BİLGİ SAVAŞI: SİPERLERDEN KLAVYELERE TAŞINAN HAREKÂTIN ANATOMİSİ

Mustafa SAĞSAN*

The article focuses on the "information warfare" concept from a theoretical point of view. Within the framework of information science, the essay argues that information is formed after going through the stages of firstly "data", then "information", and lastly "knowledge". It evaluates the information warfare in a different way, by placing it in a theoretical framework, which is based on national information infrastructure of countries that includes information resources, information systems, and information services. After defining the "strategic information warfare" concept, the essay looks at the sorts of information warfare and the threats that they create. It then concludes by examining the measures, which should be taken by the countries against any kind of information attack.

Giriş

1970'lerin sonu ve 1980'lerin başından itibaren bilgi-merkezli hareketler, sanayileşmenin de önüne geçerek sanayi toplumlarını iletişim toplumu hâline getirmeye başladı. Bu değişiklikler ise, zorunlu olarak birçok sektörde bulunan doktrinlerin de (özellikle askerî doktrininin) değişmesini zorunlu kıldı. Özellikle, 21. yüzyılda değişen ve gelişen bu tür teknolojiler, bilginin kullanıldığı alanların da artmasına neden olmuştur. Bilgi, artık her sektörde etkin bir şekilde kullanılmaya başlanmıştır. Bu sektörlerin birkaçını ekonomi, teknoloji, iletişim ve askerî stratejiler şeklinde sıralayabiliriz. Özellikle askerî stratejilerde gerek savunma gerekse saldırı amaçlı kullanılan bilgi ve istihbarat tabanlı teknolojilerin artması ve gelişmesi, "bilgi savaşı" kavramının doğmasına neden olmuştur. 1991 yılında ilk defa Körfez Savaşı esnasında kullanılan bu terim, günümüzde genelde bilgi teknolojisi ağırlıklı olmasından ötürü bilgi bilimcileri ve içeriğinde bir savaş teknolojisinin kullanılması sebebiyle de askerî stratejistleri ve uluslar

* ASAM, Dokümantasyon ve Enformasyon Merkezi, Bilgi Yöneticisi.
E-posta: msagsan@avsam.org

Avrasya Dosyası, İstihbarat Özel, Yaz 2002, Cilt: 8, Sayı: 2, ss. 213-232.

arası ilişkiler uzmanlarını ilgilendirmektedir. Nitekim Richard E. Hayes ve Gary Wheatley: "Information Warfare and Deterrence" adlı makalelerinde 'bilgi savaşı' teriminin birçok anlamda kullanıldığını ve genellikle askerî bilimlerden ziyade siber savaş alanı içerisindeki bilgisayar ve iletişim alt yapısı disiplini üzerinde odaklandığını ifade etmektedirler."[1]

Okuyacağınız bu makalede, enformasyon yöneticisi gözüyle "bilgi savaşı" kavramı değerlendirilmeye çalışılacak ve konu ile ilgili teorik boyutta açıklamalarda bulunulacaktır. Çünkü, bilgi savaşının askerî bir boyutu olduğu halde, genelde teknoloji hizmetlerinin enformasyonla birleşmesi ve daha çok karşı tarafın bilgi sistemlerini, bilgi kaynaklarını ve bilgi alt yapısını çökertmeye yönelik bir internet savaşını anlatması, bilgi savaşı teriminin, enformasyon bilimi içerisinde yer almasını sağlamıştır. Bu terimin, bilgi bilimi içerisindeki yerinin ne olduğunu ve hangi pozisyonda yer aldığını anlayabilmek için bilgi teknolojilerinin bilgi çatışması boyutunu bilmek gerekmektedir.

Enformasyon Bilimi İçerisinde 'Savaş' Kavramının Rolü

Bilgi, çok kısa olarak "bir mesajın anlamı veya içeriği"[2] şeklinde tanımlanabilir. Bir başka ifadeyle, bilgi, kağıt veya başka ortamlar üzerine kaydedilmiş, anlaşılabilen ve iletilebilen veriler topluluğudur.[3] Genelde birçok alanda kullanılmasına rağmen, enformasyon bilimciler bilgiyi, "üzerinde kesin bir yargıya varılmış, anlam kazanmış her türlü ses, görüntü ve yazılara verilen isim"[4] olarak tanımlamaktadırlar. Bilgide önemli olan nokta, herhangi bir olgunun anlaşılır ve açıklanabilir olmasıdır. Bu tür görüntü veya yazılar ise, bilgi sistemlerinden oluşmaktadır. Bilgi sistemleri ise, "bilgiyi yaymak, iletmek, göstermek ve yedeklemek için gerekli makine ve ekipmanı kullanarak oluşturulmuş alt yapı, organizasyon ve işlemci"[5] olarak ifade edilebilir. Bilgi bilimini, epistemoloji, mantık, bilgi teorisi, karar teorisi, semiyotik (göstergebilim) teorisi ve bilgi yönetimi disiplinleri içerisinde açıklamak gerekir.[6]

---

1 Richard E. Hayes ve Gary Wheatley "Information Warfare and Deterrence", N*ational Defence University*, Sayı: 87, (Ekim, 1996), s. 2.

2 Chris Mader, *Information System: Technology, Economics, Applications*, (Chicago: Science Research Associates Inc., 1974), s. 3.

3 "Information", *Harrod's Librarians Glossary of Terms Used in Librarianship*, (Gower: Documentation and Bookcrafts, Aldershoot, 1987), s. 14.

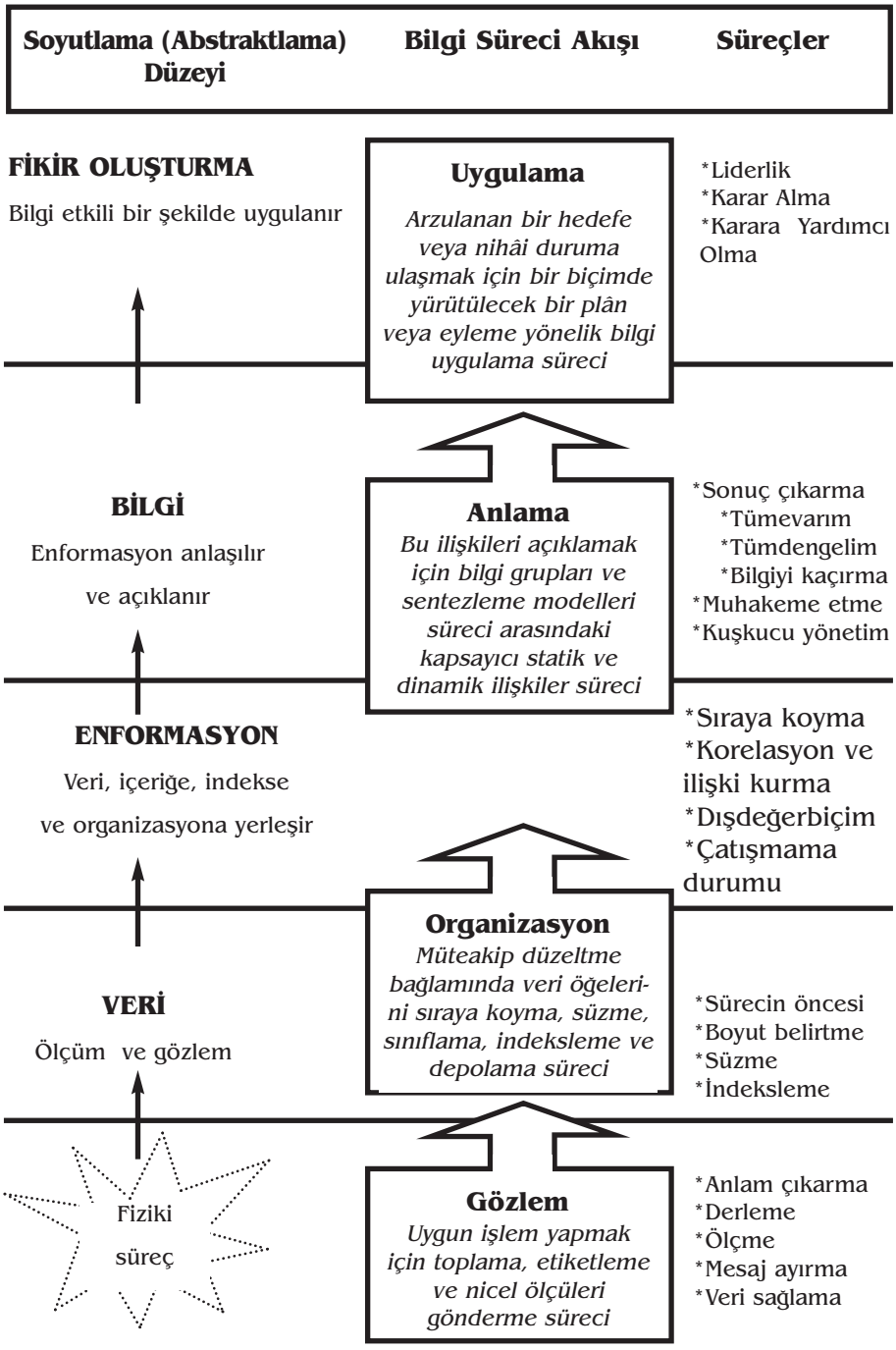
4 Uğur Yozgat, *Yönetim Bilişim Sistemleri*, (İstanbul: Beta Yayıncılık, 1998), s. 45.

