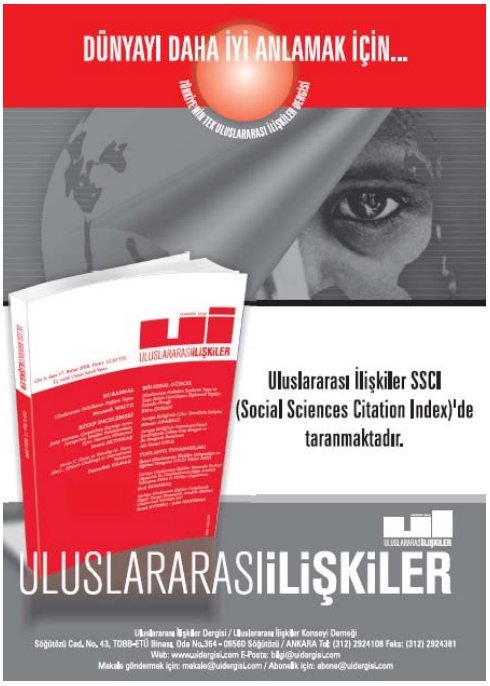
ULUSLARARASI İLİŞKİLER
Akademik Dergi

Yayın ilkeleri, izinler ve abonelik hakkında ayrıntılı bilgi:
E-mail: bilgi@uidergisi.com
Web: www.uidergisi.com



Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu

Salih BIÇAKCI

Doç. Dr., Işık Üniversitesi, Uluslararası İlişkiler Bölümü

Bu makaleye atıf için: Bıçakcı, Salih, "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", *Uluslararası İlişkiler*, Cilt 9, Sayı 34 (Yaz 2012), s. 205-226.

Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu

Salih BIÇAKCI*

ÖZET

Soğuk Savaşın bitişinden sonra uluslararası sistemin güvenlik dinamikleri değişti. Soğuk Savaş tehditlerinin ortadan kalkmasıyla birlikte Kuzey Atlantik Paktı Örgütü (NATO) yeni durumun gereklerine göre yeniden yapılanmak zorunda kaldı. Bu makale NATO'ya karşı siber tehditlerin ortaya çıkışını ve onun bu yeni güvenlik ortamına nasıl tepki vereceğini incelemektedir. Soğuk Savaş sonrasındaki dönemde, geleneksel savaş taktikleri savaş meydanının gereklerini yerine getirmekte yetersiz kalıyordu. Asimetrik savaş diğer yöntemlere göre daha öne çıktı. Kosova çatışması sırasında, NATO bombalamasına Sırp bilgisayar korsanları tarafından siber saldırılarla karşılık verilmiştir. Farklı durumlarda da benzer eğilimler görülmüştür. NATO yeni bir siber savunma stratejisi inşa etmeye ve uluslararası sistemdeki güncel tehditleri de kapsayacak bir strateji oluşturmaya başladı. Lizbon Zirvesinde siber savunma ve kritik bilgi altyapısının korunmasını da içeren yeni stratejinin hazırlanmasına onay verildi. NATO, siber savunmayı içeren hibrit savaş stratejisini başlattı ve bu yaklaşımı bütün üyelerinde uygulamaya başladı.

Anahtar Kelimeler: NATO, Siber Güvenlik, Bilgisayar Korsanlığı, Kritik Bilgi Altyapısı, Estonya, Siber Tehdit, Uluslararası Güvenlik, Hibrit Savaş

The Rebirth of NATO between New War and Cyber Security

ABSTRACT

After the end of Cold War, the security dynamics of the international system has changed. With the demise of the Cold War threats, North Atlantic Treaty Organization (NATO) has compelled to reorganize its structure to the requirements of new condition. This article examines the emergence of cyber threat against the NATO and how it responds to the new security environment. In the post-Cold War period, the conventional warfare tactics were not enough to fulfill the requirements of the battlefield. The asymmetrical warfare becomes eminent among the other methods. During the Kosovo conflict, the NATO bombing was retaliated by Serbian Hackers with the cyber attack. Similar tendencies also observed in different situations. NATO started to build a cyber defense strategy and tried to create a strategy which encompasses recent threats of the international system. The Lisbon summit endorsed the preparation of new strategy that includes cyber defense and protection of the critical information infrastructure. NATO initiated hybrid warfare strategy combining cyber defense and tries to implement this new approach to all its members.

Keywords: NATO, Cyber Security, Hacking, Critical Information Infrastructure, Estonia, Cyber Threat, International Security, Hybrid War

* Doç. Dr., Uluslararası İlişkiler Bölümü, İİBF, Işık Üniversitesi, İstanbul.
E-posta: asbicakci@isikun.edu.tr

İkinci Dünya Savaşı'nın sona ermesinin ardından Soğuk Savaş döneminin başlamasıyla birlikte yeni bir güvenlik rejimi ortaya çıktı. Ken Booth, iki kutuplu dünyanın güvenlik algısını "Hepimizin kafasında demir bir perde vardı" şeklinde tanımlar.[1] Sıcak savaştan uzak kalınan bu dönemde, tedirginlik ve tansiyon hep yüksekti. 1989 yılında Berlin duvarının yıkılması sonrasında, 25 Aralık 1991'de Sovyetler Birliği'nin dağılmasıyla birlikte, uluslararası sistem için gerilimli bu iki kutuplu dönem yavaş yavaş sona erdi.

Soğuk Savaş'ın sona ermesiyle birlikte, NATO üyeleri kendilerini bu mücadeleden galip çıkmış, diğer tarafı yenilmiş olarak tanımladılar. Yeni döneme galip gelen gücün gölgesinde başlanıldı. Bu güçlülük durumu aynı zamanda bir muhafazakârlığı da beraberinde getirmektedir. Güç müdahalelerinde galip gelenlerin durumlarını korumak eğilimleri vardır. Bu tutum, yeniliklere karşı biraz korkuyla yaklaşılmasına sebep olur. Bu dönemdeki genel kanı NATO'nun yavaş yavaş daha az görünür olacağı ve zamanla kaybolup gideceği yönündeydi.[2] Varoluş sebebi olan tehditler ve düşmanlar ne de olsa ortadan kalkmıştı. Tehditlerin ortadan kalkmasıyla güvenli bir sistemin oluşması bekleniyordu. Bu durumda güvenliğin sağlanması amacıyla kurulmuş olan uluslararası güvenlik ittifaklarının varlığının da fiili olarak (*de facto*) anlamsız kalması gerekirdi. Bu düşüncelerin geliştiği bir ortamda, ortak tehdidin yokluğu ortak hareket kabiliyetinin geliştirilmesi fikrini de kısıtlamaktaydı.[3] Bütün bu tartışmaların gölgesinde Soğuk Savaş döneminin güvenlik yapılanması başlıca ürünü olan NATO kendisini yeniden tanımlamaya ve yapılandırmaya, bölgesel oluşumlara uyum sağlayarak varlığını anlamlandırmanın yollarını aramaya başladı.

NATO'nun 1991 yılında yayınlanan stratejik belgesinin önemli bir kısmında ortadan kalkan tehditler yer almaktadır. NATO bu belgede, birbiri ardına gelen çözülmeler nedeniyle tehditlerin ortadan kalkışının yarattığı güvenlik ortamının sürdürülmesi konusundaki kararlılığını ortaya koymaktaydı.[4] Soğuk Savaş sonrası dönemin bu ilk toplantısında NATO için güvenlik öncelikleri karşılıklı diyalogun sağlanması, işbirliği ve ortak güvenlik olarak belirlemiştir. Yeni politik yapılanmaların oluşması sürecinde, Soğuk Savaş'ın dondurduğu anlaşmazlıkların/çatışmaların yeniden ortaya çıkması ihtimali üzerinde de ayrıca durulmaktaydı. Aynı zamanda yeni çatışmaların belirmesi de muhtemeldi. Bu nedenle, kriz yönetimi ve çatışmaların önlenmesi gibi konuların yeni dönemde NATO'nun varlığını anlamlandıracağı değerlendirilmekteydi. Diğer yandan, iki kutuplu uluslararası sistem yapısı etkisini kaybetmiş, buna bağlı olarak uluslararası güvenlik sadece askeri kökenli olmaktan çıkıp enerjiden ekonomiye, iklim değişiminden siber alana yönelik tehditler tartışılmaya başlanmıştır.[5]

---

1 Ken Booth (Der.), *Statecraft and Security: The Cold War and Beyond*, Cambridge University Press, Cambridge, 1998, s.1.

2 Robert B. McCalla, "NATO's Persistence after the Cold War. (North Atlantic Treaty Organization)", *International Organization,* Cilt 50, No.3, Yaz 1996, s.445–475.

3 John S. Duffield, "NATO's Functions after the Cold War" *Political Science Quarterly*, Cilt 109, No.5, Kış 1994–1995, s.764.

4 "The Alliance's New Strategic Concept 07 Nov. 1991–08 Nov. 1991", http://www.nato.int/cps/en/natolive/official_texts_23847.htm (Erişim Tarihi 3 Aralık 2011).

5 Daha detaylı bir yaklaşım için bakınız; Barry Buzan, "Rethinking Security After the Cold War", *Cooperation and Conflict,* Cilt 32, No 1, 1997, s.5–28.

Bu dönemde, gelişmeleri değerlendiren birçok araştırmacı, Soğuk Savaş sonrası dönemdeki gelişmeleri ve yapısal değişiklikleri tanımlamada "yeni" ifadesini rahatlıkla kullanmaktaydı.[6] Yeni olarak tanımlanan gelişme ve değişimleri, tarihsel sürece bakmaksızın "yeni" olarak tanımlayan bu yaklaşım ontolojik problemlere neden oldu. Yenileşme sadece isimlerin yeniliğinden öteye gitmedi. Araştırmacılar için "yeni" kavramı, genellikle bahsedilen konunun gündelik düzleminde problemleri analiz etmek için kullanılan bir araçtır. Hâlbuki yeni olarak ortaya konan birçok temel kavram esasında tarihin ve uluslararası sistemin geçmiş zamanlarında ortaya çıkmış ve "yenilenmeden" önce birçok değişim geçirmiştir. Yakından incelendiğinde, aslında yeni olarak tarif edilen uluslararası sistem, devlet, devlet-altı aktörler, savaş, barış ve milli güvenlik gibi birçok kavramın (eğer hepsi değilse) dönüşümlerinin eski dönemde inşa edildikleri dinamikler üzerinden işlemeye devam ettiği görülecektir.[7] Bu olguların esas nitelikleri varlığını korumuşlardır. Kısacası bir tür devamlılık söz konusudur. Ne var ki, devamlılığı vurgularken olayların gelişme hızını etkileyen unsurların varlığını da inkâr edemeyiz.

