Cyber Threats Against the North Atlantic Treaty Organization (NATO) and Selected Responses

Dean C. ALEXANDER*

Abstract

This article focuses on the disparate cyber threats against the North Atlantic Treaty Organization (NATO), its members, and selected NATO responses to such perils. Prior to doing so, the article shares various definitions and designations of cyber dangers. Next, the piece provides an in-depth discussion of the nature and types of cyber threats. Subsequently, a discussion of the types of individuals, organizations, and nations pursuing offensive cyber measures takes place.

Keywords: NATO, cyber terrorism, cyber espionage, cyber warfare, cyber crime

Kuzey Atlantik Antlaşması Örgütü'ne (NATO) Karşı Siber Tehditler ve Seçilmiş Yanıtlar

Öz

Bu makale, Kuzey Atlantik Antlaşması Teşkilatı (NATO), NATO üyeleri ve NATO'nun bazı siber tehlikeler ile ilgili yaptığı müdahalelere karşı yapılan benzeşmeyen, farklı siber tehditlere odaklanmaktadır. Bunu yapmadan önce, makale, siber tehlikeler ile ilgili çeşitli tanımlamalar ve belirlemeler anlatmaktadır. Daha sonra, makale, siber tehditlerin doğası ve çeşitleri ile ilgili geniş kapsamlı bir tartışma ortaya koymaktadır. Akabinde, makalede, taarruzi siber tedbirler arayışındaki bireyler, organizasyonlar ve milletler çeşitleri ile ilgili bir tartışma yer almaktadır.

Anahtar Kelimeler: NATO, siber terörizm, siber ispiyonculuk, siber savaş, siber suç.

* Assoc. Prof. Dr., Director of Homeland Security Research Programme, Western Illinois University. E-mail: deancalexander2011@gmail.com

I. Cyber Threat Terminology

A central feature of the cyber revolution is the lack of unanimity as it relates to certain terminology. From a geo-political perspective, the five leading harmful activities in cyber-space are: cyber espionage, cyber crime, cyber terrorism, cyber attacks, and cyber warfare, each with its own motivations and goals, although sometimes overlap exists.[1]

"Cyber crime is a crime enabled by or that targets computers."[2] Cyber crime can involve the theft and damage of property as well as fraudulent and espionage-related activities.[3]

A cyber attack (or computer network attack) can disrupt computer equipment and hardware reliability, change computer-processing logic, steal or corrupt data.[4] Cyber espionage is the use of computer systems or information technology to illegally obtain confidential/secret information from the government, private sector, or some other entity.[5]

The objectives of a cyber attack include the: loss of integrity, availability, confidentiality, and physical destruction.[6] Cyber attacks most frequently target critical infrastructure (financial services, manufacturing, telecommunications, electricity, water).[7] However, they increasingly inflict damage on government targets, including the military, intelligence, and law enforcement.[8]

---

[1] Wilson, C. (2008, Jan. 29). *Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for Congre ss.* Congressional Research Service. Retrieved from http://www.au.af.mil/au/awc/awcgate/crs/rl32114.pdf

[2] Ibid.

[3] Doyle, C. (2010, Dec. 27). *Cybercrime: An overview of the federal computer fraud and substance abuse statute and federal criminal laws*, Congressional Research Service. Retrieved from http://www.fas.org/sgp/crs/misc/97-1025.pdf

[4] Wilson, *supra* note 1.

[5] *Cyber Security: a Part 3 Definition.* (n.d.). Palo Alto Networks. Retrieved from http://www.paloaltonetworks.com/community/learning-center/what-is-cyber-security.html

[6] *U.S. Army Training and Doctrine Command, Cyber Operations and Cyber Terrorism Handbook.* No. 1.02, P.II-1 and II-3. (2005, Aug. 15). Retrieved from http://www.au.af.mil/au/awc/awcgate/army/guidterr/sup2.pdf

[7] McAfee. (2009). *In the Crossfire: Critical Infrastructure in the Age of Cyber War.* Retrieved from http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf ; Amoroso, E. (2010). *Cyber Attacks: Protecting National Infrastructure.* Oxford, UK: Butterworth-Heinemann.

[8] Ibid.; Olsen, K. (2009, July 9). *Massive cyber attack knocked out government websites starting on July 4th.* Retrieved from http://www.huffingtonpost.com/2009/07/07/massive-cyber-attack-knoc_n_227483.html

Cyber terrorism is unlawful attacks and threats of attack against computers, networks, and information stored therein—carried out through the computers, Internet, or the use of flash drive storage devices—when done to intimidate or coerce a government or its people in furtherance of political or social objectives.[9]

Cyber terrorism has also been used to describe radicalization, recruitment, propaganda, command and control, financing, and other activities conducted by terrorists on the Internet.[10] To some, "true" cyber terrorism requires substantial physical damage so political protesting using the Internet is simply "hacktivism," and not cyber terrorism.[11]

Cyber terrorism, like terrorism, has been defined in a variety of different, sometime contradictory ways. Some view it as simply a modality or means of attack by a terrorist group or terrorists. For others, cyber terrorism is a distinct, separate form of terrorism. Also, cyber terrorism has been classified according to two features: target-oriented (or attack) cyber terrorism and tool-oriented cyber terrorism.[12]

The main difference between a cyber attack and cyber terrorism is the intent of the perpetrator. The person undertaking a cyber attack may have a financial or other motive (political). The cyber terrorist's motive is always political, social, or religious in nature. The metaphysical activity of both may be exact, but the rationales are distinct.