5 Forsnet Bilgi Teknolojileri Web Sayfası'ndan alınmıştır. http://www.sanalteror.gen.tr/bilgi/index.html

6 Edward Walz, *Information Warfare: Principles and Operations*, (London: Artech House, 1998), s. 56.

Çünkü, bilgi tek başına bir anlam ifade etmediği gibi, aynı zamanda soyut bir kavram olarak karşımıza çıkmaktadır. Örneğin, bilgi teorisi içerisinde bilgi, istatistiksel metotların ölçülmesi, bilgi yönetimi içerisindeki bilgi de kısaca mesleklere ait olan bilginin iç ve dış dinamiklerinin değerlendirilmesi anlamını taşımaktadır. Bilginin anlaşılması için yoğunlukla kullanıldığı alanları verdikten sonra veri ve enformasyonun nasıl bilgi (knowledge) hâline dönüştüğünü izah etmek gerekir. Çünkü herhangi bir savaş sırasında iletilip alınan şeyin veri mi, enformasyon mu yoksa bilgi mi olduğunun bilinmesi ve ona göre tedbir alınması gerekir. Veri ve enformasyonun, hangi aşamalardan geçerek bilgiye dönüştüğü bilinmezse, karşı tarafın bilgilerine ulaşılamaz, ulaşılsa bile hangi veri/enformasyon/bilginin doğru hangisinin yanlış olduğu, bu istihbarata dayanarak neyin gerçekleşip gerçekleşmediği anlaşılamaz ve böylelikle yapılan bilgi savaşı olumsuz sonuçlanır. Bilgi hiyerarşisi, bilgiyi üç düzeyde tanımlamaktadır. Bunlar, veri, enformasyon ve bilgidir. Şekil-1[7] bu ilişkiyi detaylı olarak açıklamaktadır.

[7] Walz, *Information Warfare* ... s. 51.



Şekil-1. Bilgi hiyerarşisi

Kaynak: Edward Walz, Information Warfare: Principles and Operations, (London: Artech House, 1998), s. 56.

Tablo üzerinde bir örnek vermek gerekirse, özel işletmeler için pazar ve ekonomik ölçümler gözlem yolu ile elde edilebildiği için **veri** *(data)* sayılırken, bunların analizleri ve pazarın ekonomik davranış modellerinin anlaşılır bir yapıya dönüştürülmesi **enformasyon** *(information)* ve genel manada ekonomi, pazar, rekabetçilik ve stratejik plânlar uygulamaya yönelik olarak yapılan hazırlıklar **bilgi** *(knowledge)* sayılmaktadır. Son kategoride tüm bu aşamaların gerçekleşmesi ve şirketin başarıya ulaşması ise şirket ile ilgili bir fikir oluşturduğundan dolayı *(fikir oluşturma)* **wisdom** olarak adlandırılmaktadır.

Bilgi Savaşının Kavramsal Çerçevesi

Bilgi teknolojilerinin gelişmesine paralel olarak askerî trafiğin çok önemli bir kısmının ülkenin ulusal alt yapı sistemlerine yönelik olarak taşınması, kamu ve özel sektörlerin ağırlıkla bilgi tabanlı teknolojiler konusunda üretimde bulunmalarına neden olmuş ve geleneksel savaş yüzünü bilgi ve iletişim teknolojilerine çevirmiştir. Öyle ki, **gelişmiş ülkelerdeki bilgi, gelişmeyi olumlu yönde etkilerken; bu ülkeler tarafından bilginin tehdit unsuru oluşturabileceği sonradan anlaşılmıştır. Bu durumun fark edilmesiyle beraber "bilgi savaşları" teriminin doğması da çok uzun zaman almamıştır.**

Hâlen bilgi savaşı ile ilgili herhangi bir doktrin bulunmamasına ve üzerinde anlaşılmış inanç/kavram topluluğu olmamasına rağmen, bilgi savaşları çok kısa manada, "ulusal ve bu amaçla çatışmaların gerçekleşmesi için bilginin kullanılması"[8] olarak tanımlanmaktadır. Ulusal güç ise, diplomasi, ekonomik rekabet, askerî gücün kullanılması ile ulusal kaynaklardan bu yönde istifade edilmesi anlamına gelmektedir. Bilgi savaşlarında en güçlü silâh, bilgi/enformasyon ve dezenformasyondur ve bunlar savaşın biçimini tayin etmektedir. Bilgi savaşında önemli husus, bir ülkenin kendi bilgi alt yapısını koruyarak düşman birliklerinin bilgi sistemlerini, bilgi kaynaklarını ve bilgi alt yapısını imhaya yönelik olarak eylemlerde bulunmaktır.

Bilgi savaşı daha ziyade ileri teknolojiye sahip askerî silâhlar ile yapılan savaş olarak algılanmış olsa da, aslında karşı tarafa ait bilgi merkezli işlemcileri, bilgi sistemlerini ve bilgi tabanlı ağ yapılarını etkileyecek bir hareket gerçekleştirmek için oluşturulan ve savunma sistemleri ile yapılan savaştır. "Düşman birliklerinin askerî, siyasî, sosyal ve ekonomik alt yapılarını çökertmek için düşmanın bilgi tabanlı faaliyetlerine saldırılar gerçekleştirerek düşmanın gücünü ve zayıf nok-

---

[8] George J. Stein, "Information Warfare", *Airpower Journal*, (İlkbahar, 1995), s. 9.

talarını nispeten anlamaya çalışacak faaliyetlerde bulunmak"[9] olarak da anlatılmaktadır.