Yeni Oyunlar ve Yeni Kurallar

1991 sonrasında sivilleşen ve dünyanın kullanımına açılan internet uluslararası sistemin aktörleri olan devlet, toplum ve bireyleri birbirlerine daha etkin şekilde bağlamıştır. Bu noktada, internetin uluslararası sistemdeki olayların katalizörü olduğunu söylemek abartılı olmayacaktır. İnternet, zihinlerdeki Soğuk Savaş tansiyonunun düşmesinde ve farklı kamplardaki insanların arasındaki perdelerin ortadan kalkmasında önemli bir rol oynadı. 1991 Körfez Savaşı'nın detaylarının internet ve medya üzerinden canlı biçimde takip edilmesi yeni dönemin farklı olacağının en büyük göstergesiydi. Körfez Savaşı'nın bir "iletişim savaşı" olduğunun iddia edilmesi bu nedenledir.[8] Körfez Savaşı sonrasındaki döneme odaklanarak sunulan diğer bir yaklaşım da Mary Kaldor'un ileri sürdüğü "Yeni Savaş" kavramıydı. Kaldor iletişim araçlarının yaygınlaşmasıyla küçülen dünyamızda sığınmacı akımlarının, sistemik tecavüzlerin ve ulus ötesi (transnational) suç örgütlerinin savaş ortamında görülmeye başlamasını yeni bir savaş tipi olarak kavramsallaştırdı. İnsanlık tarihi boyunca "küresel bağlanmışlık" (interconnectedness) internetin sağladığı yoğunluğa hiç ulaşmamıştı.[9] Bu yüzden Yeni Savaş, Kaldor'un küreselleşme üzerinden formüle ettiği şekliyle anlaşılabilir bir olgudur. Fakat savaşın dinamikleri, şiddet bağlamında Clausewitz'in ölçütleri açısından herhangi bir değişim göstermemektedir. Kaldor iletişim teknolojisinin

---

6 Soğuk Savaş sonrasındaki yeni güvenlik, yeni dünya düzeni, yeni savaş gibi kavramların çokça üretildiğini ve kullanıldığını görüyoruz. Ancak bu kavramların ne kadar "yeni" olduğu da tartışılmaktadır; daha detaylı bir yaklaşım için Ken Booth, "Security and Emancipation", *Review of International Studies*, Cilt 17, No.4, 1991, s.314–315. Yeni ve eski kavramları üzerine sürdürülen tartışmanın bir benzeri de terörizm için yapılmaktadır. Detaylı bilgi için bkz. Thomas Copeland, "Is the 'New Terrorism' Really New?: An Analysis of the New Paradigm for Terrorism", *The Journal of Conflict Studies*, Cilt 21, No.2, Kış 2001, s.7-27; Isabelle Duyvesteyn, "How New is the New Terrorism?", *Studies in Conflict & Terrorism*, Cilt 27, No.5, 2004, s.439-454.

7 Yeni Savaş kavramına kritik bir yaklaşım için bkz. Ken Booth, "New Wars for Old", *Civil Wars*, Cilt 4, No.2, 2001, s.163–170.

8 A. Mattelart, *Mapping World Communication: War, Progress, Culture*. Minneapolis, University of Minnesota, 1994, s.117.

9 Mary Kaldor, *New and Old Wars: Organized Violence in a Global Era*, Cambridge, Polity Press, 1998, s.3.

genişlemesi ile değişen ve farklılaşan geleneksel savaş kavramını birleştiriyordu. Kaldor'un bu tanımlama çabası bile siber alanı ve iletişim teknolojisini ayrı bir savaş alanı olarak tanımlanmıyordu.

Savaş kavramının çatışmadan hemen önceki teknik kısmını organizasyon ve hazırlık oluşturmaktadır. Organizasyonu sağlayan teknik donanımın gelişmesi ve kolay kullanılır hale gelmesiyle birlikte savaşan tarafların organizasyon kabiliyetleri geçmiş dönemlere göre daha gelişmiştir. Ağ teknolojileri (ya da İnternet) ordu içindeki iletişimin hızlı ve eskisine göre daha nitelikli yapılmasını sağlamıştır. Soğuk Savaş sonrasındaki ilk sıcak savaşta (Irak Savaşı) karşılaştığımız en şaşırtıcı sahne, kaynağını göremediğimiz bir yerden gelen füzelerin "düşman" olarak belirlenen noktayı vurmasıydı. Savaşan orduların ya da insanların fiziksel karşılaşması uzunca bir süre görülemedi. Televizyon ekranlarından seyredilenlerin dünyanın bir noktasında yapılan çatışmadan bir sahne mi yoksa bilgisayar oyunun ekran görüntüsü mü olduğunun anlaşılması kolay olmadı. Açıkçası sanallaşan (virtuous war) bir savaş kavramının olgunlaştığını görmemiz de zaman aldı.[10] Der Derian'ın dediği gibi "taklit (imitasyon) ve simülasyona ait yeni teknolojilerinin yanı sıra izleme yetenekleri ve hız; gerçek ve sanal savaş arasındaki alanı (gap), coğrafi mesafeleri ve kronolojik süreyi kısalttı (collapse)".[11] Artık savunma sanayi teknolojileri sayesinde savaşın niteliği ve tanımı değişmeye başlamıştır.

Soğuk Savaş'ın bitmesiyle birlikte hızla genişleyen pazar ekonomisi, siyasi değişimleri körükleyerek hızlandırdı ve şekillendirdi. Savunma için ayrılan bütçeler azalmaya başladı.[12] Aslında değişen teknolojinin artışına paralel biçimde azalan asker ihtiyacıydı. Bugün de devam eden bu değişim sürecinde, geleneksel savaş metodu terk edilerek farklı savunma (ya da saldırı) stratejilerini yöntemleri bir arada kullanabilen ve aynı anda düzenli/düzensiz savaş icra edebilme kabiliyetine sahip olan stratejilere doğru ilerlenmektedir. Orduların sayısal büyüklükleri azalırken vuruş güçleri ve müdahale hızları artmaktadır. Değerlendirmeye alınması gereken diğer bir unsur da, bu dönemde savaş alanının ve yenen/yenilen kavramları arasındaki belirsizliğin nispeten artıyor olmasıdır. Öte yandan, internetin sivilleşmesiyle birlikte bütün çatışmalar ya da şiddet eylemleri dünyanın neresinde olursa olsun daha hızlı ve ayrıntılı bir biçimde duyulur hale gelmiştir. Çatışmaların sebep olduğu şiddet duygusu ya da (ve mesajı) internet üzerinden paylaşılmaya başlanınca etkinliği ve bilinirliği daha arttırmıştır. Böylece savaşların temelinde yer alan güç kavramı, medya unsurları sayesinde olduğundan daha büyük bir halde etkisini yaymaya devam etmektedir.

İletişimin hızlandığı ve yaygınlaştığı bu dönemde NATO'nun kuruluş dönemi aktörlerinin yanı sıra algılanan tehdidin yapısı da değişime uğramaktaydı. 1991 yılında belirlenen stratejik hedeflere bakıldığında, NATO'nun nasıl bir ortam ve tehdit algısı ile karşı karşıya kalacağı konusunda bir belirsizlik yaşandığı görülmektedir. Belgede ifade

---

10 James Der Derian, "Virtuous War/Virtual Theory", *International Affairs*, Cilt 76, No.4, Ekim 2000, s.771–788.

11 İbid.

12 Savunma bütçeleri Soğuk Savaş sonrasında 11 Eylül olaylarına kadar düşüş trendi izlemiştir; *SIPRI Military Expenditure Database 2011*, http://milexdata.sipri.org (Erişim Tarihi 23 Ocak 2012). Ayrıca çok boyutlu bir yaklaşım için bakınız; Lawrence R. Klein *et.al.*(Der.), *Arms Reduction: Economic Implications in the Post-Cold War Era*, Tokyo, United National University Press, 1995.

edildiği gibi "ittifakın başlıca endişesi olan büyük, yekpare ve potansiyel açıdan var olan tehdit ortadan kalkmıştı."[13] Yaşanan gelişmeler, bir anda ortaya çıkan etnik çatışmalar, sınır anlaşmazlıkları, organize suç örgütleri ile değişen savaş yöntemi ve araçları Soğuk Savaş döneminin dinamiklerine cevap vermek üzere kurgulanmış olan NATO'nun değişen güvenlik ortamının ihtiyaçlarına cevap verip veremeyeceği tartışmasının doğmasına neden oldu. Bu NATO'nun dönüşümü sürecine işaret etmektedir. Aksi bir durum, NATO'nun fiziki varlığını sürdürse bile işlevsel olarak anlamsızlaşması demekti.

Soğuk Savaş sonrası dönemde ortaya çıkan çatışmalarda görülen en önemli değişim güvenliğin asimetrikleşmesindeki artıştı.[14] Savaş tarihinde daha önce de görülen asimetrik savaş örneklerinin sayısı, Soğuk Savaş'ın bitiminden sonra daha da artmıştır. Özellikle internetin sivilleşmesinden sonra ortaya çıkan siber uzayın oluşturduğu yeni alan, asimetrik mücadeleyi teşvik eden bir alandır. Bilgisayar sahibi olan her birey çatışmalara tuttuğu tarafın lehinde ve çok çabuk bir biçimde dâhil olmaya başlamıştır. Birçok olayda bilgisayar sahibinin müdahalesi olmaksızın bilgisayarının kullanıldığı durumlar dahi söz konusudur.

İnternetin ve bilişim teknolojilerin hayatımıza girmeye başladığı bu dönemde, Rus birlikleri anayasayı uygulamak ve Rusya'nın toprak bütünlüğünü sağlamak için Aralık 1994'te Çeçenistan'ın başkenti Grozni'ye girdiler. Ağır silahlara sahip olan Rus birlikleri Çeçen direnişinin kısa süreceği zannediyordu. Ancak sahadaki gerçekler beklentilerle uyuşmadı. Silahlı çatışma, Soğuk Savaş sonrasında ilk defa internet ortamına yansıdı. Çeçenler başta internet olmak üzere bütün medya imkânlarını kullanarak, bilgi savaşının (information war) ilk örneklerini verdi.[15] En basitinden, Çeçenlerin internete yükledikleri ölü Rus askerlerin resimlerini gören anneler, çocuklarını kurtarmak için harekete geçtiler.[16] Ruslar geleneksel savaşın dışında oluşan bu siber alanın etkisini anlamak geciktiler ise de bir süre sonra saldırılara karşı başka siteler açarak cevap verdiler. Siber alanda gerçekleşen ilk soğuk mücadele günümüzde gerçekleşen siber savaşların öncülüğünü yaptı.

Fiber Ağlarda Savaşmak

Siber dünyanın ilk defa bir çatışmayla karşılaşması NATO için çok özel bir örnek oluşturdu. İnternetin Rus-Çeçen çatışmasındaki kullanımı, psikolojik harekât taktiklerine alan açmış oldu. İnternetin iletişimden bilgi paylaşımına kadar birçok sahada etkin olması, onu sadece bir medya aracı olmaktan çıkarıp aynı zamanda rakibe saldırılacak ve alt yapı sistemlerine zarar verilecek bir alan haline getirdi. Bu bakış açısıyla, Rus-Çeçen savaşında hem fiziki hem de sanal ortamda yaşanan mücadeleyi açıklamak için sadece

[13] "The Alliance's New Strategic Concept".

[14] T.V. Psul, *Asymmetric Conflicts: War Initiation by Weaker Powers*, Cambridge, Cambridge University Press, 1994; Rumu Sarkar, *A Fearful Symmetry: The New Soldier in the age of Asymmetric Conflict*, California, Praeger, 2010.

[15] İlk internet propaganda savaşı şu siteler üzerinden gerçekleşti: http://www.qoqaz.net, http://www.kavkaz.org, http://chechenpress.com, http://www.infocentre.ru.

[16] Brian S. Petit, "Chechen Use of the Internet in the Russo-Chechen Conflict", Yayınlanmamış Yüksek Lisans Tezi, the U.S. Army Command and General Staff College Fort Leavenworth, Kansas, 2003.

