

Bilgi Savaşı: Bilgi Tabanlı Teknolojilerin atılma Boyutuna Kavramsal Bir Erişim

Mustafa SAĞSAN*

Bu makale, "bilgi savaşı" kavramını teorik bir bakış açısıyla incelemekte ve bilgi bilimi çerçevesinde; bilginin önce veri, sonra enformasyon ve son olarak da bilgi aşamasından geçerek oluştuğunu anlatmaktadır. Bilgi savaşını, bugüne kadar yapılan açıklamalardan farklı olarak bilgi bilimi açısından değerlendirmekte ve söz konusu savaş, bilgi sistemleri, bilgi kaynakları ve bilgi hizmetlerine dayalı olarak teorik bir çerçeveye oturtmaktadır. Bilgi savaşının kapsadığı net savaş ve siber savaş terimlerini açıklayarak, aralarındaki farkı izah etmeye çalışan makale, bilgi savaşının çeşitlerini ve oluşturduğu tehditleri sıralayarak devam etmektedir. Araştırma, değişen teknolojik şartların da artarak bilgi savaşının kabul görmesiyle gelişmiş ve gelişmekte olan ülkelerin hangi pozisyonda yer alması gerektiğinden söz ederek sonuçlandırılmıştır.



This article theoretically examines the information warfare concept. It also explains that the knowledge in the information science is developed by a specific way whom elaborate data, information and knowledge. Also, in this study, information warfare is considered in the information science perspective and put this warfare in a theoretical framework relating to information systems, information sources and information services. The article, which aims to explain the difference between netwar and cyberwar by studying these concept, also explains threats and kinds of information warfare. This study concludes that how developed and developing countries determine their own positions against the information warfare.

105

Giriş

1970'lerin sonu, 1980'lerin başından itibaren bilgi-merkezli hareketler, sanayileşmenin de önüne geçerek sanayi toplumlarını iletişim toplumu haline 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 yeni ekonomi, teknoloji, iletişim ve askeri stratejiler şeklinde sıralayabiliriz. Özellikle askeri 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 kul-

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

lanılan bu terim, günümüzde genelde bilgi teknolojisi ağırlıklı olmasından ötürü bilgi bilimcileri ve içeriğinde bir savaş teknolojisinin kullanılması sebebiyle de askeri stratejistleri ve uluslararası ilişkiler üzerine çalışan uzmanları ilgilendirmektedir. Nitekim Richard E. Hayes ve Gary Wheatley "Information Warfare and Deterrence" adlı makalelerinde 'bilgi savaşı' teriminin birçok anlamda kullanıldığını ve genellikle askeri bilimlerden ziyade siber savaş alanı içerisindeki bilgisayar ve iletişim altyapısı disiplini üzerinde odaklandığını ifade etmektedirler.¹

Okuyacağınız bu makalede, enformasyon bilimci gözüyle "bilgi savaşı" kavramı değerlendirmeye çalışılacak ve konu ile ilgili teorik boyutta açıklamalarda bulunulacaktır. Çünkü, bilgi savaşının askeri bir boyutu olduğu halde, genelde teknoloji hizmetlerinin enformasyonla birleşmesi ve daha çok karşı tarafın bilgi sistemlerini 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. Genelde birçok alanda kullanılmasına rağmen, enformasyon bilimciler bilgiyi, "üzerinde kesin bir yargıya varılmış, anlam kazanmış her türlü ses, görüntü ve yazılara verilen isim"³ 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, "bilgi yaymak, iletmek, göstermek ve yedeklemek için gerekli makine ve ekipmanı kullanarak oluşturulmuş altyapı, organizasyon ve işlemci"⁴ olarak ifade edilebilir. Bilgi bilimini, epistemoloji, mantık, bilgi teorisi, karar teorisi, semiyotik (göstergebilim) teorisi ve bilgi yönetimi disip-

¹ Richard E. Hayes ve Gary Wheatley "Information Warfare and Deterrence", National Defence University, Sayı: 87, Ekim 1996, s. 2.