Bilgi savaşlarının devletler için ne denli önemli olduğunu aşağıdaki örnek açıkça anlatmaktadır. Körfez Savaşı, bilgi savaşının beşikteki dönemi olarak adlandırılabilir. Bu savaşta yeni nesil silâhların kullanılması ve 1990'larda gerçekleşen Balkan operasyonları bilgi sistemlerinde geçtiğimiz 10 yılda ciddî bir ilerleme olduğunu ortaya koymuştur. Örneğin, Körfez Savaşı sırasında Amerikan komuta kontrol mekanizmaları saniyede 2400 bit bilgi aktarımı yapabilirken, Bosna'da bu sayı saniyede 23 milyon bite çıkmıştır. 1991 yılında ancak bir saatte yollanabilen bilgi, 1998 yılında bir saniyede gönderilmektedir. Bir diğer örnek ise, 11 Eylül'de ABD'ye yapılan terörist saldırı sonucunda Afganistan'a yapılan müdahâle sırasında yaşanmıştır. Intelligence Online[10] dergisinde yer alan SOLIC[11] toplantısında ABD'nin Afganistan'a yönelik operasyonlarında bilgi savaşı teknolojilerinin tam anlamı ile kullandığını ve bunda da başarılı olduğunu yazmaktadır.

Hızı bu kadar yüksek olan bilgi savaşının olabilmesi için mutlaka bir "bilgi saldırısı"'nın (information attack) olması zorunluluğu vardır. Bilgi saldırısı, "doğrudan doğruya düşmanın gözle görülür bir şekilde fiziksel varlığına ait olan bilgileri değiştirmeden saptırmak"[12] olarak açıklanmaktadır. Bilgi saldırısına maruz kalan hedef kitle, kendini ister istemez bilgi savaşının içerisinde bulmakta ve bir bilgi operasyonu bombardımanına tutulmaktadır.

Bilgi savaşının çıkış noktasını bilgi operasyonu oluşturmaktadır. Bilgi operasyonu/harekâtı daha ziyade bilgi savaşları terimi ile bütünleşen stratejik bir terim olarak algılanmaktadır. Kısaca, "düşmanın bilgi ve bilgi sistemlerini etkileyecek eylemlerde bulunurken kendi bilgi sistemlerini savunma"[13] olarak izah edilebilir. Bilgi savaşı, bilgi operasyonları bağlamında şu şekilde değerlendirilebilir:

"Düşman olarak hedeflediğimiz kitleye belirli amaçları gerçekleştirmek veya savaşı kazanmak için kriz veya çatışma zaman-

---

9 George J. Stein, *Information Attack: Information Warfare in 2025*, (Washington: 11 Aralık 1996), s. 4.

10 "Washington Wins Infowar Battle", *Intelligence Online*, No: 423, 14-27 Şubat 2002, s. 1.

11 SOLIC toplantısı "13th Annual Operations/Low Intensity Conflict", Arlington, Virginia, 7-8 Şubat 2002'de yapılmıştır.

12 USAF, "Cornerstones of Information Warfare", (United States Air Force, 1995), s. 6. http://www.af.mil/lib/corner.html.

13 Manuel W. Wik, "Information Warfare and Information Operations", *Militarteknisk Tidskrift*, http://www.verkstaderna.se/mtt/pdf/100_4.pdf.

larında bilgi operasyonlarının idare edilmesi, yönetilmesi"[14] anlamında da kullanılmaktadır. Bu nedenle bilgi operasyonları, bilgiye yönelik bir saldırının gerçekleştirilmesinin ardından ona karşı yapılan eylemin adıdır.

Bütün bu açıklamalar, bilgi savaşının daha ziyade bilinen teorik boyutunu vermektedir. Yine bu kuramsal düzleme bağlı kalınarak bilgi bilimi çerçevesinde bilgi savaşını şu şekilde de değerlendirmek mümkündür: Enformasyon biliminde, bilgi alt yapısının içeriğini oluşturan üç adet kavram bulunmaktadır. Yalnız, bu kavramları açıklamadan önce, bilgi savaşının *"bilgi ile ilgili"* boyutunun anlaşılması için bilgi alt yapısının ne olduğu üzerinde durulmalıdır. Çünkü, bilgi savaşının temel dayanak noktası bilgi alt yapısından geçmektedir. Bir ülkenin bilgi alt yapısının çözümlenmesi; o ülke ile ilgili olarak yapılacak her türlü teknolojik istihbarat çalışmalarının başarılı olacağı anlamına gelmektedir. "Bilgisayar yazılımı ve donanımının oluşturulabilmesi için gerekli iş birliklerinin yapılması, veri depolama ve bununla ilgili ekipmanın üretilmesi, özbilgi *(abstract)* ve buna ilişkin uygulamalar ile tüm bu unsurlar arasındaki bağlantıların sağlanması ve bu alanda çalışacak olan personelin eğitimi" şeklinde tanımlanan bilgi alt yapısı, telefon ağları, uydu ve telsiz telefon ağları, özel ağlar ve internet ile diğer bilgisayar ve veri ağlarından oluşmaktadır.[15] Yani, bir ülkedeki bilgi alt yapısı, mevcut bilginin işlenmesine, depolanmasına, bir yerden bir yere iletilmesine ve bu bilgilere gerektiğinde erişilmesine olanak sağlayan teknolojileri içermektedir. Bu kadar geniş bir yelpaze içerisinde değerlendirilen bilgi alt yapısı, *bilgi kaynakları, bilgi sistemleri ve bilgi hizmetlerinden*[16] oluşmaktadır.

Bilgi savaşı ile ilgili olarak yukarıdaki açıklamalardan da anlaşılacağı üzere, bilgi alt yapısı kavramı, öncelikle bilgi sistemleri çerçevesinde ele alınmış ve buna dayanarak bilgi saldırısı ve sonrasında bilgi operasyonu/harekâtı olarak nitelenen düzeylerde gerçekleştirilmiştir. Aslında bilgi sistemi, bilgi savaşına başlanmadan önce ülkelerin alt yapılarını hazırlayarak gerekli makine ve ekipmanı temin ile organizasyonu oluşturma sürecidir. Bu, bilgi savaşının ilk ve en temel aşamasıdır. Daha sonra, gözden kaçırılmaması zorunlu olan bir 'ön araştırma

---

[14] "Information Warfare", *Information Warfare & Information Operations (IE/IO) A Bibliography Definitions*, Naval Postgraduate School Dudley Knox Library, 18 Eylül 2001, s. 1. http://web.nps.navy.mil/~library/bibs/IW-def.htm.

[15] Office of Technology Assessment, *Information Security And Privacy in Network Environments*, (Washington, D.C.: Government Printing Office, 1994), s. 27. http://www.epic.org/crypto/reports/ota_1994.html.

[16] Mustafa Sağsan, "'A k ı l l ı T o p l u m ' Olma Yolunda Ulusal Bilgi Stratejisi ve Bilgi Ortaklığı", *Stratejik Analiz*, Sayı. 18, (2001), ss. 88-89.

yapma' safhası bulunmaktadır. Bilgi savaşına başlamadan önce karşı tarafın pozisyonunu anlamak, mevcut güç kapasitesini öğrenmek ve gelebilecek saldırıların coğrafî olarak yerini tespit etmek için bilgi alt yapısının ikinci aşaması olan bilgi kaynaklarını kullanmak gelmektedir. Saldırıyı yapacak veya saldırıya uğrayacak olan ülkenin mevcut bilgi kaynaklarını kullanarak bilgi elde etme işi (bilgi kaynakları istihbaratı), bilgi kaynakları kısmında yer almaktadır.

Bilgi kaynakları istihbaratı yapabilmek için mevcut kaynakların hangi formlarda sınıflandırıldığını bilmek gerekmektedir. İstihbarat çalışması esnasında elde ettiğimiz verilerin analizini daha kolay yapabilmek için bu sınıflamanın gereği vardır. Nitekim Dorothy, bilgi savaşları bağlamında bilgi kaynaklarını beş sınıfa ayırmıştır: bilgiye erişim araçları *(containers),* bilgiyi taşıyabilen araçlar *(transporters),* bilgiyi algılayabilen araçlar *(sensors),* (bilgiyi kaydedebilen araçlar *(recorders)* ve bilgiyi işleyebilen araçlar *(processors).*[17]

Bilgi alt yapısının son aşaması olan *bilgi hizmetleri*[18] kavramını da bilgi savaşı terimi içerisinde şu şekilde teorik bir çerçeveye oturtmak mümkündür. Bilgi kaynakları sonucunda elde edilen veri/enformasyon/bilgilerin, saldırıda bulunmak isteyen veya saldırıya maruz kalacak olan ülkenin bilgi sistem ve ağına uygun olarak adapte ederek iç organizasyon yapılarının hizmetine sunulmasıdır.