"Yeni Savaş" kavramını kullanmak yeterli olmayacaktır. Elektronik savaşın tekniklerinden daha fazlasına ihtiyaç duyulan, geleneksel savaşla birlikte de sürdürülen bu kombine savaş tarzına "Hibrit Savaş" demek daha yerinde olacaktır.[17] NATO da, Soğuk Savaş sonrasındaki güvenlik ortamının belirsizliği nedeniyle ve örneklerden çıkarılan dersleri ışığında geleneksel savaş imkânlarını bırakmadan yenilerine sahip olmanın doğru olacağını düşünerek hibrit yöntemi tercih edecektir. Nitekim takip eden dönemde NATO yetkililerinin ortaya çıkması muhtemel hibrit çatışmaların en önemli unsuru olan siber savaş kabiliyetini edinmek üzere toplantılar düzenlemeye ve gelişmelere hazırlanmaya başladıkları görülmektedir. İlk aşamada askeri komuta-kontrol ağları ve sistemi siber savaş kavramının gereklerine göre düzenlenmeye başladı. İlk yıllarda bu hazırlıklar sayısal olarak az olsa da zamanla siber savaş[18] üzerine yapılan çalışmalar sıklaşmıştır. NATO'nun 1998'de düzenlediği "Harekât Sistemlerine Enformasyon Teknolojilerinin Uygulanması" ve 1999'da düzenlediği "21. Yüzyılda NATO Enformasyon Sistemlerini Korumak" başlıklı toplantıları, NATO'nun yeni döneme uyum sağlama çabasının yansımaları olarak kabul edilebilir. NATO kendisini yeni döneme ve tehditlere karşı hazırlıklı olmaya çalışırken, korkulan (beklenmedik) siber saldırının aslında çok da uzakta olmadığını gösteren bir gelişmeyle karşı karşıya kaldı.

Dağılma sürecindeki Yugoslavya Federal Cumhuriyeti'ndeki etnik unsurlar arasındaki çatışma literatüre Kosova çatışması olarak kayıt edildi. 30 Ocak 1999 tarihinde NATO'nun yaptığı basın açıklamasında "Genel Sekreterin eski Yugoslavya'daki hedeflere hava saldırısı yapma yetkisine sahip olduğu" belirtildi.[19] 24 Mart 1999, saat 19.00'da (GMT) NATO Genel Sekreteri Javier Solana'nın direktifi doğrultusunda Sırp hedeflerinin bombalanmaya başlamasıyla birlikte NATO'ya yönelik ilk siber saldırılar başladı. 9 Nisan tarihinde Londra merkezli güvenlik firması Mi2g[20], Sırp bilgisayar korsanlarının (hacker) NATO'nun nispeten yeterli hazırlığı bulunan askeri komuta-kontrol ağına değil de üye ülkelerinin ekonomik alt yapılarına saldıracakları konusunda uyarı yaptı.[21] Kısa bir süre sonra NATO karargâhına ve üye ülkelerin askeri haberleşme sistemlerine yönelik siber saldırılar yapıldı. En çok kullanılan saldırı yöntemi, Dağıtık Servis Dışı Bırakma saldırısı (Distributed Denial of Service-DDoS) tekniğiyle sunucunun işlemcilerinin taleplere cevap veremez hale getirilmesiydi. NATO'nun uluslararası web sayfasıyla e-posta trafiğini barındıran yaklaşık 100 sunucusu hedef alındı. DDoS'un yanı sıra ping doygunluğu (saturation) saldırısı ve binlerce zararlı bilgisayar virüsünü içeren e-postalar da kullanıldı. Bütün bu saldırılara karşı konulabilmesi için NATO'nun kullandığı Sun Microsystem'in SPARC–20 sunucular daha hızlı veri işleme gücü olan Ultra-SPARC'larla değiştirildi.

---

17 Matthew Rusling, "Shifting Gears For the Military, a Future of 'Hybrid' Wars", *National Defense*, Eylül 2008, s.32–34.

18 NATO siber savaş kavramına ait çalışmalarında kurumsal duruşunu açık ifade edebilmek için "siber savunma" başlığını tercih etmiştir. Bu araştırmada siber savaş terimi savaş tipini açıklayabilmek için kullanılmıştır.

19 NATO, "Statement by the North Atlantic Council on Kosovo (Basın Açıklaması)", 30 Ocak 1999, http://www.nato.int/docu/pr/1999/p99-012e.htm (Erişim Tarihi 30 Ocak 2012).

20 http://www.mi2g.com/ (Erişim Tarihi 23 Ocak 2012).

21 "Serbian Cyber Attack may Spread", http://www.mail-archive.com/ctrl@listserv.aol.com/msg10035.html (Erişim Tarihi 12 Aralık 2011).

Pingler tarafından doldurulan 256K'lık bant genişliğini de T1 bağlantı[22] seviyesine yükseltilerek, gerekenin çok üstünde bir bant genişliği sağlandı.[23] Öte yandan Melissa, Papa virüsleri ve Happy 1999 makro virüsüyle gönderilmiş e-postaları temizlemek için yapılan işlemler de zaman alıyordu.[24] NATO sunucularının yanı sıra ABD Savunma Bakanlığı'nın alt yapısına yönelik saldırılar da düzenlendi. ABD Ordusu ve Hava kuvvetleri sistemlerini virüslerden arındırabilmek için dünyadaki tüm sunucularını bir hafta sonu süreyle hizmete kapattılar. Saldırılar yakından incelendiğinde bazı sitelerde hackerların "Çok Yaşa Büyük Sırbistan" ve "Kara El (Black Hand) bu siteye el koydu"[25] benzeri ifadeler yükledikleri görülmüştür. Hackerların gruplarına verdikleri Kara El ismi, Birinci Dünya Savaşı sırasında kurulmuş olan Sırp'lara ait gizli yer altı örgütünün adıdır. Artan saldırıların izleri araştırıldığında Sırpların yanı sıra Rus ve Çinli hackerların da bu saldırılara destek verdikleri anlaşılmıştır. Bu durum fiziki dünyadaki siyasi ittifakların siber alanda da devam ettiğinin işareti olarak değerlendirilebilir. Saldırıları engellemek amacıyla Pentagon'dan uzmanların müteakip hareketleri izlemek için Sırp bilgisayarlarına sızdıkları ve daha büyük stratejik zararların oluşmasını bu yolla önledikleri iddia edilmiştir.[26]

Bu gelişmelerin yaşandığı 1999 yılı, NATO'nun güvenlik hedefleri açısından önemli bir yıldır. NATO'nun Soğuk Savaş sonrası dönemin yeni hedeflerini belirleyen 1991 tarihli stratejik dokümanı, "o tarihten bu yana siyasette ve güvenlikte dikkate değer gelişmeler oldu[ğu]"[27] için 1999'da yenilendi. Belgede işbirliği ve bölgesel güvenlik örgütleriyle bütünleşme yolunda atılması gereken adımlardan bahsedilerek, AB'ye özel bir vurgu yapıldığı görülmektedir. Siber saldırı ya da siber tehdit konusu, o sırada meydana gelen Sırp hackerların saldırılarına rağmen NATO'nun güvenlik algısında ve yeni dokümanda yeterince yer almamıştır. 1999 tarihli Stratejik Konsept belgesinde, teknolojinin küresel olarak hızla yayılmasının hasımların silah üretim bilgilerine erişmelerini sağlayabileceği ve bunun da daha karmaşık bir rakip ordu oluşturacağı vurgulanmaktaydı. Belgeden, NATO'nun artık sadece devletleri değil devlet-dışı aktörleri de tehdit algısına dâhil ettiği anlaşılmaktadır. Belgede, NATO'nun Hibrit Savaş kavramını benimsediği ve tehditleri de bu çerçevede tanımladığı görülmektedir: "İlaveten, devlet ve devlet-dışı hasımlar ittifakın bilgi sistemlerine artan güvenini bu tür sistemleri bozmak için düzenlenen enformasyon operasyonlarıyla sömürebilirler. Bu tür stratejileri NATO'nun geleneksel silah gücü üstünlüğüne karşı gelmek için kullanabilirler."[28]

---

22 T1 bağlantının bant genişliği 1.544 Mbps'dir.

23 Ellen Messmer, "Serb Supporters Sock it to NATO, U.S. Web Sites", http://articles.cnn.com/1999-04-06/tech/9904_06_serbnato.idg_1_nato-personnel-nato-headquarters-nato-sources?_s=PM:TECH (Erişim Tarihi 12 Aralık 2011).

24 Dan Verton, "Serbs Launch Cyberattack on NATO", *Federal Computer Week*, http://fcw.com/articles/1999/04/04/serbs-launch-cyberattack-on-nato.aspx (Erişim Tarihi 12 Aralık 2011).

25 Chris Nuttall, "Net Warfare over Kosovo" http://news.bbc.co.uk/2/hi/science/nature/200069.stm (Erişim Tarihi 12 Aralık 2011).

26 Julian Borger, "Pentagon Kept the Lid on Cyberwar in Kosovo" *The Guardian,* 9 Kasım 1999, http://www.guardian.co.uk/world/1999/nov/09/balkans (Erişim Tarihi 11 Aralık 2011).

27 "The Alliance's Strategic Concept, 24 Nisan 1999", http://www.nato.int/cps/en/natolive/official_texts_27433.htm (Erişim Tarihi 12 Aralık 2011).

28 "The Alliance's Strategic Concept, 24 Nisan 1999", 23. madde, http://www.nato.int/cps/en/natolive/official_texts_27433.htm (Erişim Tarihi 12 Aralık 2011).

Bu değerlendirmeden NATO'nun geleneksel savaş üstünlüğünün enformasyon teknolojilerinde yaşanan gelişmeler neticesinde etkisiz kalabileceğinden şüphelendiği sonucuna varılabilir. NATO'nun yeni güvenlik stratejisinin belirlendiği 1999 zirvesinden hemen sonra, devlet ve hükümet başkanlarının katılımıyla Washington'da düzenlenen "21. Yüzyılda İttifak" başlıklı toplantıda, ittifak iyesi ülkelerin savunma imkân ve kabiliyetlerinin artırılması için stratejik tertiplenebilme ve hareket kabiliyetinin yükseltilmesi gerektiği belirtildi. Bu çerçevede etkili enformasyon sistemlerine sahip olunmasının savunma gücünü arttıracağı vurgulandı.[29] Kosova müdahalesinden alınan derslerle bu tarihten sonra yayımlanan resmi NATO belgelerinin neredeyse tamamında siber güvenlik konusuna ve "enformasyon sistemleri"nin önemi ve korunması başlıklarına yer verilmiştir. Ne var ki, enformasyon sistemlerinin kimin için ve nasıl güvenli hale getirileceği, güvenliğin sağlanmasının maliyetinin ne olacağı türünde sorularının cevapları verilmemekteydi.

11 Eylül 2001'de New York'taki Dünya Ticaret Merkezi Kuleleri başta olmak üzere çeşitli hedeflere yönelik olarak yolcu uçaklarıyla düzenlenen terör saldırıları, bilinen güvenlik tanımlarını alt üst etti. Güvenlik yeniden birçok ülkenin öncelikler listesinde üst sıralara tırmandı ve "terörizmle savaş" sadece saldırıya uğrayan devleti değil, sistemdeki tüm aktörleri ilgilendiren bir konu başlığına dönüştü. ABD önderliğindeki uluslararası koalisyon, saldırıların ve uluslararası terörün kaynağı olarak görülen El Kaide'ye ortadan kaldırmak amacıyla 2001 sonbaharında Afganistan'a girerek Taliban rejimine son verdi. NATO'da Uluslararası Güvenlik Yardım Gücü (International Security Assistance Force-ISAF) adı altında ve müttefik ülkelerin katılımıyla Afganistan'da görev yapmaya başladı. Bu görev, merkez karargâhı ile alandaki muharip güçler arasında güvenli bilgisayar, telefon ağları ve video konferans bağlantılarının kurulabilmesi konusunu NATO'nun siber alandaki önceliklerinden birisini haline getirdi. Stratejik ve gizli bilgileri taşıyacak bu altyapıların kurulması NATO için bilgi güvenliğinin esasını teşkil etmiştir.