---

[9] Wilson, *supra* note 1; Tafoya, W. (2011, Nov.). *Cyber Terror*. FBI Law Enforcement Bulletin. Retrieved from http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/cyber-terror

[10] UN Office on Drugs and Crime. (2012, Sept.). *The use of the Internet for terrorism purposes*. Retrieved from http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf; Charvart, P. *Cyber terrorism: A new dimension in battlespace*. (n.d.). NATO Cooperative Cyber Defence, Centre of Excellence. Retrieved from http://www.ccdcoe.org/publications/virtualbattlefield/05_CHARVAT_Cyber%20Terrorism.pdf ; Alexander, D. (2010, July). *The radicalization of extremists/terrorists - why it affects you*. Security Magazine. Retrieved from http://digital.bnpmedia.com/publication/?i=41296&p=42

[11] Ibid.; Denning, D. (2009). *Terror's web: How the Internet is transforming terrorism.* Handbook on Internet Crime (Y. Jewkes and M. Yar, eds.), Willan Publishing. Retrieved from http://faculty.nps.edu/dedennin/publications/Denning-TerrorsWeb.pdf

[12] Ibid.; Ottis, R. & P. Lorents. (n.d.). *Cyberspace: definition and implications*. Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia. Retrieved from www.ccdcoe.org/articles/.../Ottis_Lorents_CyberspaceDefinition.pdf; Taliharm, A.M. (2010, Fall). *Cyberterrorism: In theory or in practice?* Defence Against Terrorism Review. 3 (2). pp. 59-71. Retrieved from http://www.coedat.nato.int/publications/datr6/DATR_Fall2010_.pdf

Cyber threats requires less personal contact, less need for formal organization, and no need for control over a geographical territory from which to undertake activities.[13] Concurrently, organized crime and terrorists are recruiting technology savvy individuals to join their groups.[14]

Cyber is the fifth domain of the battlefield after air, land, sea, and space.[15] Cyber warfare is utilizing computers and other instruments to target an enemy's information systems rather than attacking an enemy's armies or factories.[16]

Some analysts argue that a cyber attack only qualifies as an act of cyber warfare under the war of armed conflict (LOAC) standard if: it is done in conjunction with a physical attack; is attributable to a specific government; and the attack causes injury.[17] Under such a guideline, the 2008 cyber attacks against Georgia did not constitute cyber warfare.[18]

Information warfare is "combat operations in a high-tech battlefield environment in which both sides use information technology means, equipment, or systems in a rivalry over the power to obtain, control, and use information."[19] The utility of information systems rests on their

---

[13] McCusker, R. (2006). *Transnational organised cyber crime: distinguishing threat from reality*. Crime, Law and Social Change, 46 (4-5), pp. 257-273. Retrieved from http://tees.openrepository.com/tees/bitstream/10149/115450/2/115450.pdf

[14] Thachuk, K. (2008, Spring). Countering terrorist support structures. Defence Against Terrorism Review. 1 (1), pp. 13-28. Retrieved from http://www.coedat.nato.int/publications/datr/02.Kimberley%20THACHUK.pdf; Bucci, S. (2009, June 12). The confluence of cyber crime and terrorism. Lecture #1123, Heritage Foundation. Retrieved from http://www.heritage.org/research/lecture/the-confluence-of-cyber-crime-and-terrorism

[15] *War in the fifth domain*. (2010, July 1). The Economist. Retrieved from http://www.economist.com/node/16478792 ; Wagensall, P. (2011, Feb. 16). *Cyberwarfare called the fifth domain of battle by pentagon.* Technewsdaily.com. Retrieved fromhttp://www.technewsdaily.com/6620-cyberwarfare-called-fifth-domain-of-battle-by-pentagon.html

[16] Definition of cyberwarfare (n.d.). Retrieved from http://dictionary.reference.com/browse/cyberwarfare

[17] Carr, J. (2011, Aug. 12). *What is cyberwar?* Slate.com. Retrieved from http://www.slate.com/articles/technology/future_tense/2011/08/what_is_cyber_war.html; Apps, P. (2012, Feb. 3). Cyber security specialist: disagreements over hacking risk could mean digital 'cold war'. Retrieved from http://www.huffingtonpost.com/2012/02/03/cyber-security-risk_n_1252889 .html

[18] Ibid.

[19] Baocun, W. and Fei, L. (1995, June 13/20). *Information Warfare.* Chinese Academy of Military Science. Retrieved from http://www.fas.org/irp/world/china/docs/iw_wang.htm

availability, integrity, and security.[20] Electronic warfare, information warfare, and cyber warfare are often used synonymously.[21]

The differences among cyber crimes, cyber espionage, cyber warfare, and cyber terrorism are increasingly blurred.[22] The manifold perpetrators of such activities—individuals, diverse ideological groups, and countries—complicate defensive and offensive measures against such threats.

II. Nature and Types of Cyber Threats

A. Overview

In March 2012, FBI Director Robert Mueller stated that cyber threats would be the principal threat facing the United States.[23] Similarly, in September 2011, U.S. Defense Secretary Leon Panetta designated cyber as a future battlefield.[24]

In terms of preparation, Sen. Joe Lieberman, Chairman, U.S. Homeland Security and Government Affairs Committee described the readiness of the United States relative to cyber threats as unprepared, and akin to the September 11 attacks in failing to connect the dots.[25]

In July 2002, a U.S. Naval War College war game, termed "Digital Pearl Harbor," developed a scenario of a multifaceted cyber terrorism incident. "The result projected that the most vulnerable infrastructure computer systems were the Internet itself, and the computer systems that are part of the financial infrastructure."[26] Some predict a cyber version of

---

[20] Jajodia, S. et al. (1999, Apr.). *Surviving information warfare attacks*. Mitre. Retrieved from http://www.mitre.org/work/best_papers/99/jajodia_surviving/jajodia_surviving.pdf
[21] Tafoya, *supra* note 9.
[22] Masters, J. (2011, May 23). Confronting the cyber threat. Council on Foreign Relations Backgrounder. Retrieved from http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577
[23] Mueller III, R. (2012, Mar. 1). Speech at RSA cyber security conference. FBI press release. Retrieved from http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies
[24] Pellerin, C. (2011, Sept. 14). *Panetta: Regional defense, cyber highlight AUSMIN talks.* American Forces Press Service. Retrieved from http://www.defense.gov/News/NewsArticle.aspx?ID=65337
[25] Choinere, P. (2012, Mar. 11). *Lieberman warns of a cyber 9/11.* Retrieved from http://www.theday.com/article/20120311/OP04/303119943
[26] Wilson, *supra* note 2, at 21.