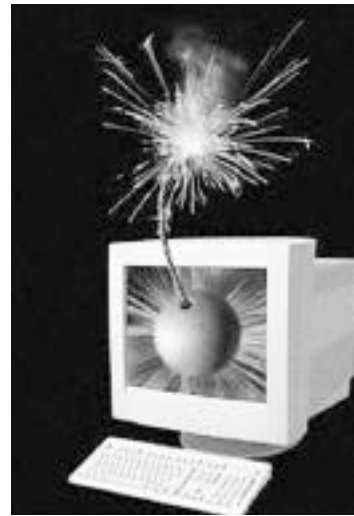
² Chris Mader, *Information System: Technology, Economics, Applications*, Chicago, Science Research Associates Inc., 1974, s. 3

³ Uğur Yozgat, *Yönetim Bilişim Sistemleri*, İstanbul, Beta yayıncılık, 1998, s. 45.

⁴ Forsnet Bilgi Teknolojileri Web Sayfası'ndan alınmıştır. <http://www.sanalteror.gen.tr/bilgi/index.html>

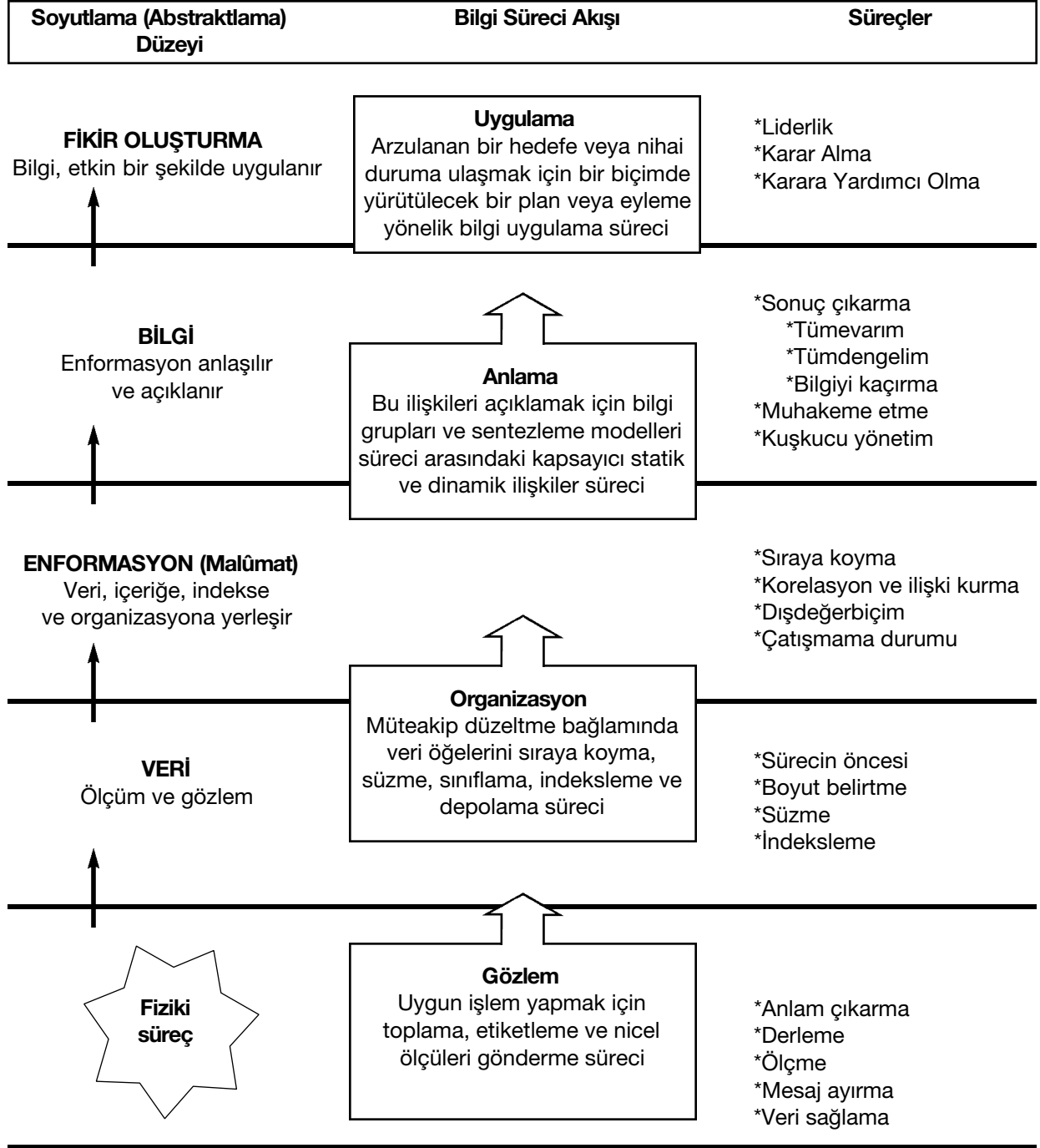
►► **Herhangi bir savaş sırasında iletilip alınan şeyin veri mi, enformasyon mu yoksa bilgi mi olduğunun bilinmesi ve ona göre tedbir alınması gerekir.** ◀◀