11 Eylül sonrasında tansiyonun yüksek olduğu dönemde üzerinde en çok tartışılan konulardan birisi, NATO'ya ya da üyelerden birine yönelik olarak gerçekleştirilebilecek Dijital Felaket (diğer adıyla dijital 9/11) senaryosudur.[30] Bu senaryo çerçevesinde üye devletlerin siber sistemlerine yapılacak herhangi bir saldırının ülkenin kritik alt yapısını etkisiz hale getirmesi ve böylece ülkedeki güvenliği derinden sarsması ele alınmaktaydı. Bu tür endişeler milli güvenlikle kavramıyla yakından ilişkilendirilmekteydi.[31] Bu değerlendirmelerin sonuçları 21 Kasım 2002'de düzenlenen Prag Zirvesi'nin gündeminde yansıdı. Zirve'de siber saldırılara karşı savunmanın güçlendirilmesi konusu ele alındı

---

29 "An Alliance for the 21st Century' Washington Summit Communiqué issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Washington, D.C. on 24th April 1999" http://www.nato.int/cps/en/natolive/official_texts_27440.htm (Erişim Tarihi 13 Aralık 2011).

30 Ralph Bendrath, "The American Cyber-Angst and the Real World – Any Link?", Robert Latham (Der.), *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, New York, The New Press, 2003, s.49–73.

31 Helen Nissenbaum, "Where Computer Security Meets National Security," *Ethics and Information Technology*, Cilt 7, 2005, s.61–73.

ve NATO'nun gerekli planlamaları yapması karara bağlandı.[32] Zirve'de siber güvenlik yapılanması tek başına bir unsur olarak ele alınmamış, askeri kabiliyetlerin arttırılması bağlamında değerlendirilmiştir. Zirve'de alanına kararı hayata geçirmek amacıyla NATO Ağ ile Etkinleştirilmiş Güç (Network-Enabled Capability-NNEC)[33] programı başlatıldı. Programın amacı NATO'nun askeri ve sivil unsurlarının enformasyon altyapısı aracılığıyla birleştirmesiydi. Anlayış, bilginin yeterince hızlı ve güvenle paylaşılmadığı takdirde üye ülkelerin muhtemel NATO harekâtlarına etkin katılımının mümkün olmayacağı üzerine inşa edilmişti.

Üye ülkelerin ağ yapısı ve askeri potansiyeli bu paylaşımı etkilemektedir. Her ülkenin askeri alt yapısı, eğitim durumu veya ağ niteliği NATO planlarının uygulanmasını etkilemektedir. Siber güvenlik açısından bakıldığından, NNEC ve Ağ merkezli Savaş (Network Centric Warfare-NCW) kavramlarından ziyade bu savaş tarzı için gerekli olan bilişim alt yapısının korunması önemlidir. Bu nedenle, Soğuk Savaş döneminde bu amaçla hizmet veren NATO İletişim ve Enformasyon Sistemleri Ajansı (Communications and Information Systems Agency-NACISA) ve Avrupa İttifak Güçleri Büyük Karargâhları (Supreme Headquarters Allied Powers Europe-SHAPE) Teknik Merkezi, yerlerini 1 Haziran 1996'da kurulan NATO Danışmanlık, Komuta-Kontrol Ajansı'na (NATO Consultation, Command and Control Agency-NC3A)[34] bıraktı. Bu ajansın görevi teknolojik boyuttaki gelişmeleri takip etmek, bunların NATO bünyesinde işlevsel hale gelmesini sağlamak ve NATO'nun askeri yetkililerinin askeri operasyonlar sırasında duydukları acil ihtiyaçlara cevap vermektedir. NC3A, NATO operasyonlarında araştırmadan takibe, hava komuta-kontrolden füze savunmasına, elektronik harpten erken uyarı ve kontrol sistemlerine, iletişimden bilişim sistemlerine kadar birçok sahada görev yapmaktadır. 11 Eylül sonrasında Hibrit Savaş kavramının daha açık bir biçimde ortaya çıkmasına müteakip, bilgi paylaşımı ve ortak komuta-kontrol fikrinin ne derece fonksiyonel olduğu anlaşılmış ve yapılanma günün şartlarına uyumlu hale getirilmiştir. Ağ merkezli savaş fikrini icra ederken siber güvenliğin öneminin artacağı da açıktır. NC3A yapılanması içinde siber güvenlik ve bilgi paylaşımının sağlanması için faaliyet gösteren bir bölüm de bulunmaktadır. Bu gün ağ merkezli savaşın daha ön plana çıkmasıyla NC3A'nın yapılanması daha da detaylandırılmıştır. Bu haliyle ilk yapılanmasından hayli farklı olduğu görülebilmektedir.[35]

Aynı dönemde NATO'nun yeni savaş anlayışına uyum sağlamak amacıyla sinyal dinlemek ve işlemek için kurulmuş olan elektronik harp merkezleri de yeniden düzenlendi ve 7 Eylül 2004'te NATO İletişim ve Enformasyon Sistemleri Servisi Ajansı (NATO Communication and Information Systems Services Agency-NCSA) oluşturuldu. 2004 yılında kurulan bu ajans, ağ ile etkinleştirilmiş güç kavramını hayata geçirebilmek için merkez karargâhı ile diğer görev güçleri arasındaki iletişimi sağlamaktadır. Kosova operasyonundan anlaşıldığı üzere siber saldırılar ilk olarak iletişim kanallarına

---

32 *The Prague Summit and NATO's Transformation*, 2003 http://www.nato.int/docu/rdr-gde-prg/rdr-gde-prg-eng.pdf (Erişim Tarihi 14 Aralık 2011).

33 Program hakkında bkz. http://nnec.act.nato.int/pages/about.aspx, (Erişim Tarihi 14 Aralık 2011).

34 Detaylı bilgi için bkz. http://www.nc3a.nato.int/Pages/default.aspx, (Erişim Tarihi 14 Aralık 2011).

35 Yapılanma için bkz. http://www.nc3a.nato.int/SiteCollectionImages/NC3A/Charts/NC3A-SimpleOrg_large.jpg (Erişim Tarihi 15 Aralık 2011).

odaklanmaktadır. Prag Zirvesi'nde alınan kararlardan bir diğeri de kritik alt yapıların terörizme karşı korunması için NATO siber savunma programının oluşturulmasıdır. Bu yüzden NCSA siber saldırılara karşı ilk müdahaleyi yapacak unsur olarak belirlenmiştir. Ajansın içindeki merkezlerden en önemlisi, muharip unsurların bilgi güvenliği ve ittifak genelinde güvenli iletişimi sağlamakla yükümlü NATO Bilgi Güvenliği Teknik Merkezidir (NATO Information Assurance Technical Centre-NIATC). NATO'nun 2007 yılına kadar iletişim, bilgisayar güvenliği ve siber güvenliği aynı kefeye koyduğunu görülmektedir. NIATC, bilgisayar ağlarını Bilgi Güvenliği Operasyon Merkezi ve NATO Bilgisayar Olayları Müdahale Gücü Teknik Merkezi'yle (NATO Computer Incident Response Capability Technical Centre-NCIRC) işbirliği içinde ve 7/24 esasında takip etmektedir. Bu gelişmeye müteakip 2006'da yapılan Riga Zirvesi'nde ağ ile güçlendirilmiş komuta-kontrol kavramı üzerinde durulmuş ve bilişim alt yapısının savunmasının iyileştirilmesinin gerektiğine vurgu yapılmıştır.[36]

Prag Zirvesi'nin NATO'nun siber güvenlik algısı ve strateji mantığının değişiminde bir başlangıç olarak kabul edilmektedir. Ancak bu denli büyük ve köklü alışkanlıklara sahip olan bir kuruluşta değişikliklerin istenilen hızda olmasını beklemek iyimserlik olacaktır. Oysa tehdit olarak tanımlanan asimetrik unsurların kendilerini çabucak güncelledikleri ve hedeflerine düzenli ya da rastgele biçimde sistematik olmayan bir yapıda saldırdıkları görülmektedir. Ayrıca uluslararası sistemde hukukla kayıt altına alınan cezaya tabi fiiller (casusluk, endüstriyel hırsızlık, bilgisayar korsanlığı, servis durdurmak, vb.) siber ortamda hiç bir kısıtlama olmadan gerçekleştirilmektedir. Siber saldırganlar çeşitli yöntemler kullanarak saldırılarının kaynağını gizlemeye çalışırlar. Bazı saldırılarda yaptıkları eylemi gizlemek için geride bıraktığı izleri sildikleri de görülmüştür. Devletlerin büyük ve hantal işleyişine karşı siber saldırılar hızlı ve asimetrik olarak ortaya çıkmaktadır. Öte yandan siber alanın zaman zaman devletler tarafından yönetilen siber saldırılar için kullanıldığı tahmin edilmektedir. Bürokrasi'nin hareket hızı ile siber saldırının gerçekleşme hızı arasındaki fark da devletlerin bu konuda kolayca mazeretler üretmesine imkân sağlıyor. Her ne kadar aksini belirtseler de, karanlık taraftaki bu korunmuşluk devletler için de cazip geliyor. İspatı bile mümkün olmayacağı için bütün ithamlarda komplodan öte gitmesi mümkün görünmüyordu. Bu yüzden birçok devlet kullanmış ya da kullanmaktadır. NATO karargâhında ve müttefik ülkelerde bu türde sorunlara nasıl yaklaşılacağı ve sorunlarla hangi yöntemlerle başa çıkılacağı konuları tartışılırken Estonya'ya yapılan uzun süreli ve yoğun siber saldırılar gündemi büyük bir hızla değiştirdi.

Bronz Asker'in Dijital Ordusu

Estonya internet kullanımının en yüksek düzeyde olduğu ülkelerden birisidir. Her vatandaşın devlet kurumlarına ve bankalarına internet üzerinden bağlanmasına imkân veren bir dijital kimliğe sahip olduğu ülkede, 355 devlet kuruluşu sanal dünyada yer almaktadır. Ernsdorff ve Berbec araştırmalarında Estonya'nın e-devlet yapılanmasında Orta ve Doğu Avrupa'da lider ve dünyada üçüncü sırada yer aldıklarını belirtir.[37] 2001

[36] "Riga Summit Declaration, 29 Kasım 2006", http://www.nato.int/docu/pr/2006/p06-150e.htm, (Erişim Tarihi 10 Kasım 2011).

[37] M. Ernsdorff ve A. Berbec, "Estonia: The Short Road to E-government and E-democracy", P. Nixon ve V. Koutrakou (Der.), E-government in Europe. Abingdon, Routledge. 2007, s.171.

yılında çalışmaya başlayan veri değişim katmanı olan *X-Road* programı Estonya'daki kurumları ve insanları birbirine bağlamaktadır. Bu E-devlet programı uygulamaları açısından diğer örneklerine nazaran en gelişmiş örnektir. Estonya, dünya üzerinde internet kullanarak yapılmış olan ilk yerel seçimlere de 2005 yılında ev sahipliği yapmıştır.[38] 2010 yılı verilerine göre, Estonya'nın 1.46 milyonluk nüfusun yüzde 75'i internet kullanıcısıdır.