Tüm bu aşamalar tamamlandıktan sonra bilgi saldırısı ve sonrasında da bilgi operasyonu/harekâtı gerçekleşir. **Bilgi savaşı konusu ile ilgili literatür, bu terimi tanımlarken bilgi savaşı için bir ön şart olan bilgi alt yapısını (yani bilgi sistemleri, bilgi kaynakları ve bilgi hizmetleri) gözden kaçırmaktadır.**

Stratejik Bilgi Savaşı

Gittikçe karmaşıklaşan uluslar arası ortam ülkeleri yeni stratejik çıkarların peşinde koşmaya ve bu bağlamda kendilerine yeni stratejik hedefler koymaya itmiştir. Böylelikle, her ülke kendi çıkarları doğrultusunda yeni stratejik güç oluşturmaya başlamıştır. Bu güç içerisinde de bilgi savaşları çok geçmeden yerini almış ve 21. yüzyılda yeni bir konsept olan "stratejik bilgi savaşı" doğmuştur. Stratejik bilgi savaşı, bir ülkenin stratejik hedeflerinin dikkate alındığı ve geleneksel stratejik

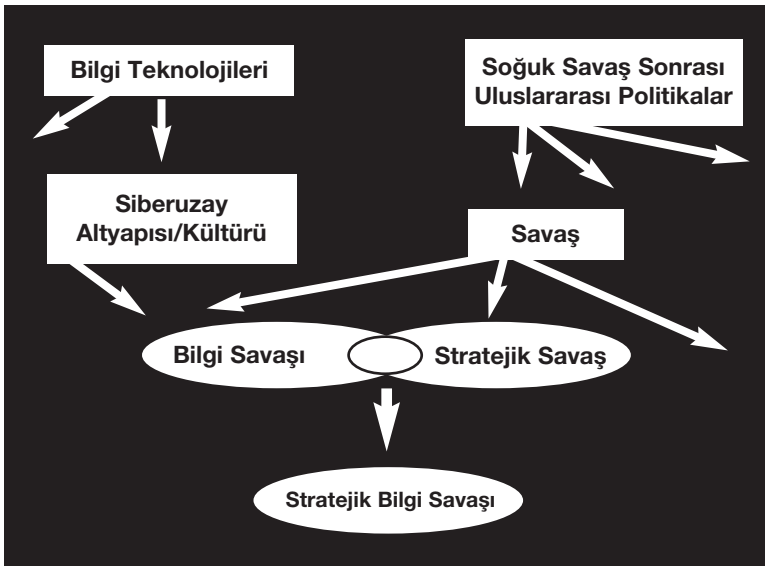
---

17 Doroty E. Denning, *Information Warfare and Security*, (New York: Addison-Wesley, 1999), s. 21.

18 Bilgi Hizmetleri: Bilginin sağlanması, düzenlenmesi ve yayımı ile ilgili kamu ve özel sektörde bulunan çeşitli türdeki sistem ve ağlardır. Bunlar veri bankaları, veri tabanları, kütüphane sistemleri, kütüphane hizmetleri, dokümantasyon merkezleri ve hizmetleri, arşivler ve istatistiksel hizmetlerle bunların kablolarla bağlantılı kurulmuş olan şeklidir.

savaş konseptinden farklı olarak bilgi teknolojileri sayesinde ulusal bilgi alt yapısını (bilgi kaynakları, bilgi sistemleri, bilgi hizmetleri) ve buna ilişkin noktaları çökertmek amacıyla yapılan savaş olarak tanımlanmaktadır.

Aşağıdaki şekilde de görüldüğü gibi stratejik bilgi savaşının oluşabilmesi için iki farklı açının birleştirilmesi gerekmektedir. Bunlardan birincisi, bir ülkenin sahip olduğu bilgi teknolojileri ve siber uzay alt yapısı/kültürü; diğeri ise o ülkenin etrafında cereyan eden uluslar arası siyasal ortama ilişkin durumlardır. Birinci yöndeki bilgi teknolojileri ve siber uzay alt yapısı/kültürü çalışmaları "bilgi savaşlarını" oluştururken; ikinci kısım ise, Soğuk Savaş sonrası uluslar arası ortamdaki mevcut geleneksel savaş modelleri sonucunda stratejik savaş modeli oluşturmaktadır. İşte bu iki kısmın; yani stratejik savaş ile bilgi savaşının kesiştiği nokta, "stratejik bilgi savaşı" konseptini meydana getirmektedir.



Şekil-2. Stratejik Bilgi Savaşı
Kaynak: (Roger C. Molander, Andrew S. Riddile, *Strategic Information Warfare: A New Face of War,* (California: RAND, National Defence Research Institute, 1996), ss. 15-33.

Stratejik bilgi savaşı kavramını daha iyi anlamak için Molander ve Riddile'ın bu konuda geliştirdiği tanımlayıcı yedi özelliği bulunmaktadır.[19]

1-Düşük Giriş Maliyeti: Stratejik bilgi savaşının oluşabilmesi için öncelikle çok güçlü iki unsura ihtiyaç vardır. Bunlardan birincisi, mikrobilgisayarlar; diğeri de bu mikrobilgisayarların bağlantılarını ve haberleşmelerini sağlayan karmaşık ve hızlı iletişim ağlarıdır. Potansiyel düşmanların kapasitelerinin, sayılarının ve çeşitlerinin artması bilgi savaşının dayanağı olan bu tür teknolojilerin maliyetlerinin düşmesini zorunlu kılmıştır. Ayrıca, bilgi teknolojilerinin kullandığı sistemlerin karmaşıklığının ve bilgi/gücün dağılımının artması stratejik bilgi savaşlarının tanımlayıcı özelliğini ortaya koymaktadır. Stratejik bilgi savaşında maliyetlerin düşük olmasının en önemli sonuçlarından bir tanesi herhangi bir ülke, kurum veya kişinin kolaylıkla saldırıya maruz kalabilmesidir.

2-Geleneksel Sınırların Belirsizliği: Bu tanımlayıcı özellik, stratejik bilgi savaşı için coğrafîk, bürokratik, hukuksal ve kavramsal anlamda yeni sorunlar ortaya çıkarmaktadır. Stratejik bilgi savaşının gerçekleşmesi durumunda bu sorunların varlığı söz konusu değildir. Çünkü artık taraflar arasında bu tür ilişkilerin geçerliliği ortadan kalkmıştır ve savaş da bu anlaşmazlıklardan ötürü çıkmıştır. Örneğin, saldırıya uğrayan bir ülkenin sınırlarını bilmek, coğrafîk yapısını çözümlemek, hukuksal ve bürokratik olarak yapısını çözümlemek ve geleneksel savaş yöntemlerini kullanmanın önemi kalmamıştır. Burada dikkati çeken en temel etken belirsizliklerin, tartışmaların ve saldırıya maruz kalabilme ihtimallerinin oldukça yüksek olmasıdır. Stratejik bilgi savaşına taraf olan ülkeler için artık iç/dış politikalar, geliştirilen stratejiler, doktrinler, roller ve misyonların modası geçmiştir ve yeniden gözden geçirilme ihtiyacı vardır. Tüm bunların sonucu olarak da saldırı altında kalan ülke, kim tarafından saldırıya uğradığını bilememektedir.