linleri içerisinde açıklamak gerekir.⁵ 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*) haline 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 ulaşamaz, ulaşılsa bile hangi veri/enformasyon/bilginin doğru hangisinin yanlış olduğu, bu istihbarata dayanarak neyin gerçekleşip gerçekleşmediği anlaşılabilir ve böylelikle yapılan bilgi savaşı olumsuz sonuçlanır. Bilgi hiyerarşisi bilgiyi üç düzeyde tanımlamaktadır. Bunlar, veri, enformasyon ve bilgidir. Şekil-1⁶ bu ilişkiyi detaylı olarak açıklamaktadır.



⁵ Edward Walz, *Information Warfare: Principles and Operations*, London, Artech House, 1998, s.56.

⁶ Walz, *Information Warfare ...* s. 51.



Şekil-1. Bilgi hiyerarşisi.

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 anlamda ekonomi, pazar, rekabetçilik ve stratejik planlar uygulamaya yönelik olarak yapılan hazırlık-

lar ise **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 askeri trafiğin çok önemli bir kısmının ülkenin ulusal altyapı sistemlerine yönelik olarak taşınması, kamu ve özel sektörlerin ağırlıklı bilgi tabanlı teknolojiler konusunda üretimde bulunmalarına neden olmuş ve geleneksel savaş yüzünü bilgi ve iletişim teknolojilerine dayalı olarak 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.

Halen 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”⁷ olarak tanımlanmaktadır. Ulusal güç ise, diplomasi, ekonomik rekabet, askeri gücün kullanılması ile ulusal kaynaklardan bu yönde istifade edilmesi anlamına gelmektedir. Bilgi savaşlarında en güçlü silah, bilgi/enformasyon ve dezenformasyondur ve bunlar savaşın biçimini tayin etmektedir. Bilgi savaşında önemli husus, bir ülkenin kendi bilgi altyapısını koruyarak düşman birliklerinin bilgi sistemlerini imhaya yönelik olarak eylemlerde bulunmaktır.

Bilgi savaşı daha ziyade ileri teknolojiye sahip askeri silahlar ile yapılan savaş olarak algılanmış olsa da, aslında karşı tarafa ait bilgi merkezli işlemleri, bilgi sistemlerini ve bilgi tabanlı ağ yapılarını etkileyecek bir hareket gerçekleştirmek için oluşturulan ve savunma sistemleri ile yapılan savaştır. “Düşman birliklerinin askeri, siyasi, sosyal ve ekonomik altyapılarını çöktürmek için düşmanın bilgi tabanlı faaliyetlerine saldırılar gerçekleştirerek düşmanın gücünü ve zayıf noktalarını nispeten anlamaya çalışacak faaliyetlerde bulunmak”⁸ olarak da anlatılmaktadır.

►► **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.** ◀◀

Bilgi savaşlarının devletler için ne denli önemli olduğunu aşağıdaki örnek açıkça anlatmaktadır. Körfez Savaşı, bilgi savaşının beşikteki dönemi olarak adlandırılabilir. Bu savaşta yeni nesil silahların kullanılması ve 1990’larda gerçekleşen Balkan operasyonları bilgi sistemlerinde geçtiğimiz 10 yılda ciddi 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.