an "Armageddon," namely, a "Cybergeddon," which would unleash crippling cyber attacks globally.[27]

Among the possible cyber attack scenarios include the take over of air traffic control systems of airports, which could bring down hundreds of planes.[28] Similarly, railway traffic systems or nuclear energy plants could be subject to cyber attacks.[29]

Cyber security risks have increased for infrastructure control systems because of the persistence of interconnections with the Internet, and continued open availability of detailed information on the technology configuration of the control systems, including energy and water plants, among others.[30]

"[T]here are 2,000 to 3,000 successful hacker attacks on computers throughout the world on any given day, with an estimated 60 percent of sites vulnerable to cyber vandalism."[31] The number of network incidents at U.S. government agencies has increased over 650%between 2006 and 2011.[32]

Unfortunately, cyber threats are not new. In 2003, the Slammer computer worm infected "more than 90 percent of vulnerable hosts within

---

[27] Glenny, M. (2010, May 24). *The countdown to cybergeddon*. FT.com. Retrieved from http://www.ft.com/cms/s/0/47b390e4-66ca-11df-aeb1-00144feab49a.html#axzz2T6t8My9N

[28] Newton, S. (2001, Nov.). *Can cyberterrorists actually kill people?* SANS Institute. Retrieved from http://www.sans.org/reading_room/whitepapers/warfare/cyberterrorists-kill-people_820

[29] Waugh, R. (2011, Dec. 29). *Computer hackers 'could bring rail network to a standstill' warns security expert – but would we even notice?* Daily Mail. http://www.dailymail.co.uk/sciencetech/article-2079449/Computer-hackers-bring-rail-network-standstill-warns-security-expert--notice.html

[30] *Executive order - - Improving critical infrastructure cybersecurity*. (2013, Feb. 12). Office of the Press Office, White House. Retrieved from http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity; *Examining the cyber threat to critical infrastructure and the American economy*. (2011, Mar. 16). Subcommittee on cyber security, infrastructure protection, and security technologies, Committee on homeland security, U.S. House of Representatives. Retrieved fromhttp://www.gpo.gov/fdsys/pkg/CHRG-112hhrg72221/html/CHRG-112hhrg 72221.htm

[31] Hellman, Z. (2012, Feb. 22). *Hackers or terrorists*. Jpost.com. Retrieved from http://m.jpost.com/Headlines/Article.aspx?id=86258350&cat=2

[32] *Cyber attacks against US government growing at rapid pace* (n.d.). Secure128.com. Retrieved from http://www.secure128.com/cyber-attacks-against-us-government-growing-at-rapid-pace.aspx; Hosenball, M. and Zengerle, P. (2013, Mar. 12). *Cyber attacks leading threat against U.S.: Spy agencies*. Reuters.com. Retrieved from http://www.reuters.com/article/2013/03/12/us-usa-threats-idUSBRE92B0LS20130312

10 minutes, causing significant disruption to financial, transportation, and government institutions and precluding any human-based response."[33]

In some respects, cyber warfare can often inflict the same type of damage as a conventional war. Cyber technology can do this without shooting a single bullet.[34]

Since 2007, the world has seen several major politically oriented cyber attacks (denial of service attacks) against four former Soviet Union countries: Kyrgyzstan (January 2009), Georgia (August 2008), Lithuania (June 2008), and Estonia (April-May 2007).[35] All four likely originated from Russia, and may have implicitly involved the Kremlin, despite official denials.

Still, there are several difficulties in assessing cyber threats. First, there is the lack of established indicators that would show that an attack is underway. Second, there is an inability to identify who is responsible for the attack. Third, there is a lack of dedicated resources to assist in returning cyber operations to a pre-attack condition.[36]

The ability of countries to assign responsibility for cyber attacks to another nation may lead to a cyber or other retaliation. The retaliation could be characterized as self-defense, if it is proportional and done out of necessity. However, there is still some reticence about responding to a cyber threat with a cyber attack or conventional weapons.[37]

İGÜSBD
Cilt: 1 Sayı: 2
Ekim /
October 2014

---

[33] Moore, D. et al. (2003, July/Aug.). *Inside the slammer worm*. IEEE Security & Privacy, at 33. Retrieved from http://cseweb.ucsd.edu/~savage/papers/IEEESP03.pdf

[34] *War of the worms: cyber-attacks pose increasing danger to Israeli society* (n.d.). Wharton. Retrieved from http://kw.wharton.upenn.edu/israel/war-of-the-worms-cyber-attacks-pose-increasing-danger-to-israeli-security/

[35] Kirk, J. (2007, May 17). *Estonia recovers from massive denial-of-service attack*. Infoworld. Retrieved from http://www.infoworld.com/d/security-central/estonia-recovers-massive-denial-service-attack-188 (hereinafter Kirk 2007); Kirk, J. (2008, July 4). *Lithuania: Attacks focused on hosting company*. PC World. Retrieved from http://www.pcworld.com/article/147960/article.html (hereinafter Kirk 2008) ; Mackey, R., (2009, Feb. 9). *Are 'cyber-militias' attacking Kyrgyzstan?* NY Times. Retrieved from http://thelede.blogs.nytimes.com/2009/02/05/are-cyber-militias-attacking-kyrgyzstan/ ; Markoff, J. (2008, Aug. 13). *Before the gunfire, cyberattacks*. Retrieved from http://www.nytimes.com/2008/08/13/technology/13cyber.html

[36] Rollins, J. and Wilson, C. (2007, Jan. 22). *Terrorist capabilities for cyberattack: Overview and policy issues*. Congressional research service. Retrieved from http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-024.pdf

[37] Graham, D. (2010). *Cyber threats and the laws of war*. 4 Journal of national security law and policy 84. Retrieved from http://jnslp.com/wp-content/uploads/2010/08/07_Graham.pdf; Anderson, R. (n.d.). *Countering state-sponsored cyber attacks: Who should lead?* Information as power. Army War College. Retrieved from

