***Küresel İstihbarat***, çev. Enver Günsel, Truva Yayınları, İstanbul, 2006.
TOFFLER, Alvin. ***Üçüncü Dalga***, Çev. Selim Yeniçeri, Koridor Yayıncılık, İstanbul, 2012.
Türkçe Sözlük-Türk Dil Kurumu, Cilt:1, Türk Tarih Kurumu Basım Evi, Ankara, 1998.
ÜNVER, Mustafa vd., ***Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler***, Bilgi Teknolojileri ve İletişim Kurumu, Ankara, 2009.
YILMAZ, Sait. ***21. Yüzyılda Güvenlik ve İstihbarat***, Alfa Yayınları, İstanbul, 2006.

Makaleler

BABACAN, Mehmet E. vd., "Sosyal Medya ve Arap Baharı", ***Sakarya Üniversitesi Sosyal Bilgiler Enstitüsü Akademik İncelemeler Dergisi***, 2011, Cilt:6, Sayı:2, 63-91.

BARNES, Julian E. "Cyber Combat: Act of War", ***Wall Street Journal***, 31 May 2011.
BURKE, Anthony. "Just war or ethical peace? Moral discourses of strategic violence after 9/11", ***International Affairs***, 2004, Vol. 80, No.2, 329-353.
CANBEK, Gürol ve Şeref SAĞIROĞLU. "Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma", ***Gazi Üniv. Müh. Mim. Fak. Der.***, 2007, Cilt:22, Sayı:1, 121-136.
CANLI, Hakan ve Ahmet Kandakoğlu. "Hava Gücü Mukayesesi İçin Bulanık AHP Modeli", ***Havacılık ve Uzay Teknolojileri Dergisi,*** 2007, Cilt:3, Sayı:1, 71-82.
CAŞIN, Mesut Hakkı. "Soğuk Savaş Sonrası Askerî Stratejik İstihbaratın Yeni Vizyonu", ***Avrasya Dosyası***, 2002, Cilt: 8, Sayı: 2, 254-294.
CORDESMAN, Anthony H. and Justin G. CORDESMAN. "Cyber-Threats, Information Welfare, and Critical Infrastructure Protection: Defending the U.S. Homeland", ***Praeger,*** Connecticut, 2001, 1-18.
ÇOMAK, Hasret. "Avrupa'da Güvenlik Yapılanmasının Yeni Parametreleri ve Türkiye'nin Konumu", ***Avrupa Araştırmaları Dergisi,*** 2006, Cilt:15, Sayı:1, 97-120.
DASTYCH, David. "Another Watergate? Promisgate: World's Longest Spy Scandal Still Glossed Over", ***Canada Free Press***, http://www.canada freepress.com/2006/dastych013106.htm (Erişim Tarihi: 21.04.2013)
DEPTULA David D. and R.Greg Brown. "A House Divided: The Indivisibility of Intelligence, Surveillance, and Reconnaissance", ***Air & Space Power Journal***, 2008, Vol.22, No.2, 5-15.
HARLEY, Matthew M. "For and From Cyberspace Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance", ***Air & Space Power Journal,*** 2012, 12-33.
JOHNSON, Loch K. "Bricks and Mortar for a Theory of Intelligence", **Compative Strategy**, 2003, Vol.22, 1-28.
KAHN, David. "İstihbaratın Tarihsel Teorisi", **Avrasya Dosyası**, 2002, Cilt:8, Sayı:2, 5-20.

ÖĞÜN, Mehmet Nesip ve Adem Kaya. "Siber Güvenliğin Millî Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", ***Güvenlik Stratejileri Dergisi***, 2013, Cilt:9, Sayı:18, 145-181.
ÖZTEKE, Cengiz. "Cyber-A New War Domain", ***Defence Turkey,*** 2013, Vol.8, No.48, 8-9.
RICHELSON, Jeffrey. "Desperately Seeking Signals", ***Bulletin of the Atomic Scientists***, 2000, Vol.56, No.2, 47-51.
ROBERTS, T. et. al. "Cyber Intelligence: Setting the Landscape for an Emerging Discipline", ***Intelligence and National Security Alliance***, 2011, Vol.9, 1-20.
SANDIKLI, Atilla ve Bilgehan Emeklier. "Güvenlik Yaklaşımlarında Değişim ve Dönüşüm", Atilla Sandıklı (ed.), ***Teoriler Işığında Güvenlik, Savaş, Barış ve Çatışma Çözümleri***, Bilgesam Yayınları, 2012, 3-70.
SCOTT, Len and Peter JACKSON. "The Study of Intelligence in Theory and Practice", ***Intelligence and National Security***, 2004, Vol.19, No. 2, 139-169.
SEPER, Jerry. "Software Likely in Hands of Terrorist (Promis/Inslaw)", ***Washington Times***, http://www.freerepublic.com/forum/a3b28933d7f22.htm (Erişim Tarihi: 22.04.2013)
STARR, Barbara. "Pentagon Sites: Journalism or Propaganda", ***CNN News***, 05 February 2005.
YILMAZ, Sait. "Batı İstihbaratı ve Sosyal Medya", ***USAM,*** http://usam.aydin.edu.tr/analiz/guvenlik_isthbrt.pdf (Erişim Tarihi: 10.12. 2012)

İnternet Kaynakları

AYDIN, Ülkü Arslan ve Cüneyt ACARTÜRK. "Kullanılabilir Güvenlik ve Grafik Parolalar", http://inet-tr.org.tr/inetconf16/bildiri/28.pdf (Erişim Tarihi: 27.04.2013)
CEYLAN, Cenk. "Siber Savunma İçin Karar Destek Sistemi ve İstihbarat Stratejisi", http://www.bilgiguvenligi.gov.tr/siber-savunma/siber-savunma-icin-karar-destek-sistemi-ve-istihbarat-stratejisi.html (Erişim Tarihi: 16.01.2013)

"Eavesdropping 101: What Can The NSA Do?", ***American Civil Liberties Union***, http://www.aclu.org/safefree/nsaspying/23989res 20060131.html#echelon (Erişim Tarihi: 22.04.2013)
"Elektromanyetik Dinleme ve Güvenlik (EDG)", ***Olympos Security***, http://www.olympos.org/article/articleview/278/1/10/elektromanyetik_ dinleme_ve_ guvenlik_edg (Erişim Tarihi: 22.04.2013)
"Facebook Statistics", ***Socialbakers,*** http://www.socialbakers.com/ countries/continents (Erişim Tarihi: 27.04.2013)
FELTUS, Pamela. *"Aerial Reconnaissance in World War I"* http://www.centennialofflight.gov/essay/Air_Power/WWI-reconnaissance/AP2.htm (Erişim Tarihi: 01.02.2013).
LEWIS, James A. "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", http://www.csis. org/media/ csis/pubs/021101_risks_of_cyberterror.pdf (Erişim Tarihi: 10.03.2013)
National Security Agency (NSA) Resmî İnternet Sitesi, *"World War I Radio Intercept Site Exhibit"*, http://www.nsa.gov/museum/ museu00012.cfm.
TESLIK, Lee Hudson. "New Media Tools and Public Diplomacy, Interviewee: Elliot Schrage, VP of Global Communications, Marketing, and Public Policy, Facebook, Interviewer", http://www.cfr.org/ public-diplomacy/new-media-tools-public-diplomacy/p19300 (Erişim Tarihi: 27.04.2013)

Raporlar

The National Security Strategy of The United States of America, The White House, Washington, 2002.