Estonya, NATO'nun 2002 Prag Zirvesi sonrasında üyelik görüşmelerine başladı ve Mart 2003'te de üye olarak kabul edildi. Bu süreç ülkenin Rusya'dan zihinsel olarak hızla uzaklaşmasına sebep oldu. Bu çerçevede Estonya'nın başkenti Tallinn'e Kızıl Ordu'nun girişinin ifadesi olarak 1947 yılında yapılmış olan "Tallinn'in Kurtarıcısı Heykeli" ya da popüler adıyla "Bronz Asker" heykeli de bu süreçten nasibini aldı. Heykelin yıkılmasını isteyenler ile yer değiştirmesi gerektiğini savunanlar arasında yürüyen tartışma sonucunda heykel, hükümetin kararıyla Tallinn'deki askeri mezarlığa taşındı. Rus kökenli Estonya vatandaşlarının[39] protesto gösterileri devam ederken ülkenin siber altyapısını hedef alan saldırılar 27 Nisan gece yarısından sonra başladı ve giderek hız kazandı. Ping yoğunluyla başlayan hareket çok hızlı bir şekilde servis dışı bırakma saldırısına dönüştü.[40] Çeşitli Rus internet forumlarında Estonya'daki adresler hedef olarak gösterildi ve teknik bilgisi olmayan sıradan bilgisayar kullanıcılarına kadar ulaşan bir kitleye saldırıyı gerçekleştirmenin yöntemleri açıklanarak saldırı yaygınlaştırıldı. Ülkedeki *Hansabank* ve *SEB* gibi bankalar siber saldırılara hazırlıklı oldukları için ilk gün yapılan saldırılardan çok zarar görmediler. Fakat hazırlıksız olan Estonya hükümet siteleri işlevlerini yerine getiremez hale geldi. Başkanlık ve parlamento siteleri, bütün bakanlık siteleri, siyasi partilerin siteleri bu hedefler arasındaydı. Estonya'daki altı büyük medya kuruluşu ve iletişim firmaları da saldırıdan nasibini aldı.[41] Ülkede IP'leri kontrol eden ve izleyen sistemlerin olmaması da tehdidi daha hissedilir hale getirdi. Saldırılara tek cevap verecek kurum ülkedeki e-seçimlerin alt yapısını kuran uzmanlardı. 28 Nisan'da zirve noktasına ulaşan saldırılar yavaş yavaş azaldı ve 3 Mayıs'ta aralarında ping taşması şeklinde tanımlanan saldırıların da olduğu kontrol edilebilir seviyedeki saldırılar başladı. Rusya'nın İkinci Dünya Savaşı'nda Nazi Almanya'sını yendiği gün olan 9 Mayıs'ta da botnet saldırıları başladı.[42] 11 Mayıs'ta yavaşlayan bu saldırılar, 18 Mayıs'ta tekrar başladı ve 23 Mayıs'a kadar devam etti. Çok sayıda Rus sitesinin katıldığı bu saldırılar sırasında Rusya'daki http://2ch.ru ve http://forum.xaker.ru sitelerinin kullanıcılarını basit programlarla saldırıya katılımı teşvik ettiği bilinmektedir. Özellikle kanal genişliği doldurmak amacıyla ping saldırıları detaylı bir şekilde belirtilmiştir. Bir Rus sitesinden alınan ping yaparak bant genişliğini doldurmayı hedefleyen bu saldırı da belirli adresler ve IP numaraları da verilmiştir:

---

38 Katri Kerem, Internet Banking in Estonia, Tallinn, Praxis Center for Policy Studies, 2003, s.4–7.

39 Estonya'da 2009 nüfus sayımına göre Estonlar nüfusun yüzde 68,7'sini oluştururken, Ruslar tüm nüfusun yüzde 25,6'sını oluşturuyorlar. Daha detaylı bilgi için bakınız; http://www.stat.ee/public/rahvastikupyramiid/ (Erişim Tarihi 31 Ocak 2012).

40 Kaynak bilgisayardan karşıdaki bilgisayara paket gönderilerek o anda çalışmakta olduğu ve ağın kayıp paket oranını hakkında bilgi veren programcıktır. Fazla gönderilerek sistemlerin çalışmasını engellenebilir ve durdurabilir.

41 Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia", *The Guardian,* 17.05.2007, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia, (Erişim Tarihi 17 Aralık 2011).

42 Botnet saldırıları kullanıcının bilgisi dışında ele geçirilmiş zombi bilgisayarların bir merkezden hedefe doğru saldırı için yönlendirilmesidir.

```
@echo off
SET PING_COUNT=50
SET PING_TOMEOUT=1000
:PING
echo Pinguem estonskie servera
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% dns.estpak.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.126.115.18
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.eenet.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.56.245
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.kbfi.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.133.222
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.online.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.106.96.21
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.uninet.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.204.0.1
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.ut.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.5.99
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.uu.net
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 137.39.1.3
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% sunic.sunet.se
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 192.36.125.2
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% muheleja.eenet.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.0.132
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns2.eenet.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.0.12
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% kbfi.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.204.58.129
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% smtp.uninet.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.204.0.4
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ptah.kbfi.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.204.58.129
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.gov.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 195.80.106.241
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.aso.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 195.80.96.222
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns2.ut.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.5.76
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% mail.gov.ee
GOTO PING[43]
```

İnternet forumundaki mesajda, Estonya'nın Rusları aşağılanmasına son vermek için bu saldırıların yapıldığı ve hükümet sitesinin artık çalışmadığı belirtilmektedir. Ayrıca başka hedeflere saldırabilmek için sonsuzluk döngüsüyle çalışan yukarıdaki programcığı yazdıkları ve "bat" uzantılı dosya oluşturarak e-posta ve alan adı sunucularını (*domain name server*-dns) çökertebilecekleri de mesajda yer alıyordu.[44] Başka bir sitede de saldırıların 9 Mayıs gece

[43] 10 Mayıs 2007 tarihinde yayınlanmış bu bilgi için bakınız, http://krezi.livejournal.com/168695.html, (Erişim Tarihi 17 Aralık 2011).

[44] Rusça metin için bakınız, http://terror.3bb.ru/viewtopic.php?id=960, (Erişim Tarihi 12 Aralık 2011).

yarısında yapılması tavsiye edilmekteydi.[45] *X-Road* sistemini çökertmek için daha teknik beceri gerektiren esrarengiz veri paketlerinin *router*'lara gönderildiği de farklı kaynaklarda belirtilmekteydi.[46] Dağıtık servis dışı bırakma saldırısı ile ABD, Kanada, Rusya, Türkiye, Almanya, Belçika, Mısır ve Vietnam gibi ülkelerden gelen IP'ler kaydedilmişti. Bu kayıtlara bakıldığında Estonya için saldırılarda düşmanın ve saldırganın kim olduğu açık değildir. Estonya hükümeti saldırıların etkisini azaltmak için bant genişliğini iki Gbps'ten 8 Gbps'e çıkardı. Özel sektör de sunucuların sayısını ve alan genişliğini arttırdı.

Makalenin konusuyla ilgili en önemli gelişme Estonya Savunma Bakanı Dr. Jaak Aaviksoo'nun NATO'ya ve diğer ülkelere yönelik olarak yaptığı yardım çağrısıdır. NATO tarafından oluşturulan geçici (*ad hoc*) yardım takımları Estonya'da göreve başladı ve NATO da gelişmelere hızlı ve etkili bir biçimde müdahil oldu.[47]

Estonya siber saldırısı sonrasında konuyla ilgili olarak 15 Ağustos 2007'de İngiliz raportör Lord Jopling tarafından hazırlanan raporla, daha önce terörizm önceliğiyle yazılan 2006'daki güvenlik belgesine[48] siber güvenlik önceliği ilave edildi.[49] Bu düzenleme, NATO'nun savaş algısının Soğuk Savaş dönemine göre ne denli farklılaştığına işaret etmektedir. NATO'nun 2008 Bükreş Zirvesi, siber güvenlik konusunun kapsamlı bir biçimde ele alındığı ve Sonuç Bildirgesi'nde özel bir yer edindiği ilk Zirve'dir. Zirve sonrasında şekillenen NATO'nun yeni Strateji Belgesi'nde, NATO'nun, savaş kavramında yaşanan değişikliğe cevap verecek yapılanmaya dönüşmesinin gerekli kaynaklar ayrılmadan mümkün olamayacağı belirtilmektedir. Bu çevrede Zirve Bildirgesi'nin 46. maddesinde, NATO'nun bu değişimin sağlanması için gereken kaynağı temin edeceği belirtilmiştir. Ancak kaynağın nasıl sağlanacağı hakkında metinde bilgi verilmemiştir. Sonraki maddede ise ittifak üyelerinin enformasyon sistemlerinin siber saldırılara karşı güçlendirilmesi için NATO'nun kararlılıkla çalışacağı vurgulanmıştır. İttifak üyelerinin siber savunma konusunda tecrübelerini paylaşmaları ve gerektiğinde birbirlerine yardım etmeleri konusunun altı çizilmiştir. 47. Maddede vurgulanan diğer bir nokta, devlet ve uluslararası organizasyonların siber alandaki gelişmelerin hızını yakalamadaki zafiyetlerinin farkında olunduğunun ve bunu aşmak için, NATO ile üye ülkeler arasındaki ilişkinin güçlendirilmesinin hedeflendiğinin belirtilmesidir.[50]

---

45 http://forum.nov.ru/lofiversion/index.php?t109658.html, (Erişim Tarihi 15 Aralık 2011).

46 http://aebr.home.xs4all.nl/wl/tallinn/tallinn.html (Erişim Tarihi 31 Ocak 2012).

47 Finlandiya, Almanya, İsrail ve Slovenya'dan yardım için bilgisayar olaylarına müdahale ekipleri gelmiştir. Detaylar için bkz. Kertu Ruus, "Cyber War I: Estonia Attacked from Russia", European Affairs, Cilt 9, No.1, Kış-Bahar 2008, http://www.europeaninstitute.org/2007120267/Winter/Spring-2008/cyber-war-i-estonia-attacked-from-russia.html, (Erişim Tarihi 18 Aralık 2011). Estonya savunma bakanı Aaviksoo Haziran 2007 NATO Savunma Bakanları toplantısında siber saldırıların detaylarıyla ilgili olarak meslektaşlarını bilgilendirdi. Bkz. Ministries of Defence of Estonia, Latvia and Lithuania, "Defense Policies'07 in Brief: Estonia, Latvia and Lithuania", Baltic Security and Defence Review, Cilt 10, 2008, s.262.

48 Kritik Bilgi Altyapısı güvenlik raporları hakkında bakınız; https://www.rdb.ethz.ch/projects/project.php?proj_id=22156&type=search.

49 "162 CDS 07 E rev 1-The Protection of Critical Infrastructures", http://www.nato-pa.int/default.asp?SHORTCUT=1165 (Erişim Tarihi 16 Aralık 2011).

50 "Bucharest Summit Declaration 03 Nisan 2008", http://www.nato.int/cps/en/natolive/official_texts_8443.htm, (Erişim Tarihi 16 Aralık 2011).