Countries that are unwilling or unable to prevent their territory being used by sub-state groups to launch cyber attacks could be designated as sanctuary states. As such, they might be susceptible to the use of force by a victim state.[38]

B. Botnets

Botnets consist of numerous "compromised computers that have been infected with malicious code, and can be remotely controlled through commands sent via the Internet."[39] These infected computers "can operate concurrently to disrupt or block Internet traffic for targeted victims, harvest information, or to distribute spam, viruses, or other malicious code."[40] Cyber criminals can initiate these disruptive effects in cyberspace by renting botnet services from another cyber criminal.[41] Botnets are becoming the weapon of choice for fraud and extortion.[42]

"Successful botnet development and operations use techniques similar to legitimate businesses, including the involvement of personnel with various specialties, feature-based pricing structures, modularization, and software copy protection. The development and sale of kit-based botnets has made it easier for criminals with limited technical expertise to build and maintain effective botnets."[43]

"Botnet development and management is approached in a business-like fashion. Some criminals rent or sell their botnets or operate them as a specialized portion of an ad hoc criminal organization. At least one botnet kit author implemented a copy protection scheme, similar to major

---

http://www.csl.army.mil/usacsl/Publications/infoaspowervol2/IAP2%20-%20Section%20Two%20%28Anderson%29.pdf ; Grauman, B. (2012, Feb.). *Cyber-security: the vexed question of global rules*. Retrieved from http://www.securitydefenceagenda.org/Contentnavigation/Library/Libraryoverview/tabid/1299/articleType/ArticleView/articleId/3064/SDA-cybersecurity-report.aspx

[38] Anderson, *supra* note 37.

[39] Wilson, *supra* note 1, at 5.

[40] Ibid

[41] Ibid at 6.

[42] Ibid at 6; *Botnets: The new threat landscape white paper*. (n.d.). Cisco. Retrieved fromhttp://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns441/networking_solutions_whitepaper0900aecd8072a537.html

[43] Snow, G. (2011, Apr. 12). *Statement before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism*, at 3. Retrieved from http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism

commercial software releases, which attempts to limit unauthorized use of the botnet kit."[44]

In Spring 2007, government computer systems in Estonia suffered distributed denial-of-service cyber attacks. Botnets were used to essentially over-capacitate Estonian government websites, media channels and the servers of commercial banks. The attacks initially thought to be orchestrated by Russian organized crime and (possibly) the Russian government blurred the boundaries among cyber crime, warfare, and terrorism. Subsequently, NATO and the United States sent experts to aid Estonia recover from the attacks. In 2008, a 20-year-old ethnic Russian Estonian, was fined for attacking an Estonian government website.[45]

In June 2008, Lithuania faced cyber attacks three days after it passed a law outlawing the use of Soviet and communist symbols; over 300 websites were attacked. Some were denial of service attacks while other sites were vandalized with the Soviet hammer and sickle. Prior to the attacks, relations between Russia and Lithuania had deteriorated.[46]

On July 20, 2008, the website of the Georgian president came under a denial of service cyber attack. The attack shut the website down for 24 hours. On August 8, 2008, a coordinated denial of service attack was made against Georgian government websites at the same time that Russian forces were engaged in combat with Georgian forces. As the ground attacks accelerated, the cyber attacks did as well. This was believed to be the first time that a cyber attack was done concurrently with armed conflict.[47]

---

[44] Ibid

[45] Kirk 2007, *supra* note 37; *Estonia fines man for 'cyber war.' (*2008, Jan. 25). BBC news, Retrieved from http://news.bbc.co.uk/2/hi/technology/7208511.stm; Traynor, I. (2007, May 16). *Russia accused of unleashing cyberwar to disable Estonia*. The Guardian. Retrieved from http://www.guardian.co.uk/world/2007/may/17/topstories3.russia **;** Tikk, E. et al. (2010). International cyber incidents legal considerations. Cooperative Cyber Defence Centre of Excellence. Retrieved from http://www.ccdcoe.org/publications/books/legalconsiderations.pdf

[46] Tikk, *supra* note 45; Lithuanian tax office website hit by cyber attack. (2008, July 21). Reuters. Retrieved from http://www.reuters.com/article/2008/07/21/lithuania-web-attacks-idUSMAR14153920080721; Rhodin, S. (2008, July 1). *Hackers tag Lithuanian website with Soviet symbols*. NY Times. Retrieved from http://www.nytimes.com/2008/07/01/world/europe/01baltic.html?_r=1&scp=3&sq=lithuania&st=nyt&oref=slogin

[47] Tikk, *supra* note 45; *War redefined*. (2008, Aug. 17). LA Times. Retrieved from http://articles.latimes.com/2008/aug/17/opinion/ed-cyberwar17; Tikk, E. et al. (2008, Nov.). Cyber attacks against Georgia: Legal lessons identified. Cooperative Cyber Defence Centre of Excellence. Retrieved from http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf

On Jan. 18, 2009, Kyrgyzstan's two main Internet servers came under a denial of service attacks shutting down websites and email within the country. The originators of the attacks were tracked back to Russia. The attacks coincided with the Russian government pressuring Kyrgyzstan to stop U.S. access to the airbase in Bishkek.[48]

C. Malicious Code Hosted on Websites and Email

"Malicious code, including viruses or Trojan Horses are used to infect a computer to make it available for takeover and remote control. Malicious code can infect a computer if the user opens an email attachment"[49] or clicks on a link on a website.[50] In 2007, Google reported that millions of web pages contained malicious software.[51]

Identity theft occurs online, inter alia, by individuals clicking on links in email or on websites. "Malicious code can scan the victim's computer for sensitive information"[52] (date of birth, bank account numbers, etc.), which can then be sold online or used for making false identity documents. Also, hackers and insiders (employees) can access sensitive data worldwide.[53]

D. Other Cyber Challenges

The dissemination routes of malicious software are not restricted to networks. Rather, promotional gifts like USB-sticks (jump drives) are given away at trade shows and conferences can contribute to infiltrating systems. A computer virus (e.g., Trojan) can be pre-installed on the USB. By connecting the USB to a computer, the Trojan can become installed on the computer, and subsequently, is secreted into the computer network. Therefore, the threat is injected directly onto the target system or network, bypassing the security system. In by passing the security system is possible due to inattentive employees or malicious workers. USB-sticks (jump drives) can also be used to steal significant amounts of information.[54]

---

[48] Mackey, *supra* note 35; Bradbury, D. (2009, Feb. 4). *The fog of cyberwar*. The Guardian. Retrieved from http://www.guardian.co.uk/technology/2009/feb/05/kyrgyzstan-cyberattack-internet-access ; Ashmore, W. (2009, May 21). *Impact of alleged Russian cyber attacks.* US Army Command and General Staff College. Retrieved from http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA504991

[49] Wilson, *supra* note 1, at 10.