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”⁹ 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”¹⁰ olarak izah edilebilir. Bilgi savaşı, bilgi operasyonları bağlamında şu şekilde değerlendirilebilir:

“Düşman olarak hedeflediğimiz kitleye belirli amaçları gerçekleştirmek veya savaşı kazanmak

⁷ George J. Stein, “Information Warfare”, *Airpower Journal*, İll-bahar, 1995, s. 9.

⁸ George J. Stein, *Information Attack: Information Warfare in 2025*, Washington, 11 Aralık 1996, s. 4.

⁹ USAF, “Cornerstones of Information Warfare”, United States Air Force, 1995, s. 6. <http://www.af.mil/lib/corner.html>

¹⁰ Manuel W. Wik, “Information Warfare and Information Operations”, *Militarteknisk Tidskrift*, http://www.verkstader-na.se/mtt/pdf/100_4.pdf

için kriz veya çatışma zamanlarında bilgi operasyonlarının idare edilmesi, yönetilmesi"¹¹ 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 savaşı şu şekilde de değerlendirilmelidir: Bilgi/enformasyon bilimi kapsamında, enformasyon altyapısının içeriğini oluşturan üç adet kavram bulunmaktadır. Bunlar, bilgi kaynakları, bilgi sistemleri ve bilgi hizmetleridir.¹² Bilgi savaşı ile ilgili olarak yukarıdaki açıklamalardan da anlaşılacağı üzere, bu kavram sadece bilgi sistemleri çerçevesinde ele alınmış ve buna dayanarak bilgi saldırısı ve sonrasında bilgi operasyonu/harekâtı olarak nitelenen düzeyler gerçekleştirilmiştir. Aslında bilgi sistemi, bilgi savaşına başlamadan önce ülkelerin altyapılarını 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 yapma' aşaması bulunmaktadır. Bilgi savaşına başlamadan önce karşı tarafın pozisyonunu anlamak, mevcut güç kapasitesini öğrenmek ve gelebilecek saldırıların coğrafi olarak yerini tespit etmek, vs. için bilgi altyapısının ikinci aşaması olan bilgi kaynaklarını kullanmak gelmektedir. Saldırısı yapacak veya saldırıya uğrayacak olan ülkenin mevcut bilgi kaynaklarını kullanarak bilgi elde etme işi, bilgi kaynakları kısmında yer almaktadır.

Bilgi altyapısının son aşaması olan bilgi hizmetleri¹³ 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/hare-

kâtı gerçekleşir. Bilgi savaşı konusu ile ilgili literatür, bu terimi tanımlarken bilgi savaşı için bir ön şart olan bilgi altyapısını (yani bilgi sistemleri, bilgi kaynakları ve bilgi hizmetleri) gözden kaçırmaktadırlar.

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*"¹⁴ 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, siyasi ve kültürel yıkım, düşman birliklerin yerel medyalarında parazitlik yapma ve aldatma, bilgisayar ağları ve veritabanlarının süzülmesi, bilgisayar ağları karşısında muhalif birliklerin ilerlemesini engellemek gibi faaliyetleri içermektedir.¹⁵ Yani rakibin algılamasını engelleyip onu savaştan caydırmak ve bilgisayar ağ-

►► **Bilgi savaşı konusu ile ilgili literatür, bu terimi tanımlarken bilgi savaşı için bir ön şart olan bilgi altyapısını (yani bilgi sistemleri, bilgi kaynakları ve bilgi hizmetleri) gözden kaçırmaktadırlar.** ◀◀

¹¹ "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/IWdef.htm>

¹² Mustafa Sağsan, "Akıllı Toplu' Olma Yolunda Ulusal Bilgi Stratejisi ve Bilgi Ortaklığı", *Stratejik Analiz*, Sayı: 18, 2001, ss. 88-89.

¹³ Bilgi Hizmetleri: Bilginin sağlanması, düzenlenmesi ve

¹⁴ 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/>

¹⁵ 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

ları aracılığı ile gerçekleştirdiği eylemleri engellemek amacı ile yapılmaktadır.