3- Algı Yönetiminin Genişlemesi ve Yeni Roller: Devlet ve devlet dışı aktörler için bilginin rekabetçi bir ortamda güvenilir kaynakları kullanarak kapasitenin yükseltilmesi anlamına gelen bu niteleyici özellik ile hedeflenen; hükümet tarafından gerçekleştirilen girişimlerin kapasitesini düşürerek tartışmalı eylemler için iç desteğin yaşamasını ve inşa edilmesini sağlamaktadır. Bu amaçla da devlet ve devlet dışı aktörlerinin algılarının savaş psikolojisine girdirilmesi gerekliliği vardır.

---

[19] Roger C. Molander, *Andrew S. Riddile, Strategic Information Warfare: a New Face of War*, (California: RAND, National Defence Research Institute, 1996), ss. 15-33.

4-Yeni Stratejik İstihbarat Modellerinin Oluşması: Karşı taraftaki düşmanın niyetini anlamak ve kapasitesini öğrenmek amacıyla yapılan stratejik istihbarat, klâsik istihbarat toplama ve analiz etme metotlarının etki alanını sınırlamıştır. Ayrıca, devletler, kendilerine gelebilecek tehditlerin doğasının hızla değişmesinden ötürü, ülkelerinin gerek coğrafî gerekse sanal ortamda yerlerinin belirlenmesi zorluğu ile karşı karşıya kalmaktadırlar. Bu özelliğin bir sonucu olara da düşmanın kim olduğu, niyeti ve kapasitesinin durumunun bilinmesi gittikçe daha da zorlaşmaktadır. Bu zorluğu da aşabilmek için yeni istihbarat modelleri üzerinde çalışmak gerekmektedir.

5-Taktik İkaz ve Saldırıların Anlaşılması Zorluğu: Stratejik bilgi savaşında, taktik ikaz/hücumların tespit edilmesi aşırı derecede zordur. Çünkü, saldırı amaçlı üretilen bir enformasyonun karşısında dezenformasyon bulunma ihtimali vardır. Bu yüzden kim tarafından nasıl saldırıya uğranıldığının bilinmesi imkânsızdır.

6-Yeni Müttefiklerin Oluşumu ve Devamlılığının Zorluğu: Stratejik bilgi savaşları sayesinde, devletlerin herhangi bir çatışma durumunda gerek bölgesel, gerekse uluslar arası bir koalisyona girmesi zorlaşmaktadır. Çünkü, bu tür bir savaşta saldırıda bulunan taraflar özellikle müttefik ise, birbirlerinin niteliklerini belirlemede zorluklar yaşamaktadırlar. Çünkü her ne kadar müttefik gibi de görünseler ulusal güvenlikleri için birbirlerinden gizledikleri bilgiler bulunmaktadır. Bu nedenle, müttefik olarak stratejik bilgi savaşına girmek, başkalarına dolaylı veya doğrudan bağlı olmak anlamına geldiğinden müttefik devletler arasında da bir çatışma çıkabilme ihtimali bulunmaktadır.

7-ABD'nin Saldırıya Açık Bir Ülke Olması: ABD'nin hegemon güç olmasından kaynaklanan saldırıya maruz kalabilme ihtimali ABD'yi siber uzay çalışmalarında daha atak ve hızlı olmaya itmiştir. ABD'nin stratejik bilgi savaşına yönelik olarak attığı adımlardan birisi, yararlı stratejik hedefleri genellikle bilgi-tabanlı alt yapı etrafında toplamasıdır. Bu nedenle 2002 yılı bütçesinden **2,7 milyar dolar** ve 2003 yılı bütçesinden ise **4,2 milyar dolar "sanal güvenlik harcamaları"** için ayrılmıştır.[20]

Stratejik bilgi savaşının niteliksel özelliklerini oluşturan bu yedi unsur, bir ülkenin ulusal bilgi alt yapısına yönelik olarak gelebilecek saldırıların ve sonuçlarının neler olabileceğini anlatmaktadır. Bu nedenle, yüksek teknolojiyi elinde bulunduran bir ülke, siber saldırılar sonucu oluşan tehditlere karşı hazırlıklı olmalı ve bu konuda güvenlik poli-

[20] [Bağımsız İletişim Ağı Online Web Sayfası], "Enformasyon Savaşı İçin Ağır Silâhlanma", http://www.bianet.org/diger/makale8406.htm , s. 2.

tikalarını yeniden gözden geçirmelidir. Örneğin, bir ülkenin bilgi alt yapısının savunulmasının hangi kurum veya kuruluş tarafından sorumlu olabileceği hususu belirginleşmelidir. Siber saldırıların kim tarafından ne zaman ve nerede yapılacağı belli olmadığı için bilgi teknolojilerini yoğun olarak kullanan ülkeler, bu konuda mutlaka savunma stratejilerini oluşturmalıdırlar. Örneğin, siber saldırıya uğrayan bir ülke ister istemez kendisini stratejik bir bilgi savaşının içerisinde bulacaktır. Böyle bir durumda: "saldırıya maruz kalan taraf, karşı tarafa benzer bir şekilde mi cevap vermeli veya bunun için geleneksel silâhlarını mı kullanmalı yoksa her iki yöntemi de mi uygulamalı?" sorularını gözden geçirmeli ve buna göre tedbir almalıdır.

Net Savaş ile Siber Savaş Arasındaki Fark

Birçok yazar, bilgi savaşını tanımlarken siber savaş veya net savaş kavramlarından söz etmekte ve bu kavramların izah edilmesiyle bilgi savaşı kavramının açıklığa kavuşacağını iddia etmektedir. Örneğin, editörlüğünü John Arquilla and David Ronfeldt'in yaptığı *'In Athena's Camp: Preparing for Conflict in the Information Age'*[21] adlı kitapta, yazarı yine kendileri olan *"Cyberwar is Coming"* adlı makalede de belirtildiği gibi: "her iki savaş çeşidi de birbirinin benzeridir." yorumu bu iddiayı açıkça ortaya koymaktadır. Halbuki, siber savaşlar ve net savaşları bilgi savaşlarının çeşitleri olmakla birlikte 'Net Savaşı', toplumlar veya devletler arasında bilgiyle ilişkili çatışmaların düzeylerinden bahsetmektedir. Net savaşı, sivil alanda gerçekleşen ve rakiplerin algılama süreçlerini etkilemeye çalışan bir savaştır. Diplomasi, propaganda ve psikolojik mücadele, siyasî ve kültürel yıkım, düşman birliklerin yerel medyalarında parazitlik yapma ve aldatma, bilgisayar ağları ve veri tabanlarının süzülmesi, bilgisayar ağları karşısında muhalif birliklerin ilerlemesini engellemek gibi faaliyetleri içermektedir.[22] Yani rakibin algılamasını engelleyip onu savaştan caydırmak ve bilgisayar ağları aracılığı ile gerçekleştirdiği eylemleri engellemek amacı ile yapılmaktadır.

Siber Savaş ise, bilgi ile ilişkili ilkelere göre askerî operasyonların yürütülmesi anlamına gelmektedir. Siber savaş ile düşman birliklerinin bilgi ve iletişim sistemlerinin kesilmesi ve yıkılması amaçlanmaktadır. Başta komuta kontrol olmak üzere, istihbarat toplamak, işlemek ve dağıtmak; dost veya düşman birliklerini tanımak, pozisyonlarını sapta-

---

[21] John J. Arquilla, David F. Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age*, (RAND Corporation, 1997), s. 27., Elektronik kitap için bkz. http://www.rand.org/publications/MR/MR880.