[50] Ibid.

[51] Ibid.

[52] Ibid. at 11.

[53] Ibid.

[54] *Insider security threats: State CIOs take action now*. (2007). National Association of Chief Information Officers of States. Retrieved from

E. Cyber terrorism

Several case studies of cyber terror activities are worth highlighting. In July 2007, UK-based Younes Tsouli, Waseem Mughal, and Tariq Al-Daour, pleaded guilty to inciting another person to commit an act of terrorism outside the UK, which, if committed in the UK, would constitute murder. They also admitted conspiring together and with others to defraud banks, credit card companies, and charge card companies. They ran websites, online forums, produced and distributed online literature and videos in support of violent jihad. They were sentenced as follows: Tsouli (16 years), Mughal (12 years), and al-Daour (10 years).[55]

The three were particularly close to al-Qaeda in Iraq, formerly led by Abu Musab al-Zarqawi. Among the materials they disseminated on the web were graphic videos, including beheadings, and step-by-step procedures on making a suicide bomb vest.[56]

In November 2011, the Turkish Ministry of Finance announced that the PKK terrorist organization attacked its web site www.maliye.gov.tr and injected pro-PKK materials on the web pages.[57]

In 1997, the Internet Black Tigers (of Tamil Tigers) attacked the email systems of several Sri Lankan embassies throughout the world. By flooding these accounts with over 800 emails a day, the IBT was able to disable embassy networks for nearly two weeks. The emails sent by IBT identified the group as of the LTTE, specializing in suicide e-mail bombings.

---

http://www.nascio.org/publications/documents/NASCIO-InsiderSecurity Threats .pdf; Rafter, M. (2010). *New security risks from USB flash drives*. Norton. Retrieved from http://us.norton.com/yoursecurityresource/detail.jsp?aid=usbdrives ; *Social engineering using a USB drive*. (n.d.). Carnegie Mellon University. Retrieved from http://www.cmu.edu/iso/aware/be-aware/usb.html

[55] *British Muslim computer geek, son of diplomat, revealed as al Qaeda's top cyber terrorist*. (2008, Jan. 16). Daily Mail. Retrieved from http://www.dailymail.co.uk/news/article-508543/British-Muslim-geek-son-diplomat-revealed-al-Qaedas-cyber-terrorist.html ; *Three admit inciting terror acts*. (2007, July 4). BBC News. Retrieved from http://news.bbc.co.uk/2/hi/uk_news/6268934.stm ; Whitlock, C. and Hsu, S. (2007, July 6). *Washington Post*. Retrieved from http://www.washingtonpost.com /wp-dyn/content/article/2007/07/05/AR200 7070502120.html

[56] Ibid.

[57] *PKK attacks Turkey's finance ministry website*. (2011, Nov. 9). Today's Zaman. Retrieved from http://www.todayszaman.com/news-262152--pkk-attacks-turkeys-finance-ministry-website.html

The group said the attack was an effort to counter Sri Lankan government propaganda.[58]

III. Who is a Cyber Threat?

İGÜSBD
Cilt: 1 Sayı: 2
Ekim / October 2014

A. Countries, Groups, and Individuals Conducting Cyber Espionage

Cyber espionage includes the unlawful "probing to test a target computer's configuration or evaluate its system defenses, or the unauthorized viewing and copying of data files."[59] The U.S. government estimates that over one hundred foreign intelligence organizations "regularly attempt to hack into the computer systems of the U.S. government and U.S. companies."[60] The majority of cyber attacks against U.S. government systems appear to originate in China.[61]

Foreign collectors of intelligence are particularly interested in U.S. information relating to the following:

- Information and communication technologies
- Business information about natural resources or content related to doing business with U.S. businesses or government
- Military technologies and other aerospace/aeronautics technology
- Civilian and dual-use technologies in emerging industries[62].

B. Cyber terrorists

Terrorist groups can recruit highly skilled hackers (based on ideological and/or financial) to aid them in their prospective cyber terrorist activities.[63] Computer vulnerabilities—including automated bot

---

[58] Daly, J. (2007, June 5). *LTTE: Technologically innovative rebels*. ISN Eth Zurich. Retrieved fromhttp://isn.ch/isn/Digital-Library/Articles/Detail/?ots783=4888caa0-b3db-1461-98b9-e20e7b9c13d4&lng=en&id=53217 ; Puran, R. (2003, Feb. 28). *Beyond conventional terrorism… the cyber assault*. SANS Institute. Retrieved from http://www.sans.org/reading_room/whitepapers/threats/conventional-terrorismthe-cyber-assault_931

[59] Wilson, *supra* note 1, at 12.

[60] Ibid.

[61] Ibid. at 15.