Bükreş Zirve'si sonrasında siber güvenlik alanında iki önemli gelişme yaşandı.[51] İlk olarak Brüksel'de bir NATO Siber Savunma Yönetimi Otoritesi'nin (*Cyber Defense Management Authority*-CDMA) kurulmasına karar verildi. Siber savunma kapasitesini bir merkezde toplayarak harekât kabiliyetini daha arttırmak isteyen NATO, bununla yetinmeyerek Estonya Tallinn merkezli bir NATO Siber Savunma İşbirliği Mükemmeliyet Merkezi (*Cooperative Cyber Defence Centre of Excellence*–NATO CCD COE) kurdu.[52]Merkez, Estonya Savunma Bakanlığı'nın NATO'ya bu türde bir merkezin kurulması için 2007 saldırıları öncesinde teklif vermiş olmasına rağmen ancak Ekim 2008'de kurulabilmiştir.[53] 30 personelden oluşan Merkez'in görevleri şunlardır:

1) Siberle ilgili konularda ittifak için doktrinler ve kavramlar üretmek;
2) NATO'ya üye ülkeler için eğitim kursları, atölye çalışmaları düzenlemek. Tatbikatlar yapmak;
3) Araştırmalar yapmak ve gelişmeler üzerine toplantılar düzenlemek;
4) Geçmişteki ve hâlihazırdaki saldırıları çalışarak dersler çıkarmak;
5) Devam eden saldırılarda eğer istenirse tavsiyeler vermek.[54]

Estonya'ya yönelik siber saldırıların üzerinden bir yıl henüz geçmişti ki Rus Federasyonu ile Gürcistan arasında Güney Osetya nedeniyle bir çatışma patlak verdi.[55] 7 Ağustos 2008 Gürcistan kuvvetlerinin Gürcistan'ın toprak bütünlüğünü tesis etmek amacıyla Güney Osetya'ya yönelik operasyona başlamasına cevaben Rus güçleri 8 Ağustos'ta Osetya'ya girdiler ve sonrasında da Gürcistan'ı işgal ettiler.

Aslında Ruslar Gürcistan'a ilk cevabı 7 Ağustos 2008 akşam saatlerinde düzenlenen siber saldırılarla vermeye başladı. Gürcistan'daki enformasyon alt yapısı Estonya kadar gelişmiş olmaması Gürcistan açısından büyük boyutlu sorunlara neden olmadıysa da saldırının olayların gelişimi ve izlenen yöntemler bağlamında Estonya örneğiyle bire bir örtüştüğü görülmektedir. Gürcistan'ın Rusya ile yaşadığı gerginliğin ardında NATO'ya üyelik hedefi yatmaktadır. Fakat Gürcistan'ın ittifaka üyeliği henüz gerçekleşmediği için Gürcistan NATO'nun güvenlik şemsiyesinden faydalanamamıştır. Siber saldırıları gerçekleştirilen siteler incelendiğinde bunların ABD'den çalınana kredi kartlarıyla Rusya ve Türkiye'de açılan siteler olduğu belirlenmiştir.[56] Saldırı için gönderilen *spam* postaların

---

51 "NATO Agrees Common Approach to Cyber Defence", http://www.euractiv.com/infosociety/nato-agrees-common-approach-cyber-defence/article-171377, (Erişim Tarihi 17 Aralık 2011).

52 Rex B. Hughes, NATO and Cyber Defence: Mission Accomplished?, Atlantisch Perspectief, No 1, Nisan 2009.

53 Ministries of Defence of Estonia, Latvia and Lithuania, "Defense Policies'07 in Brief: Estonia, Latvia and Lithuania", Baltic Security and Defence Review, Cilt 10, 2008, s.262.

54 173 DSCFC 09 E bis - NATO and Cyber Defence, 2009, http://www.nato-pa.int/default.Asp?SHORTCUT=1782 (Erişim Tarihi 13 Aralık 2011).

55 Gürcü ve Osetler arasında 1991'de meydana gelen silahlı çatışma sonrasında 1992'de Güney Osetya'da güvenliği sağlamak amacıyla Rus, Gürcü ve Osetlerden oluşan bir barış gücü oluşturuldu. Bölgede yaşanan anlaşmazlıklara rağmen bir düzen kurulduğu söylenebilir. Rusya ile Gürcistan arasındaki gerginliğin 2004'ten itibaren artmaya başlaması Güney Osetya'daki istikrarın sonu oldu.

56 Siobhan Gorman, "Hackers Stole IDs for Attacks" The Wall Street Journal, http://online.wsj.com/article/SB125046431841935299.html (Erişim Tarihi 18 Aralık 2011).

Rusya'nın önemli siber suçlularından Rus İş Ağı (*Russian Business Network*) tarafından gönderildiği tespit edilmiştir.[57] St. Petersburg merkezli bu ağ, NATO tarafından hazırlanan bir raporda da saldırganlık eğilimiyle suçlanmıştır.[58]

Gürcistan'a yönelik olarak düzenlenen siber saldırılardan çıkartılabilecek en önemli sonuç bunun gerçek bir hibrit savaş niteliği taşımasıdır. Geleneksel savaş yöntemlerini kullanan Rusya, eş zamanlı olarak siber saldırıları da başlatmıştır. Rusya'nın uyguladığı bu savaş düzenine hibrit savaş olarak tanımlamak mümkündür. Olayın bu şekilde gerçekleşmesi NATO'nun hibrit savaşa olan inancını destekledi. Ancak siber savaş konusunda NATO'nun kavramsal tercihi "siber güvenlik" kavramını kullanmak olmuştur. Saldırıyla cevap verilmesinin gerekeceği durumlar için de müttefik güçlerinin siber saldırı yeteneklerini kullanmayı planlamaktadır.[59] Geleneksel savaş konusunda hazırlıklı olan NATO siber savunma konusundaki eksikliklerini de Bükreş zirvesi sonrasında hızlıca gidermeye çalıştı. Özellikle CDMA'nın kuruluşunu takip eden ilk 10 ay içinde Siber Harekât'a yönelik kavramları tartışmak üzere beş kez toplanmıştı. Bu toplantılarda NATO'ya ait kavramlar oluşturulmuştu. CDMA ilk iki siber savunma tatbikatını da Rusya'nın Gürcistan'a saldırısından önce gerçekleştirmişti.

Gürcistan saldırısı gerçekleştikten sonraysa durumu değerlendirmek üzere bir CDMA uzmanı bölgeye sevk edilmiştir. Gürcistan hükümetinin saldırı altındaki sunucuları ülkenin içinden daha güvenli sunuculara taşınmıştır. Bütün bu girişimlere rağmen siber dünyada tehdit düzeyinin artması ve siber araçlarla saldırının çok küçük eğitimlerle gerçekleştirilebildiği gerçeği NATO üyelerini korkutmaktadır. Üye ülkeler, Nisan 2009'da Strazburg/Kehl'de yapılan zirvede yeni siber savunma tavırlarının geliştirilmesini istediler. Siber savunmanın NATO tatbikatlarının parçası haline getirilmesine ve NATO ile üye ülkeler arasındaki bağın siber tehditlere karşı güçlendirilmesine karar verildi. NATO karargâhında görevlendirilen 43 uzmanın, üye ülkelerle siber savunmanın hukuki yönleri konusunda görüşmeler yapmaya başlaması, NATO stratejisinin geliştiği yönü göstermektedir.[60] Siber saldırıların hangi hukuk esaslarına göre değerlendirileceğinin belirsiz olmaması ve bu konudaki uluslararası hukukun gelişmemiş olmasının ittifak üyelerinin siber savunmasını zayıflattığına vurgu yapılmaktadır.

NATO'nun 2009'da attığı en büyük adımlardan bir diğeri de Hızlı-Tepki Takımları'nın (*Rapid-Reaction Teams*-RRTs) kurulmasıdır. Bu takımlar ihtiyaç halinde üye ülkelere yardım etmek üzere hazır tutulmaktadırlar. Tam anlamıyla 2012'de aktif hale gelecek olan bu takımlar; üye ülkelerdeki uzmanlardan ve NATO çalışanlarından oluşmaktadır. Takımların ilgili üye ülke tarafından çağrı yapıldığında saldırıya uğrayan ülkenin komutası altında çalışması öngörülmektedir. Donanım ve yazılıma bağlı olarak siber tehditlerin her gün kendini yeniliyor olması ona karşı koymak için organize olan

---

57 Alexander Klimburg, "Mobilising Cyber Power", Survival, Cilt 53, No.1, 2011, s.50.

58 Sverre Myrli (Norway) - Rapporteur, "173 DSCFC 09 E bis - NATO and Cyber Defence", http://www.nato-pa.int/default.Asp?SHORTCUT=1782 (Erişim Tarihi 16 Kasım 2011).

59 Süleyman Anıl, NATO Bilgisayar Olayları Müdahale Gücü Teknik Merkezi Başkanı ile yapılan görüşme, NATO COE DAT, Ankara, Mayıs 2011.

60 "Strasbourg/Kehl Summit Declaration, 04 Nisan 2009", http://www.nato.int/cps/en/natolive/news_52837.htm?mode=pressrelease (Erişim Tarihi 19 Aralık 2011).

güçleri zor durumda bırakmaktadır. Yetkililer NATO'nun, bütün bu yeniliklere rağmen, tehdidin hızlı değişen tarzı nedeniyle karşılık vermede yeteri kadar hızlı olmadığının da farkındadırlar. Ancak hali hazırdaki NATO organizasyonu içinde asimetrik karakterli siber tehditlere karşı hızlı bir şekilde nasıl cevap verilebileceği yönünde tartışmalar devam etmektedir.

Siber İttifak'a Doğru

Strazburg zirvesinde konuşulan ana konulardan bir diğeri değişen tehditlerin belirlenmesi ve buna uygun stratejinin geliştirilmesiydi. Stratejinin altyapı teşkil edecek raporun hazırlanması için bir akil adamlar grubu oluşturuldu. Başkanlığını ABD eski Dışişleri Bakanı Madeleine K. Albright'ın yaptığı heyette Jeroen van der Veer (Başkan Yardımcısı, Hollanda), Büyükelçi Giancarlo Aragona (İtalya), Büyükelçi Marie Gervais-Vidricaire (Kanada), Milletvekili ve Devlet Adamı Geoff Hoon (İngiltere), Büyükelçi Ümit Pamir (Türkiye), Büyükelçi Fernando Perpiñá-Robert Peyra (İspanya), Büyükelçi Dr Hans-Friedrich von Ploetz (Almanya), Bruno Racine (Fransa), Büyükelçi Aivis Ronis (Letonya), Profesör Adam Daniel Rotfeld (Polonya) ve Büyükelçi Yannis-Alexis Zepos (Yunanistan) yer almaktaydı.[61] Grup raporunu NATO Genel Sekreterine 17 Mayıs 2010'da sundu. Raporda yer alan ve gelecek yıllarda karşılaşılacak başlıca tehditler arasında siber saldırılar da yer almaktaydı.[62] NATO'nun bu tarihe kadar gösterdiği bütün çabalara rağmen siber savunma kapasitesinde önemli boşluklar olduğu kaydedilmişti.[63] Bu çerçevede, ittifakın ani bir siber saldırıyla karşı karşıya kalması durumunda, Genel Sekreter ya da NATO komutanlarından birinin karşılık vermek üzere görevlendirmesi istenmekteydi.[64] Böylece saldırı gerçekleşirse karşılığı verecek ekibin üst düzeyde yönetilmesi gerektiği vurgulanmıştır. Gerçekleşebilecek herhangi bir siber saldırı, ittifak anlaşmasının 4 ve 5. Maddeleri çerçevesinde saldırı sayılacağı için, meselenin ortak güvenlik kavramı şemsiyesi altında değerlendirilebileceği de açıkça ifade edilmekteydi. Raporda şu noktalar tavsiye olarak belirtilmiştir:

1- NATO'nun kritik ağları takip etme gücü arttırmalı ve tanımlanmış bütün zayıflıklar sağlamlaştırılmalıdır.