Siber Savaş ise, bilgi ile ilişkili ilkelere göre askeri 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 saptamak gibi taktik iletişimlerini belirlemek ve akıllı silah sistemleri gibi farklı teknolojileri içermektedir. Siber savaşın mahiyetinde, düşmanın bilgi ve iletişim devreleri içerisine zorla veya izinsiz olarak girerek dezenformasyonun yayılmasını elektronik olarak çöktürmek vardır.¹⁶ 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 amacı ile 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 altyapılarını bozguna uğratmıştır. Böylelikle, her devlet kendi teknoloji üstünlüğünü kullanarak karşı tarafla çatışma içerisine girmeye başlamıştır. Bu teknolojik üstünlük sağlama çatışması ise, doğrudan doğruya uluslararası sistemleri, ticari 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 hukuki düzenleme yoktur. Uluslararası anlaş-

►► **Yüksek düzeydeki bilgi teknolojileri, bir yandan bilgi sistemlerinin bütünlüğünün bozulmasını sağlarken, diğer yandan da karşı güçlerin devlet altyapılarını bozguna uğratmıştır.** ◀◀

maların olmaması onu daha da etkili hale getirmektedir.

- Bu alanda uluslararası anlaşmaların yokluğu ortaya bir üçüncü tehdit unsurunun çıkmasına neden olabilir: Algılanamayan duyguların; menfaat ve tercihleri etkileyebilecek, yönlendirecek yeni teknolojilerin ortaya çıkması.
- Dördüncü tehdidi enformasyon savaşında saldırıların gelişme hızı, kriz yönetimi sürecine izin vermemektedir.
- Beşinci tehdit ise eskiden herkese açık olmayan enformasyonun artık hemen herkes için neredeyse açık olmasıdır.¹⁷

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 uluslararası hukuk çerçevesinde düzenlenmesi gerekli 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

¹⁶ Arquilla, Ronfeldt, "Cyberwar and Netwar..."

¹⁷ Timothy L. Thomas, "Deterring Information Warfare: A New Strategic Challenge", *Parameters*, Cilt 24 (4), 1996, ss. 3-4.

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 7 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.¹⁸

ABD Hava Kuvvetleri'ne 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.Askeri Aldatma
- 3.Güvenlik Tedbirleri
- 4.Fiziki Yıkım
- 5.Bilgi Saldırısı
- 6.Elektronik Savaş.¹⁹

Son olarak, Edward Walz,²⁰ bilgi savaşlarının çeşitlerini bilgi operasyonları başlığı içerisinde yerleştirmiş ve şu şekilde bir sınıflandırma yapmıştır:

- 1.Psikolojik Operasyonlar
- 2.Operasyonel Aldatma
- 3.Elektronik Operasyonlar

4. Fiziki 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.²¹

- **Komuta Kontrol Savaşı:** (C2W): Düşmanın iletişim sistemini ve orduların sevk ve komutasını engellemek için yapılan saldırılardan oluşur.
- **İstihbarat Merkezli Savaş:** Tarayıcıların, işlemcilerin ve keşif belirleme ve zarar tespit sistemine entegrasyonunu gerçekleştirmekle kullanılmasıdır.
- **Elektronik Savaş:** Hedef birliğin elektron ve enformasyon akışını kesmek, bozmak veya müdahale 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, askeri ve sivil olarak bilgi sistemlerini tahrip etmek, bozmak, sömürmek veya uyumlulaştırmak için kötü yazılım tekniklerini kullanmak (yani virüs programları üretmek) vardır.
- **Ekonomik Bilgi Savaşı:** Bilgi ticaretinin gerçekleşmesi için bilgi ekonomilerine karşı yapılan savaştır. Devlet politikasının bir aracı

¹⁸ Martin C. Libicki, "What is Information Warfare", National Defence University, 28 Mayıs 1995, s. 1.

¹⁹ USAF, "Cornerstones of Information Warfare", United States Air Force, s.4. <http://www.af.mil/lib/corner.html>

²⁰ Edward Walz, *Information Warfare: Principles and Operations*, London, Artech House, 1998.

²¹ 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>