[62] Federal Bureau of Investigation. (2012, May 11). *Economic espionage: how to spot a possible insider threat.* Retrieved from http://www.fbi.gov/news/stories/2012/may/insider_051112/insider_051112

[63] Wilson, C. (2005, Apr. 1). *Computer attack and cyberterrorism: Vulnerabilities and policy issues for Congre ss.* Congressional Research Service at 20. Retrieved from http://www.history.navy.mil/library/online/computerattack.htm; Conway, M. (n.d.). *Hackers as terrorists? Why it does not compute*. Computer Fraud &

networks—are for sale by hackers to the highest bidders, including to terrorists.[64]

It is estimated that advanced cyber attacks against multiple systems and networks might require several years of preparation; those aiming at causing mass disruption against integrated, heterogeneous systems would require even more time.[65] Some studies predict that a significant cyber terror attack will be used in conjunction with a large traditional physical (offline) terrorist attack.[66]

C. Hacktivists

Hacktivist groups, such as Anonymous and LulzSec, undertake protests and commit computer crimes as a collective unit. These groups do not have a leader or a controlling party, but instead rely on the collective power of individual participants. They have members who utilize the Internet to communicate, advertise, and coordinate their actions.[67]

Anonymous describes itself as an online community with the goal of promoting Internet freedom and freedom of speech. Since 2008, it has participated in international hacktivism and protests.[68]

Lulzsec is believed to be a splinter of group Anonymous, though it distances itself from the group. Lulzsec often posts taunting or mocking messages to corporations or agencies they have compromised.[69] Lulzsec

---

Security. Retrieved from http://www.arifyildirim.com/ilt510/maura.conway.pdf ; Charvart, *supra* note 10.

[64] Wilson, *supra* note 1.

[65] Mueller III, *supra* note 23.

[66] Wilson, *supra* note 63 at 17.

[67] Id.; Lewis, J. (2002, Dec.). *Assessing the risks of cyber terrorism, cyber war, and other cyber threats*. Center for Strategic and International Studies at 9.Retrieved from http://www.steptoe.com/publications/231a.pdf

[68] Germany, W. (2012, Feb. 29). *What is 'Anonymous' and How Does it Operate?* Radio Free Europe/Radio Liberty. Retrieved from http://www.rferl.org/content/explainer_what_is_anonymous_and_how_does_it_operate/24500381.html; Sterner, E. (2012, Apr.). *The paradox of cyber protest*. Marshall Policy Institute Outlook. Retrieved from http://www.marshall.org/pdf/materials/1087.pdf ; Krupnick, S. (2011, Aug. 16). *Freedom fighters or vandals? No consensus on Anonymous.* Contra Costa Times. Retrieved from http://www.mercurynews.com/top-stories/ci_18686764 ; Silicon Republic. (2012, Jan. 9). *Anonymous attack reveals US, UK and Nato email passwords*. Retrieved from http://www.siliconrepublic.com/strategy/item/25247-anonymous-attack-reveals-us

[69] Murphy, D. (2011, June 19). *Three reasons to fear Lulzsec: Sites, skills, and slant*. PC Magazine. Retrieved from http://www.pcmag.com/article2/0,2817,2387219,00.asp

ceased operations in June 2011, while several of its leadership was prosecuted.[70]

Wikileaks publishes and comments on leaked documents alleging government and corporate misconduct. The data that Wikileaks releases are often acquired by cyber espionage and other cyber-based methodologies.[71]

D. "Profit-Driven" Cyber Criminals

Some cyber criminals are forming "organized groups to conduct cyber crime. The adoption of specialized skill sets and professionalized business practices by these criminals is steadily increasing the complexity of cyber crime by providing individuals all technical abilities with the necessary tools and resources to conduct cyber crime. Not only are criminals advancing their abilities to attack a system remotely, but also, they are becoming adept at tricking victims into compromising their own systems."[72]

As cyber crime groups increasingly recruit technology-experienced individuals and pool resources and knowledge, they advance their ability to be successful in conducting crimes against more profitable targets. Also, they learn the additional skills necessary to evade the security industry, intelligence community, military, and law enforcement.[73]

E. Nation-States

Over 100 countries are believed to have some cyber threat capabilities.[74] Of particular concern to NATO are Russia and China.[75] The

---

[70] *Kretsinger, Sony hacker Recrusion, jailed for year.* (2013, Apr. 13). BBC News. Retrieved from http://www.bbc.co.uk/news/technology-22214506; Schwartz, M. (2011, June 27). *LulzSec hackers retire: time to rethink risk*. Information Week. http://www.informationweek.com/security/attacks/lulzsec-hackers-retire-time-to-rethink-r/231000472

[71] Spiegel Online International. (n.d.). WikiLeaks *Diplomatic Cables.* Retrieved from *http://www.spiegel.de/international/topic/wikileaks_diplomatic_cables/*

[72] Snow, G. (2011, Sept. 11). *Statement before the House Financial Services Committee*. Subcommittee on Financial Institutions and Consumer Credit. Retrieved from http://www.fbi.gov/news/testimony/cyber-security-threats-to-the-financial-sector

[73] Ibid.

[74] Paganini, P. (n.d.). *The rise of cyber weapons and relative impact of cyber space*. Infosec Institute Resources. Retrieved from http://resources.infosecinstitute.com/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace/

[75] Clapper, J. (2012, Jan. 31). *Unclassified statement for the record on the worldwide threat assessment of the US intelligence community for the Senate Select Intelligence*

Russian government, including its military, will continue to develop systems to improve their offensive and defensive cyber capabilities. Russia is conducting a range of activities, including collecting economic information and technologies from Western countries. Also**,** in 2008, Russian hackers attacked the computer networks with the U.S. military's Central Command, the headquarters that oversees U.S. involvement in Iraq and Afghanistan, and affected computers in combat zones. The attack included penetration of at least one highly classified network.[76]

"[T]he Chinese government, in addition to employing thousands of its own hackers, manages massive teams of experts from academia and industry in cyber militias that act in Chinese national interests with unclear amounts of support and direction from China's People's Liberation Army."[77]

According to some estimates, for over a decade China has tried to steal political, commercial, and security/intelligence information from the West and others. The main protagonists of these activities are believed to be the Third Department of the People's Liberation Army. It is likely that other parts of the Chinese state and even the private sector may be carrying out similar activities.[78]

Committee. Senate Select Intelligence Committee, at 3. Retrieved from http://www.intelligence.senate.gov/120131/clapper.pdf

[76] (2011, Oct.). *Foreign spies stealing U.S. economic secrets in cyberspace.* Office of the National Counterintelligence Executive. Retrieved from http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