2- Siber Savunma Mükemmeliyet merkezi daha fazla eğitim yaparak ittifak üyelerinin siber savunma programlarını geliştirmelidir.

3- İttifak üyeleri, NATO genelindeki alıcıları ve ağ düğümlerini (*node*) izleyerek erken uyarı kabiliyetlerini arttırmalıdır.

4- İttifak, büyük siber saldırı yaşayan ya da bu tehdidi hisseden üyelerine uzman takımı göndermelidir.

---

61 http://www.nato.int/strategic-concept/experts-strategic-concept.html, (Erişim Tarihi 17 Aralık 2011).

62 "NATO 2020: Assured Security; Dynamic Engagement", s.17, http://www.nato.int/strategic-concept/expertsreport.pdf (Erişim Tarihi 18 Aralık 2011).

63 İbid., s.45.

64 İbid., s.35.

5- Zaman içinde NATO, aktif ve pasif siber savunma unsurlarının tamamına cevap verebilecek yeterlilikte bir stratejiyi uygulamayı planlamalıdır.[65]

2010 yılında sunulan bu raporun değerlendirmeleri, aynı yılın Kasım ayında Lizbon'da yapılan zirvede değerlendirildi. Toplantıda imzalanan belgenin 40. Maddesi Akil Adamlar grubunun raporunda belirtilen hususları tekrarlıyordu. En önemli farklılık siber savunmada BM ve AB ile yakın işbirliği içinde çalışılacağının belirtilmesiydi.[66] Belgede aynı zamanda Haziran 2011'e kadar detaylı bir siber savunma politikasının oluşturulacağı da yer almaktaydı. Belgelerin tamamında benzer noktaların tekrarlanarak ilerleme kaydedilmeye çalışıldığı görülmektedir. Bu noktada, siber tehdidin gözle görülemez bir yapıya sahip olması nedeniyle tehdidin anlatımında/tanımlanmasında zorluk yaşandığı anlaşılmaktadır. Bu niteliğin siber tehdidin diğer tehditlere oranla daha az önemsenmesine yol açmaktadır. Bu durumun ittifak üyeleri için de geçerli olduğunu söylemek yanlış olmayacaktır. Haziran 2011 siber savunma politikasında derinlemesine NATO'nun politikaları irdelenmiştir. Bu siber savunma politikası başlıca noktaları NATO Kamu diplomasisi bölümünün çıkardığı bir kitapçıkta şöyle özetlenmiştir:

- Siber savunma konusu NATO yapısına entegre edilmelidir. NATO'nun ortak güvenlik ve kriz yönetimi gibi temel görevlerinin planlamasında siber savunma da yer almalıdır.
- NATO, üyelerinin kritik siber varlıklarını hedef alabilecek saldırıyı önlemeye, hızlıca toparlanabilmeye (*resilience*) ve savunmaya odaklanmalıdır.
- Güçlü bir siber savunma kapasitesi geliştirilmeli ve NATO'nun kendi ağlarını koruması merkezileştirilmelidir.
- Ulusal kritik ağları korumada asgari gerekler sağlanmalıdır.
- NATO ittifak üyelerine asgari seviyede siber savunma yapabilmek için gerekli yardımı sağlayarak, ulusal kritik altyapıların zayıflıklarını gidermelidir.
- Uluslararası organizasyonlar, özel sektör ve akademik dünyadan ortaklarla bağlantı kurulmalıdır.[67]

NATO'nun oluşturduğu politikalar, ittifakı ve üyelerinin tamamını siber tehditlerden uzakta tutmaya yetmemektedir. NATO web sunucularına ideolojik sebeplerle saldırılar düzenlenmektedir. Bunun en yeni örneklerinden biri, sıfır gün açığı (*zer0 day exploit*) kullanan *Inj3ct0r Takımı*'nın ana web sitesini (dolayısıyla sunucusunu) ele geçirmesidir. Grup, bilgisayar korsanlığını ispat etmek için gelişigüzel 2.646 dosyayı kopyalamıştır. Daha da ileri giderek sunucunun üzerindeki programın ayarlarının bulunduğu dosyaları da internete yüklemiştir. Grup saldırının sebebini nükleer silahların

---

65 İbid.

66 "Lisbon Summit Declaration, 20 Nov. 2010", http://www.nato.int/cps/en/natolive/official_texts_68828.htm, (Erişim Tarihi 16 Aralık 2011).

67 "Defending the Networks: The NATO Policy on Cyber Defence", NATO Public Diplomacy Section, 4 Ekim 2011, http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf (Erişim Tarihi 15 Aralık 2011).

geliştirilmesi ve finanse edilmesi olarak açıklamaktadır.[68] NATO'ya karşı yapılan buna benzer saldırılar günden güne artmaktadır. Genellikle zarar gören kurumlar itibarlarını korumak amacıyla yapılanları saklamayı tercih ettikleri için açığa çıkmasa da medya tarafından ortaya çıkarılandan daha fazla sayıda siber saldırı yapılmaktadır.

NATO ve Siber Geleceği

Bütün bu çalışmalara rağmen NATO Merkezi Karargâhı'nda ve ittifak üyesi ülkelerde siber güvenlik önlemlerini almanın kolay olmadığı ortadadır. 1999 yılından bugüne farklı seviyelerde ve değişik anahtar kelimelerle tartışılan siber güvenliğin tam anlamıyla gerçekleştirilmesi kolay değildir. Bu zorluk ve sürecin zaman alıyor olması, NATO'nun Hibrit Savaş Stratejisi'ni uygulamaya geçirmesini ötelemektedir. Konvansiyonel taktikler açısından uzmanlaşma ve hızlı intikal beklentilerinin cevaplanması önemlidir. Siber savunma kavramı ise konvansiyonel savaş taktiklerine göre şekillendirilmiş ordular için yeni bir alandır ve farklı yaklaşımları gerektirmektedir. Siber savunma stratejisine geçişin önündeki en büyük yanılgı, NATO merkez karargâhlarının biçimlendirdiği bir stratejinin ittifakın bütün üyeleri tarafından hemen kabul edildiği yanılgısıdır. Üye ülkeler kendi özelliklerine göre farklı biçimlerde dirençler göstermektedir. Günümüzde genel kabul görmüş birçok teknolojinin ilk aşamada ihmal edildiği ve kullanılmadığı akılda tutulmalıdır. Günümüzde yaygın olarak kullanılan denizaltıların, deniz muharebesinde kullanılmaya başlandığı günlerde her ülkenin aynı hızla bu teknolojiyi kucaklamadığı örnek olarak verilebilir.[69] Öte yandan, NATO'nun stratejik kararlarının politik olarak kabul edilmesinin, uygulamanın hızla gerçekleşeceği garantisini veremediği de unutulmamalıdır. NATO'nun merkezindeki gelişimin hızıyla ittifak üyelerindeki değişimin hızı birbirinden farklıdır. Bu ikili yapının tamamını kapsayacak bir değişim, düşünülenden daha uzun bir zamana yayılabilir. Konuya siber güvenlik açısından bakıldığında, NATO'nun üyeleri arasında dijital bir bölünmüşlük olduğu açıkça görülmektedir. Bir yanda *Echelon*[70] gibi gelişmiş sinyal izleme sistemleri kullanan siber ordulara[71] sahip ABD ve İngiltere gibi ülkeler yer alırken diğer tarafta dijital yarışta çok geride bulunan Romanya, Bulgaristan, Litvanya ve Çek Cumhuriyeti gibi ülkeler bulunmaktadır.[72] Etkin ve başarılı bir siber savunma stratejisinin uygulanması ancak bu iki grup arasındaki dijital farkın giderilmesi halinde söz konusu olabilecektir. Dolayısıyla NATO'nun kapsamlı ve etkin bir siber savunma stratejisini tam anlamıyla uygulayabilmesi ve Hibrit Savaş kavramını yürütebilmesi tahmin edilenden daha uzun bir süre zarfında olabilecektir.

---

68 "NATO Server Hacked by 1337day Inj3ct0r and Backup Leaked!" http://thehackernews.com/2011/07/nato-server-hacked-by-1337day-inj3ct0r.html, (Erişim Tarihi 18 Aralık 2011).

69 Holger Herwig, "Innovation Ignored: The Submarine Problem-Germany, Britain, and the United States, 1919–1939", Murray Williamson ve Allan R. Millett (Der.) Military Innovation in the Interwar Period, Cambridge, Cambridge University Press, 1996, s.227–24.

70 Steve Wright, "The ECHELON Trail: An Illegal Vision", Surveillance & Society, Cilt 3, No.2/3, 2005, s.198–215.

71 Detaylı bilgi için bakınız http://www.arcyber.army.mil/index.html, (Erişim Tarihi 21 Aralık 2011).

72 Jan A.G.M. van Dijk, "One Europe, Digitally Divided", Andrew Chadwick ve Philip N. Howard (Der.), Routledge Handbook of International Politics, Oxon, 2009, s.288–304.

NATO'nun siber savunma konusunda hızla ilerlemesinin önündeki engellerden bir diğeri de tehdidin niteliğidir. Tehdidin neredeyse her gün değişikliğe uğrayan niteliği ona karşı alınacak tedbirlerin de dinamik olmasını gerektirmektedir. Bu durum, siber tehdidi diğer tehditlerden farklılaştırarak sürekli takip ve izlemeyi gerektirmektedir. Bu türde bir faaliyetin gerektirdiği enerjinin miktarı ve devamlılık gereği maliyetleri de artırmaktadır. Siber tehdidin nispeten görünmez oluşu da tehdidin algılanmasında bir takım yanılgıların doğmasına yol açmaktadır. Dolayısıyla böyle bir tehdidi anlayabilmek ve değerlendirmek için siber dünyanın işleyişini yakından anlamış olmak gerekmektedir. Bu durum NATO merkez karargâhında çalışanların bilgisayar erişimine ne düzeyde sahip oldukları ve siber dünyayı nasıl algıladıkları ile yakından ilgilidir.[73] Gelecek neslin bilgi teknolojileri kaynaklı tehditleri daha iyi anlaması muhtemeldir.

Tehdidi oluşturan teknolojinin üretiminin çoğunluğu özel sektör tarafından yapılmaktadır. Dolayısıyla ürünlerdeki hatalar siber savunmanın zayıflığı olarak görülebilmektedir. Bu nedenle NATO'nun özel sektörle sıkı bir iletişim içinde olması gerekmektedir. Siber güvenliği geleneksel askeri stratejilerden ayıran en önemli unsur sistemdeki aktörlerin hepsinin[74] işbirliğine ihtiyaç duyulmasıdır. Estonya örneğinde görüldüğü gibi saldırı sadece askeri hedeflere yönelmemektedir. Saldırılar 1999 yılındaki Sırp saldırıları örneğinde olduğu gibi NATO üyelerinin hazırlıksız oldukları alanları hedeflemektedir. Bu yüzden ittifak üyelerinin kendi içlerinde de işbirliği ve koordinasyonu sağlaması hayati önem taşımaktadır. Bütün bu yapılanmalara ve gelişmelere rağmen tehdidin varlığını sürdürmesinin nedeni ise asimetrik oluşudur. Saldırı yapıldıktan sonra saldırganların hızla izlerini silebiliyor olması, tehdide verilecek karşılığın hız konusunda ipucu sağlamaktadır. Günümüzün yapılanmayla hem NATO hem de üye ülkeler seviyesinde siber saldırılara ve suçlularına hızla cevap vermek mümkün gözükmemektedir. Belki de gelecek strateji belgelerinde NATO'ya bağlı olarak hareket eden ama yarı-bağımsız ya da asimetrik harekâta göre eğitilmiş siber askerlerin yetiştirilmesi söz konusu olacaktır. Böylece simetrik ordunun, asimetrik yetenekler kazanarak asimetrik tehdide cevap vermesi mümkün olacaktır. NATO'nun ancak büyük imkânlar sağlayarak yetiştireceği bu elemanlara daha fazla gelir fırsatı sunacak güvenlik ve teknoloji firmalarının var olacağı da unutulmamalıdır. Gelişmelere yakından bakıldığında, NATO'nun siber savunma stratejisinin geleneksel savaş kavramına paralel olarak geliştiği görülmektedir. Görünen o ki gelecekteki çatışmalar Hibrit Savaş düzleminde gerçekleşecektir. NATO 1999 saldırısından bu yana bu alanda çok yol almıştır. Ancak siber dünyanın ve teknolojinin gelişimiyle kıyaslanarak incelendiğinde, NATO'nun siber savunma kapasitesinin gelişim hızının daha da arttırması gerektiği ortadadır.