[22] John J. Arquilla, David F. Ronfeldt, "Cyberwar and Netwar: New Modes, Old Concept of Conflict", http://www.rand.org/publications/randreview/issues/RRR.fall95.cyber/cyberwar.html.

mak gibi taktik iletişimlerini belirlemek ve akıllı silâh sistemleri gibi farklı teknolojileri içermektedir. Siber savaşın mahiyetinde, düşmanın bilgi ve iletişim devreleri içerisine zorla veya izinsiz olarak girerek dezenformasyonun yayılmasını elektronik olarak çökertmek vardır.[23] Bu savaşta, bilgi savaşçıları düşmanın bilgi merkezlerine (bilgisayar ağlarına, haber kanallarına) ani ve kesin saldırılar yaparken; net savaşı daha ziyade dışarıdan gelecek tehditlere karşı düşmanın algılamasını engellemek amacıyla yapılmaktadır. Sonuç olarak, siber savaş, genel olarak saldırı amaçlı olurken, net savaş dışarıdan gelecek saldırılara karşı savunma amacına yönelik olarak sistem geliştirmektedir.

Bilgi Savaşı ve Yeni Tehditlere Karşı Tedbirler

Yüksek düzeydeki bilgi teknolojileri, bir yandan bilgi sistemlerinin bütünlüğünün bozulmasını sağlarken, diğer yandan da karşı güçlerin devlet alt yapılarını bozguna uğratmıştır. Böylelikle, her devlet kendi teknoloji üstünlüğünü kullanarak karşı tarafla çatışma içerisine girmeye başlamıştır. Bu teknolojik üstünlük sağlama çatışması ise, doğrudan doğruya uluslar arası sistemleri, ticarî iletişimleri ve uydu gizli izleme sistemlerine olumsuz yönde yansımıştır. Bu çatışma, devletleri ve toplumları bilginin kullanılması ve iletilmesi hususunda bir takım tehditlerle karşı karşıya bırakmıştır. Bilgi savaşı bu tehditleri beş çeşit başlık altında toplamıştır.

- Enformasyon teknolojilerinin hızla yayılması ve görece ucuz olması, devlet dışı aktörlerin, mafya örgütlerinin, terörist grupların, hatta bağımsız bireylerin ve küçük devletlerin de enformasyon savaşı sürecine geçmesini kolaylaştıracaktır.
- Enformasyon savaşı hususunda henüz bir hukukî düzenleme yoktur. Uluslar arası anlaşmaların olmaması onu daha da etkili hâle getirmektedir.
- Bu alanda uluslar arası anlaşmaların yokluğu ortaya bir üçüncü tehdit unsurunun çıkmasına neden olabilir: Algılanamayan duyguların; menfaat ve tercihleri etkileyebilecek, yönlendirecek yeni teknolojilerin ortaya çıkması.
- Enformasyon savaşında saldırıların gelişme hızı, kriz yönetimi sürecine izin vermemektedir.
- Eskiden herkese açık olmayan enformasyonun artık hemen herkes için neredeyse açık olmasıdır.[24]

---

[23] Arquilla, Ronfeldt, "Cyberwar and Netwar:..."

[24] Timothy L. Thomas, "Deterring Information Warfare: A New Strategic Challenge", *Parameters*, Cilt. 24, Sayı. 4, (1996), ss. 3-4.

Üretilen her ürünün, beraberinde bir takım olumsuzlukları getirmesi kaçınılmazdır. Teknolojinin de toplumlar için bir ürün olduğunu düşünürsek; bunun, özellikle devletlerin ulusal güvenliğini tehdit edici yönde kullanılmasını engellemek olanaksızdır. Ancak, bu teknoloji üretilirken beraberinde üretilen bu teknolojiye karşı gelebilecek tehditlerin de bilgisi çıkartılırsa, alınacak karşı tedbirler sayesinde ulusal güvenliğe gelebilecek saldırıları en aza indirme şansımız bulunmaktadır.

Bilgi savaşları konusunda alınması gerekli bir diğer tedbir ise, teknoloji-yoğun ülkelerde, teknolojinin hangi amaçlara yönelik olarak kullanılacağını belirlemek için gerekli yasal uygulamaların başlatılmasıdır. Özellikle uluslar arası hukuk çerçevesinde düzenlenmesi gereken bu durum, objektif olarak hazırlanmalı ve yaptırım gücü güçlü olmalıdır.

Son tehdit olan bilginin artık herkese açık olmama durumu ise, ancak gelişmemiş devletlerin uygulayabileceği bir durumdur. Bu görüşün tam tersine bilgi, 21. yüzyıl teknolojileri aracılığı ile bilakis herkes tarafından kullanılabilir ve paylaşılabilir olmalıdır. Gelebilecek tehditlere ve yanılgılara karşı güçlü bir bilgi savunma sistemi geliştirilmeli ve bu sistem değişen teknolojilere karşı sürekli gözden geçirilmelidir.

Bilgi Savaşının Çeşitleri

'Bilgi Savaşı''nın çeşitlerini vermeden bilgi savaşı terimini teorik bir çerçeveye oturtmak mümkün değildir. Bilgi savaşı çeşitleri kaynaklarda farklı şekillerde ele alınmıştır. Örneğin, National Defence University'den Martin C. Libicki *"What is Information Warfare"* adlı makalesinde yedi başlık altında sıralamıştır:

1.C2W Komuta-kontrol Savaşı

2.İstihbarat Merkezli Savaş

3.Elektronik Savaş

4.Psikolojik Operasyonlar

5.Korsan Savaşı

6.Ekonomik Bilgi Savaşı

7.Siber Savaş.[25]

[25] Martin C. Libicki, "What is Information Warfare", *National Defence University*, 28 Mayıs 1995, s. 1.

ABD Hava Kuvvetlerine ait *"Cornerstones of Information Warfare"* isimli dokümanda ise, bilgi savaşları genel olarak 'Saldırı ve Savunma Bilgisi' ile 'Sömürü Amaçlı Bilgi' olarak ikiye ayırmış ve 'Saldırı ve Savunma Bilgisi' başlığı altında bilgi savaşının çeşitlerine yer verilmiştir:

1.Psikolojik Operasyonlar

2.Askerî Aldatma

3.Güvenlik Tedbirleri

4.Fizikî Yıkım

5.Bilgi Saldırısı

6.Elektronik Savaş.[26]

Son olarak, Edward Walz,[27] bilgi savaşlarının çeşitlerini bilgi operasyonları başlığı içerisine yerleştirmiş ve şu şekilde bir sınıflandırma yapmıştır:

1.Psikolojik Operasyonlar

2.Operasyonel Aldatma

3.Elektronik Operasyonlar

4. Fizikî Yıkım

5.İstihbarat

6.Karşı İstihbarat

7.Bilgi Güvenliği

8.Operasyon Güvenliği

Tüm bu sınıflamalardan da anlaşıldığı üzere, bilgi savaşları genel olarak "bilgi operasyonları" veya "saldırı ve savunma bilgisi" başlıkları altında geçmektedir. Bu sınıflamalar verdikten sonra şimdi de genel olarak bu terimlerin anlamlarına göz atmakta yarar vardır.[28]

- **Komuta Kontrol Savaşı:** (C2W): Düşmanın iletişim sistemini ve orduların sevk ve komutasını engellemek için yapılan saldırılardan oluşur.

---

26 USAF, "Cornerstones of Information Warfare", (United States Air Force), s.4. http://www.af.mil/lib/corner.html.

27 Edward Walz, *Information Warfare: Principles and Operations*.

28 Bu maddelerin açıklanması için National Defence University'nin web sayfasında, "What is Information Warfare" isimli makalede ek olarak bulunan "The World Of Information Warfare" isimli resim dosyasından faydalanılmıştır. Resmi görmek için bkz. http://www.ndu.edu/inss/strforum/forum28.gif.