[77] Rogin, J. (2010, Jan. 22). *The top 10 chinese cyber attacks that we know of*. Foreign Policy. Retrieved from http://thecable.foreignpolicy.com/posts/2010/01/22/the_top_10_chinese_cyber_attacks_that_we_know_of

[78] Riley, M. & J. Walcott. (2011, Dec. 12). *China-based hacking of 760 companies shows cyber cold war*. Businessweek. Retrieved from http://www.businessweek.com/news/2011-12-22/china-based-hacking-of-760-companies-shows-cyber-cold-war.html ; Rogin, *supra* note 79 ; (2012, Mar. 11). *Hidden Chinese Hackers Crouching Dragon, Stolen Data*. Cyber War Zone. Retrieved from http://www.cyberwarzone.com/cyberwarfare/hidden-chinese-hackers-crouching-dragon-stolen-data?page=4 ; *Chinese cyber-attacks: Hello, Unit 61398*. (2013, Feb. 19). The Economist. Retrieved from http://www.economist.com/blogs/analects/2013/02/chinese-cyber-attacks ; Fox News. (2011, Aug. 3). *Massive global cyberattack targeting U.S., U.N. discovered; experts blame China*. Retrieved from http://www.foxnews.com/scitech/2011/08/03/massive-global-cyberattack-targeting-us-un-discovered-experts-blame-china/ ; Goldman, D. (2011, July 28). *China v. U.S.: The cyber cold war is raging*. Retrieved from http://money.cnn.com/2011/07/28/technology/government_hackers/index.htm; Nakashima, E. (2012, Mar. 7). *China testing cyber-attack capabilities, report says*, Washington Post. Retrieved from http://www.washingtonpost.com/world/national-security/china-testing-cyber-attack-capabilities-report-says/2012/03/07/gIQAcJwDyR_story.html ; *China gone cyber-wild – cyber attacks by China*. (2011, Sept. 23). Retrieved from http://uscyberlabs.com/blog/2011/09 /23/china-cyber-

China seeks acquisition of specific technologies, which will aid its military and commercial interests. The likely recipients of stolen commercial data are Chinese state-owned enterprises that dominate the Chinese economy.[79] Chinese-aligned hackers target various Western industry sectors, including electronics, telecom, energy, aerospace, and defense.[80]

IV. Selected Cyber Attacks Against NATO

A variety of NATO interests have suffered cyber attacks during the past few years. For instance, on April 3, 2012, "the official NATO Croatia site (nato.mvp.hr), hosted on the main website of the Ministry of Foreign and European Affairs, was hacked and defaced by two of the members of TeaMPOisoN, TriCk and Phantom."[81]

In March 2012, "several senior British military officers and British Ministry of Defense officials received 'friend requests,' from a bogus Facebook account of U.S. Admiral James Stavridis,"[82] who is NATO's Supreme Allied Commander. Individuals believed to be connected to the Chinese government acquired personal information on their Facebook accounts—"private email addresses, phone numbers, and pictures from these unsuspecting 'friends'."[83]

In December 2011, over "50 websites belonging to NATO were hacked and defaced by the Pak Cyber Combat Squad."[84] In their message, the PCCS wrote that NATO was destroying homes and killing children.[85]

---

wild-cyber-attacks-china/ ; Context Information Security. (2012, Mar.). *Crouching tiger, hidden dragon, stolen data*. Retrieved from http://www.contextis.co.uk/

[79] Ibid.

[80] Ibid.

[81] Kovacs, E. (2012, Apr. 3). Site of NATO Croatia hacked and defaced by TeaMp0ison. Softpedia. Retrieved from http://news.softpedia.com/news/Site-of-NATO-Croatia-Hacked-and-Defaced-by-TeaMp0isoN-262429.shtml

[82] Lewis, J. (2012, Mar. 10). *How spies used to steal Nato chief's details*, Daily Telegraph. Retrieved from http://www.telegraph.co.uk/technology/9136029/How-spies-used-Facebook-to-steal-Nato-chiefs-details.html ; Hopkins, N. (2012, Mar. 10). *China suspected of facebook attack on Nato' s supreme allied commander*. The Guardian. Retrieved from http://www.guardian.co.uk/world/2012/mar/11/china-spies-facebook-attack-nato

[83] Ibid.

[84] (2011, Dec. 5). *NATO under cyber attack, 50+ sites hacked by pak cyber combat squad.* Retrieved from http://www.voiceofgreyhat.com/2011/12/nato-under-cyber-attack-50-sites-hacked.html

[85] Ibid.

In July 2011, the hacker group Anonymous claimed credit "for hacking into NATO services and stealing 1 gigabyte of sensitive information as part of its campaign to harass and humiliate prominent government targets."[86] The group tired "to post online some documents collected in the incident"[87] and promised to disclose others.[88]

Among the documents Anonymous posted was a restricted NATO PDF document related to the outsourcing of a communications and information system in Kosovo in 2008 and in Afghanistan in 2007.[89] In July 2011, Anonymous also warned NATO not to challenge its activities.[90] In June 2011, NATO's e-Bookshop website was hacked.[91]

V. Selected Cyber Attacks Against NATO Member Countries

A. United States

In June 2011, LulzSec hacked the CIA's public website making it temporarily inaccessible due to a denial of service attack.[92] In April 2009, China was suspected of being behind a major theft of data from U.S. defense contractor Lockheed Martin's $300 billion F-35 fighter Joint Strike Force program, the most advanced airplane ever designed.[93] Also, "Chinese spies hacked into computers belonging to BAE Systems, Britain's biggest defense company, to steal details about the design, performance and electronic systems"[94] of the F-35.[95]

---

[86] Nakashima, E. (2011, July 21). *Anonymous claimed it hacked NATO web site, tells FBI we're back.* Washington Post. Retrieved from http://articles.washingtonpost.com/2011-07-21/world/35266809_1_anonymous-claims-richard-stiennon-hackers-group

[87] Ibid.

[88] Ibid.

[89] Albanesius, C. (2011, July 21). *Anonymous: We hacked NATO*. PC Magazine. Retrieved from http://www.pcmag.com/article2/0,2817,2388823,00.asp

[90] Ibid.