---

[73] NATO yaş ortalaması için bakınız; "Age Groups in NATO Headquarters International Staff 2009", www.nato.int/nato.../20100625_PDF_Library_-_Age_Groups_in_NATO_HQ_2009.pdf (Erişim Tarihi 15 Aralık 2011).

[74] Alt yapı için çalışan kurumların tümü, belediyeler, finans kuruluşları, eğitim kurumları, fabrikalar, teknolojik alt yapı sağlayıcıları, vb.

Kaynakça

"An Alliance for the 21st Century' Washington Summit Communiqué issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Washington, D.C. on 24th April 1999" http://www.nato.int/cps/en/natolive/official_texts_27440.htm (Erişim Tarihi 13 Aralık 2011).

"Age Groups in NATO Headquarters International Staff 2009", www.nato.int/nato.../20100625_PDF_Library_-_Age_Groups_in_NATO_HQ_2009.pdf (Erişim Tarihi 15 Aralık 2011).

Bendrath, Ralph. "The American Cyber-Angst and the Real World – Any Link?", Robert Latham (Der.), *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, New York, The New Press, 2003.

Booth, Ken. "New Wars for Old", *Civil Wars*, Cilt 4, No.2, 2001, s.163–170.

Booth, Ken. "Security and Emancipation", *Review of International Studies*, Cilt 17, No.4, 1991, s.313–326.

Booth, Ken (Der.), *Statecraft and Security:The Cold War and Beyond*, Cambridge University Press, Cambridge, 1998.

Borger, Julian. "Pentagon Kept the Lid on Cyberwar in Kosovo" *The Guardian*, 9 Kasım 1999, http://www.guardian.co.uk/world/1999/nov/09/balkans (Erişim Tarihi 11 Aralık 2011).

"Bucharest Summit Declaration 03 Nisan 2008", http://www.nato.int/cps/en/natolive/official_texts_8443.htm (Erişim Tarihi 16 Aralık 2011).

Buzan, Barry. "Rethinking Security After the Cold War", *Cooperation and Conflict,* Cilt 32, No.1, 1997, s.5–28.

Copeland, Thomas. "Is the 'New Terrorism' Really New?: An Analysis of the New Paradigm for Terrorism", *The Journal of Conflict Studies*, Cilt 21, No 2, Kış 2001, s.7-27.

"Defending the networks The NATO policy on Cyber Defence", NATO Public Diplomacy section, 4 Ekim 2011, http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf (Erişim Tarihi 15 Aralık 2011).

Der Derian, James. "Virtuous War/Virtual Theory", *International Affairs* (Royal Institute of International Affairs 1944-), Cilt 76, No.4, Ekim 2000, s.771–788.

Dijk, Jan A. G. M. Van. "One Europe, Digitally Divided", Andrew Chadwick ve Philip N. Howard (Der.), *Routledge Handbook of International Politics*, Oxon, 2009.

Duffield, John S. "NATO's Functions after the Cold War", *Political Science Quarterly*, Cilt 109, No.5, Kış 1994–1995, s.763–787.

Duyvesteyn, Isabelle. "How New is the New Terrorism?", *Studies in Conflict & Terrorism*, Cilt 27, No.5, 2004, s.439–454.

Ernsdorff, M. ve A. Berbec. "Estonia: The Short Road to E-government and E-democracy", P. Nixon ve V. Koutrakou (Der.), *E-government in Europe*. Abingdon, Routledge. 2007, s.171–183.

Grieco, Joseph M. "Anarchy and the Limits of Cooperation", *International Organization*, Cilt 42, Yaz 1988, s.485–507.

Gorman, Siobhan. "Hackers Stole IDs for Attacks" *The Wall Street Journal*, http://online.wsj.com/article/SB125046431841935299.html (Erişim Tarihi 18 Aralık 2011).

Holger, Herwig. "Innovation Ignored: The Submarine Problem - Germany, Britain, and the United States, 1919–1939", Murray Williamson ve Allan R. Millett (Der.) *Military Innovation in the Interwar Period*, Cambridge, Cambridge University Press, 1996.

Hughes, Rex B. "NATO and Cyber Defence : Mission Accomplished?", *Atlantisch Perspectief*, Cilt 1, No.4, Nisan 2009, http://www.carlisle.army.mil/dime/getDoc.cfm?fileID=212 (Erişim Tarihi 11 Aralık 2011).

Kaldor, Mary. *New and Old Wars. Organized Violence in a Global Era*, Cambridge, Polity Press, 1998.

Kerem, Katri. *Internet Banking in Estonia*, Tallinn, Praxis Center for Policy Studies, 2003.

Klimburg, Alexander. "Mobilising Cyber Power", *Survival*, Cilt 53, No.1, 2 s.41–60.

"Lisbon Summit Declaration, 20 November 2010", http://www.nato.int/cps/en/natolive/official_texts_68828.htm (Erişim Tarihi 16 Aralık 2011).

Mattelart, Armand. *Mapping world communication: War, Progress, Culture*, Minneapolis, University of Minnesota, 1994.

McCalla, Robert B. "NATO's Persistence after the Cold War. (North Atlantic Treaty Organization)", *International Organization*, Cilt 50, No.3, Yaz 1996, s.445–475.

Messmer, Ellen. "Serb Supporters Sock it to NATO, U.S. Web Sites", http://articles.cnn.com/1999-04-06/tech/9904_06_serbnato.idg_1_nato-personnel-nato-headquarters-nato-sources?_s=PM:TECH (Erişim Tarihi 12 Aralık 2011).

Ministries of Defense of Estonia, Latvia and Lithuania "Defense Policies'07 in Brief: Estonia, Latvia and Lithuania", *Baltic Security and Defense Review*, Cilt 10, 2008.

Myrli, Sverre (Norway)-Rapporteur. "173 DSCFC 09 E bis - NATO and Cyber Defence", http://www.nato-pa.int/default.Asp?SHORTCUT=1782 (Erişim Tarihi 16 Kasım 2011).

"NATO 2020:assured security; dynamic engagement", http://www.nato.int/strategic-concept/expertsreport.pdf (erişim tarihi 18.12.2011)

"NATO agrees common approach to cyber defence", http://www.euractiv.com/infosociety/nato-agrees-common-approach-cyber-defence/article-171377 (Erişim Tarihi 17 Aralık 2011).

"NATO Server Hacked by 1337day Inj3ct0r and Backup Leaked!" http://thehackernews.com/2011/07/nato-server-hacked-by-1337day-inj3ct0r.html (Erişim Tarihi 18 Aralık 2011).

Nissenbaum, Helen. "Where Computer Security meets National Security," *Ethics and Information Technology*, Cilt 7, 2005, s.61–73.

Nuttall, Chris. "Net Warfare over Kosovo" http://news.bbc.co.uk/2/hi/science/nature/200069.stm (Erişim Tarihi 12 Aralık 2011).

Paul, T. V. *Asymmetric Conflicts: War Initiation by Weaker Powers*, Cambridge, Cambridge University Press, 1994.

Petit, Brian S. "Chechen Use of The Internet in The Russo-Chechen Conflict." Yayınlanmamış Yüksek Lisans Tezi, the U.S. Army Command and General Staff College Fort Leavenworth, Kansas, 2003.

Riga Summit Declaration, 29 Kasım 2006, http://www.nato.int/docu/pr/2006/p06-150e.htm (Erişim Tarihi 10 Kasım 2011).

Rusling, Matthew. "Shifting Gears For the Military, A Future of 'Hybrid' Wars", *National Defense*, Eylül 2008, s.32–34.

Ruus, Kertu. "Cyber War I: Estonia Attacked from Russia", *European Affairs*, Cilt 9, No 1, Kış/Bahar 2008, http://www.europeaninstitute.org/2007120267/Winter/Spring-2008/cyber-war-i-estonia-attacked-from-russia.html (Erişim Tarihi 18 Aralık 2011).

Sarkar, Rumu. *A Fearful Symmetry: The New Soldier in the age of Asymmetric Conflict*, California, Praeger, 2010.

Schröfl, Josef, Bahram M. Rajaee ve Dieter Muhr (Der.). *Hybrid and Cyber War as Consequences of the Asymmetry: A Comprehensive Approach Answering Hybrid Actors and Activities in Cyberspace : Political, Social and Military Responses*, New York, Peter Lang Pub Inc, 2011.

"Serbian cyber attack may spread," http://www.mail-archive.com/ctrl@listserv.aol.com/msg10035.html (Erişim Tarihi 12 Aralık 2011).

"Strasbourg / Kehl Summit Declaration, 04 Nisan 2009", http://www.nato.int/cps/en/natolive/news_52837.htm?mode=pressrelease (Erişim Tarihi 19 Aralık 2001).

The Alliance's New Strategic Concept, 07 Kasım 1991–08 Kasım 1991, http://www.nato.int/cps/en/natolive/official_texts_23847.htm (Erişim Tarihi 03 Aralık 2011).

The Alliance's Strategic Concept, 24 Nisan 1999, http://www.nato.int/cps/en/natolive/official_texts_27433.htm (Erişim Tarihi 12 Aralık 2011).

"The Prague Summit and NATO's Transformation, NATO, 2003" http://www.nato.int/docu/rdr-gde-prg/rdr-gde-prg-eng.pdf (Erişim Tarihi 14 Aralık 2011).

Traynor, Ian. "Russia accused of unleashing cyberwar to disable Estonia", *The Guardian*, 17 Mayıs 2007, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia (Erişim Tarihi 17 Aralık 2011).

Verton, Dan. "Serbs Launch Cyberattack on NATO", *Federal Computer Week*, http://fcw.com/articles/1999/04/04/serbs-launch-cyberattack-on-nato.aspx (Erişim Tarihi 12 Aralık 2011).

Wright, Steve. "The ECHELON Trail: An Illegal Vision", *Surveillance & Society*, Cilt 3, No.2/3, 2005, s.198–215.

"162 CDS 07 E rev 1 - The Protection of Critical Infrastructures", http://www.nato-pa.int/default.asp?SHORTCUT=1165 (Erişim Tarihi 16 Aralık 2011).

"173 DSCFC 09 E bis - NATO and Cyber Defence", 2009, http://www.nato-pa.int/default.Asp?SHORTCUT=1782 (Erişim Tarihi 13 Aralık 2011).