- **İstihbarat Merkezli Savaş:** Tarayıcıların, işlemcilerin ve keşif belirleme ve zarar tespit sistemine entegrasyonunu gerçekleştirmekle kullanılmasıdır. İstihbarat merkezli savaşı anlayabilmek için özellikle teknolojik istihbarat çeşitlerinin neler olduğunu bilmek gerekir. Teknolojik istihbarat çeşitlerinin izah edilmesiyle istihbaratın herhangi bir savunma veya saldırı amaçlı çatışma esnasında nasıl kullanılması gerektiği açıkça ortaya çıkmaktadır. Dünyada 100 ülkenin kayıtlı yaklaşık elli bin bilgisayar ağı olduğunu düşünürsek;[29] teknolojik istihbaratın bilgisayar destekli çeşidinin 21. yüzyıldaki kapasitesini algılamak hiç de zor olmayacaktır. Bilgisayar teknolojilerinden istifade edilerek gerçekleştirilen ve bilgisayarın bilgiyi toplama, sistemleştirme ve dağıtma amacına yönelik olarak kullandığı bu teknolojik istihbarat türüne kısaca "bilgisayar tabanlı istihbarat" denilebilir. Bir diğer teknolojik istihbarat türü ise, iletişim araçlarının kullanılarak yapıldığı bilgi toplama faaliyetleridir. Örneğin, dijital iletişimin en önde gelen araçlarının (telefon, TV, faks) kullanılarak yapıldığı bu tür, popüler olarak yapılan istihbarat çalışması niteliğini taşımaktadır. Bunun en güzel ispatı ise, Tayland'da yaklaşık 500 bin; Macaristan'da ise 700 bin kişinin hücreli (dijital) abonelik için sıra beklemesidir.[30] Bilgi teknolojileri ile ilgili son istihbarat türü ise, uydu yayın sistemlerinin kullanarak yapıldığı bilgi toplama faaliyetidir. "gerçek zamanlı istihbarat"[31] şeklinde de ifade edilen bu tür; bilgi istihbaratı türleri içerisinde en etkilisi olmakla birlikte 21. yüzyılda da en fazla tercih edilenidir.
- **Elektronik Savaş:** Hedef birliğin elektron ve enformasyon akışını kesmek, bozmak veya müdahâle etmek üzere tasarlanan komuta kontrol veya istihbarat merkezli savaşa uygulanabilir teknikler bütünüdür.
- **Psikolojik Operasyonlar:** Diğer savaş modellerinin algılamalarını, niyetlerini ve oryantasyonlarını etkilemek için kullanılmaktadır. Bilgi savaşları psikolojik savaşın bir yöntemidir. Psikolojik operasyonların temel amacı, bir ülkenin halkının ve karar alıcılarının zihinlerini ele geçirmek ve ülkenin menfaatleri doğrultusunda yönlendirmektir.
- **Korsan Savaşı:** Yazılım korsanlarının bilgi sistemlerine saldırmalarına dayalı olan bu savaş tipinde, askerî ve sivil olarak bilgi sistemlerini tahrip etmek, bozmak, sömürmek veya uyumlu-

---

29 Richard F. Ricardelli, "The Information and Intelligence Revolution," *Military Review*, Cilt 75, Sayı 5, (1995), s. 4.

30 "The Information Revolution: How Digital Technology is Changing the Way We Work and Live", *Businessweek*, (Mayıs, 1994), s. 49.

31 Ricardelli, "The Information and Intelligence...," s. 5.

laştırmak için kötü yazılım teknikleri kullanmak (yani virüs programları üretmek) vardır.

- **Ekonomik Bilgi Savaşı:** Bilgi ticaretinin gerçekleşmesi için bilgi ekonomilerine karşı yapılan savaştır. Devlet politikasının bir aracı olarak ticarette kullanılan bilginin manipülasyonunu içerir.
- **Siber Savaş:** Sanal alemde savaşma olarak da bilinen bu bilgi savaşı türü, bireylere veya gruplara karşı bilgi sistemleri kullanılarak yapılmaktadır.

Bilgi savaşı kavramı içerisine giren diğer terimleri de şu şekilde açıklamak mümkündür:

- **Fiziksel Yıkım:** Bilgi alt yapısının fiziksel öğeleri olarak tanımlanan hava koşulları, operatörler ve elektrik güçlerini tahrip etmek veya öldürmek hedeflenmektedir. Fiziksel saldırılar, özellikle sistem için kritik noktada bulunan insanları öldürmeye yönelik olarak yapılmaktadır. Bu hedeflenirken de sistem yöneticisinin kullandığı yazılım, donanım, iletişim linkleri ve veri tabanları sistemin alt yapısını öğrenmek ve etkilemek için ele geçirilmeye çalışılır.[32]
- **Operasyonel Aldatma:** Düşmanın askerî karar alıcılarını dost gibi görünerek önceden tasarlanmış bir şekilde yanıltmasını amaçlamaktadır. Ayrıca, düşmanın hareketini veya hareketsizliğinin bilinmesini sağlar.[33] Askerî aldatma ile aynı anlamda kullanılan bu kavram, düşmanı kendi kapasitemiz ve niyetlerimiz hususunda yanıltmak olarak açıklanabilir.
- **Güvenlik tedbirleri:** Operasyonel veya askerî aldatmanın tam tersine, düşmanın bir ülkenin niyetini ve kapasitesini öğrenmesi konusunda engelleyici tedbirleri almaktır.[34]

Saldırı ve Savunma Amaçlı Bilgi Savaşı (Operasyonu) Modelleri

1-Saldırıya Yönelik Bilgi Savaşı

Bilgi savaşının tüm bu çeşitlerinden farklı olarak bilgi ile ilgili operasyonlar iki amaca yönelik olarak yapılmaktadır. Bunlardan birincisi, saldırı *(offensive)* temeline dayalı olan bilgi operasyonudur. "Bu savaş modelinin hedefi, karşı tarafın bilgiye yönelik faaliyetlerini etkilemek veya ele geçirmektir."[35] Bilgiye yönelik faaliyetler ise genel olarak

---

32 Edward Walz, *Information Warfare*, ss.217-218.

33 Edward Walz, *Information Warfare*, s.211.

34 USAF, "Cornerstones of Information Warfare", s. 5.

35 Edward Walz, *Information Warfare*, s. 251.

daha önceki bölümlerde de bahsettiğimiz "bilgi alt yapısı" başlığı altında toplanan bilgi kaynakları, bilgi sistemleri ve bilgi hizmetleridir. Bilgi kaynaklarının tahribi, ele geçirilmesi veya yok edilmesi anlamını da içeren saldırı amaçlı operasyonlar, hücum eden ve savunmayı gerçekleştiren aktörler arasında yapılmaktadır.[36] Bu saldırılar, casusluk ve istihbarat operasyonları vasıtasıyla gizliliğin sağlanması, bilginin korsanlığı, bilginin çalınması veya sızdırılması, kimlik hırsızlığı ve fiziksel hırsızlık olarak kategorilere ayrılmaktadır.

Bu kategorilerden ilki olan **"istihbarat operasyonları ve casusluk"** farklı şekillerde yapılmaktadır. Örneğin, "açık kaynaklı bilgi istihbaratı" gazeteler, dergiler, ticarî veri tabanları ve internet gibi sınıflanmamış bilgi kaynakları vasıtasıyla gerçekleştirilmektedir. "Beşerî istihbarat" ise kaynağını insanlardan almakta ve savunma hattında bulunan herhangi bir aktörün saldırıda bulunacak tarafa casusluk yaptırılmasıyla oluşmaktadır. Radyo veya iletişim dalgalarının yönünü değiştirmek veya ele geçirmek şeklinde nitelendirilen "sinyal istihbaratı" ve kameraların, casus uyduların ve diğer tip araçların savunmadaki tarafın fiziksel çevresini betimlemek amacı ile kullanıldığı "betimleme istihbaratı", bilgi operasyonları içerisinde saldırıda bulunacak tarafın kullandığı istihbarat modelleri olarak örnek gösterilebilir. Bunlara ek olarak "rekabetçi istihbarat" ve "ekonomik istihbarat" da bu saldırgan aktörlerin kullandığı istihbarat operasyonları metotlarıdır.[37]

İkinci tip bilgi saldırısı bilgi korsanlığıdır. Bilgi ile ilgili telif hakları ve ticarî markaların bir gizliliğinin olmaması, entelektüel mülkiyetin daha fazla elde edilebilir ve saldırıya maruz olacak kadar değerlenmesi, bilginin dağıtımını ve satılmasını zorlaştırmış hatta tehlike altına sokmuştur.

Üçüncü tip bilgi operasyonu bilginin fizikî alanlara veya bir kurumun bilgisayar sistemlerine sızması veya sızdırılmasıdır. Casuslar veya bilgisayar korsanları tarafından gerçekleştirilen bu işlemin amacı kurumun bilgi kaynaklarına, basılı dokümanlarına ve elektronik bilgi ve bilgisayar ağlarına saldırmaktır. Bunlara ek olarak "kimlik hırsızlığı" ve "fiziksel hırsızlık" başlıkları altında anılan saldırı amaçlı bilgi operasyon çeşitleri bulunmaktadır.

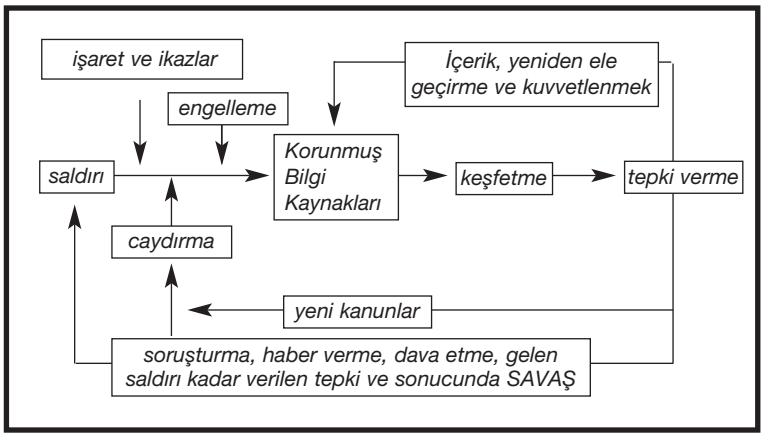
---

[36] Doroty E. Denning, *Information Warfare*, s. 28.

[37] Doroty E. Denning, *Information Warfare*, ss. 32-33.

2-Savunmaya Yönelik Bilgi Savaşı

İkinci bilgi savaşı modeli ise, saldırı amaçlı operasyona karşılık olarak yapılan savunma bilgi savaşıdır. Savunma bilgi savaşı bilgi kaynaklarını korumak için yapılmaktadır. Savunma amacına yönelik olarak yapılan altı tip bilgi savaşı türü bulunmaktadır: engelleme, caydırma, bildirme ve uyarma, keşfetme, acil duruma hazır olma ve tepki verme.[38] Aşağıdaki şekilde savunma amaçlı bilgi savaşı ve güvenliğinin unsurları yer almaktadır.



Şekil-3. Savunma amaçlı bilgi savaşı ve güvenliğinin unsurları
Kaynak: Doroty E. Denning, *Information Warfare and Security*, (New York: Addison-Wesley, 1999), s. 38

Sonuç

Teorik olarak kavramların açıklaması amacını güden bu makalede kısaca şu söylenebilir: 21. yüzyılın en büyük tehdidinin adını oluşturan "siber tehdit"'lere karşı alınabilecek önlemlerin başında bilgi savaşlarına hazır olmak gelmektedir. İleri teknolojiyi kullanan devletler, bu tehdit bilincinin etkisiyle bilgi savaşlarına karşı gerekli tedbirleri almışlar ve atılması gerekli adımları hızla tamamlamaya çalışmaktadırlar. Durum böyle olunca, gelişmekte olan ülkelerin durumunun ne olacağı konusu tartışmaya açık olmakla birlikte, ciddî anlamda bir tehditle karşı karşıya kaldıkları gerçeği göz önüne çıkmaktadır. **Teknoloji-yoğun (gelişmiş) ülkeler, bilgi teknolojilerini tehdit amaçlı kullanma olanağına sahipken, gelişmekte olan ülkelerin bu teknolojileri takip etmekten başka bir alternatiflerinin olma-**

[38] Doroty E. Denning, *Information Warfare*, ss. 3-33.

yacağı düşünülebilir. Bu yüzden gelişmekte olan ülkeler, takipten nasıl korunuruz? sorusuna çok geçmeden yanıt bulmalı ve bu yönde teknoloji politikası gütmelidirler.

Araştırmada çıkarılacak ikinci bir sonuç ise, bilgi savaşının aşamaları ile ilgilidir. Bilgi savaşının gerçekleşmesi için öncelikle bilgi alt yapısına yönelik olarak çalışmalar başlatılmalıdır. Bu girişimler, saldırıda bulunacak ülkenin iç bilgi sistemlerinin oluşturulması aşamasıyla başlamaktadır. Sonra, saldırıya maruz kalacak bölge veya ülkenin, bilgi toplama faaliyetlerini içeren bilgi kaynaklarını inceleme ve araştırma kısmı ile devam etmektedir. Elde edilen bilgiler daha sonra savaş yapmak isteyen ülkenin iç hizmetine sunularak incelemeye alınmakta; bu ise bilgi biliminin bilgi hizmetleri aşamasını oluşturmaktadır. Tüm bu işlemler gerçekleştikten sonra da, bilgi saldırısı ile start verilen bilgi savaşı; yapılacak olan bilgi operasyonları ile desteklenmektedir.

Stratejik bilgi savaşının tanımlayıcı özelliğinden yola çıkarak şöyle bir sonuca da varılabilir. Geleneksel savaş teorisi içerisinde yer alan stratejik savaşın bilgi teknolojileri destekli biçimi olarak ifade edilen stratejik bilgi savaşları, bilgi savaşlarının da ötesinde daha az maliyetle, tahrip gücü daha yüksek olan bir savaş modelidir ve bilgi savaşlarını dahi gelenekselleştirmiştir. Bu nedenle, gelişmiş ülkeler bilgi savaşı aşamasını tamamladıktan sonra stratejik bilgi savaşı konseptini uygulamaya sokmaktadırlar.

Son olarak, bilgi savaşının saldırı ve savunmaya yönelik olarak gerçekleştirilen iki amacı, geleneksel savaşın da doğasında bulunan bir yöntemdir. Ancak, bilgi teknolojilerinin ilerlemesi ile birlikte, saldırıda bulunacak ve/veya savunmayı gerçekleştirecek müttefiklerin de bir gün gelip düşman olabileceği ihtimali unutulmamalı ve bu vesile ile bilgi savaşı için gerçekleştirilen stratejik ortaklıklar sınırlı tutularak ülkenin ulusal güvenliğini tehdit edici yönde olmamasına özen gösterilmelidir. Bir diğer husus ise, gerek hücum edecek, gerekse savunmayı gerçekleştirecek ülkelerin istihbarat ve casusluk operasyonları da hızla gelişen bilgi teknolojilerine ayak uyduracak şekilde plânlanmalıdır. 21. yüzyılın, bilgi teknolojileri çağı olduğu düşünülürse, gelişmekte olan ülkelerin tıpkı gelişmiş ülkelerde olduğu gibi gelecekteki "savunma amaçlı bilgi teknolojilerine" ayıracakları pay, bu yöndeki hedefleri gerçekleştirebilir nitelikte olmalıdır.