[91] (2011, June 23). *Probable data breach from a NATO-related site*. NATO. Retrieved from http://www.nato.int/cps/en/natolive/news_75729.htm

[92] Schwartz, M. (2011, June 16). *LulzSec claims credit for CIA site takedown*. Information Week. Retrieved from http://www.informationweek.com/security/cybercrime/lulzsec-claims-credit-for-cia-site-taked/230800019

[93] Gorman, S. et al. (2009, Apr. 21). *Computer spies breach fighter-jet project*. Wall Street Journal. Retrieved from http://online.wsj.com/article/SB124027491029837401.html.html

[94] *Security experts admit China stole secret jet fighter plans*. (2012, Mar. 21). The Australian. Retrieved from http://www.theaustralian.com.au/news/world/security-experts-admit-china-stole-secret-fighter-jet-plans/story-fnb64oi6-1226296400154

[95] Ibid.

In August 2008, the laptops and cell phones of the campaign staffs of Senators Barack Obama and John McCain were hacked by Chinese interests in an effort to predict the policy options of the future presidential election winner.[96] The whistleblower website, Wikileaks, released hundreds of thousands of U.S. diplomatic cables and other sensitive data. U.S. Army soldier Bradley Manning provided the materials to Wikileaks.[97]

In August 2011, FBI contractor ManTech International suffered a cyber attack at the hands of the AntiSec campaign — a collaborative effort between Anonymous and spin-off hacker group LulzSec. The attack was believed to have compromised 400 megabytes of data, including numerous documents belonging to NATO, the U.S. Army, the U.S Department of Homeland Security, the U.S. State Department, and the U.S. Department of Justice.[98]

In December 2006, computers at the U.S. Naval War College had to taken offline for several weeks as a result of cyber attacks believed to have originated in China.[99] In October 2006, the U.S. Dept. of Commerce's Bureau of Industry and Security had to throw away all of its computers due to targeted attacks originating in China. The bureau issues export licenses of security-related products.[100]

B. Other Countries

In April 2012, hackers claiming adherence to Anonymous release personal details about thousands of members of the largest of the three parties in the Czech coalition, the Civic Democrats. The cyber attacks on the

---

[96] Bohn, K. and Todd, B. (2008, Nov. 6). *Obama, McCain campaigns' hacked for policy data*. CNN. Retrieved from http://www.cnn.com/2008/TECH/11/06/campaign.computers.hacked/

[97] Spiegel Online International. (n.d.). WikiLeaks *Diplomatic Cables.* Retrieved from *http://www.spiegel.de/international/topic/wikileaks_diplomatic_cables/;* Ball, J. (2011, Sept. 2). *Wikileaks publishes full cache of unreduced cables*. The Guardian. Retrieved from http://www.guardian.co.uk/media/2011/sep/02/wikileaks-publishes-cache-unredacted-cables; Savage, C. (2013, Feb. 28). *Soldiers admits providing files to WikiLeaks*. NY Times. Retrieved from http://www.nytimes.com/2013/03/01/us/bradley-manning-admits-giving-trove-of-military-data-to-wikileaks.html?pagewanted=all&_r=0

[98] Hoffman, S. (2011, Aug. 1). *Anonymous hackers target FBI cybersecurty [sic] contractor Mantech*. www.crn.com. Retrieved from http://www.crn.com/news/security/231003077/anonymous-hackers-target-fbi-cybersecurty-contractor-mantech.htm

[99] Avlon, J. (2009, Oct. 20). *The growing cyberthreat*. Forbes. Retrieved from Retrieved from http://www.forbes.com/2009/10/20/digital-warfare-cyber-security-opinions-contributors-john-p-avlon.html

[100] Ibid.

Czech government web sites, including on the Cabinet's website, occurred following protests against the ratification of the Anti-Counterfeiting Trade Agreement.[101]

In April 2012, two teenagers were arrested as part of an investigation into recordings made of conversations on Scotland Yard's anti-terrorism hotline, which were posted on the Internet. The two used readily available software to bombard the Scotland Yard phone line, but routed the activity through a computer served based in Malaysia in order to cover their tracks.[102] Two months earlier, the hacker group Anonymous released a recording of a conference call between the FBI and UK police in which they were discussing efforts to catch hackers.[103]

In July 2011, Anonymous hacked a division of the Italian government focused on combating cyber crime. The group released some of the documents, which included content about government offices and commercial data.[104] In June 2011, Anonymous hacked the Spanish National Police website.[105]

In August 2011, "U.S. defense contractor Vanguard Defense Industries was hit with an attack that lifted and published thousands of e-mail and sensitive documents."[106] Vanguard develops the "remote controlled Shadow Hawk helicopters used by the U.S. military."[107]

İGÜSBD
Cilt: 1 Sayı: 2
Ekim /
October 2014

---

[101] Jones, T. (2012, Apr. 2). *Anonymous again targets Czech ruling party*. Czechposition.com. Retrieved from http://www.ceskapozice.cz/en/news/politics-policy/anonymous-again-targets-czech-ruling-party

[102] Evans. M. et al. (2012, Apr. 12). *Two arrested after hackers attacked anti-terror hotline*. The Telegraph. Retrieved from http://www.telegraph.co.uk/news/9201621/Two-arrested-after-hackers-attacked-anti-terror-hotline.html

[103] Duell, M. (2012, Feb. 3). *'What about McDonald's in the Pentagon?: Extraordinary top secret call between FBI and Scotland Yard 'tapped' by Anonymous.* Daily Mail. Retrieved from http://www.dailymail.co.uk/news/article-2096035/Secret-FBI-Scotland-Yard-tapped-Anonymous--trying-catch.html

[104] Hoffman, S. (2011, July 11). *Anonymous hackers release classified information from Italian cybercrime division.* www.crn.com Retrieved from http://www.crn.com/news/security/231002570/anonymous-hackers-release-classifed-documents-from-italian-cybercrime-division.htm

[105] (2011, June 21). *Anonymous target Spanish national police website after hacker arrests*. www.huffingtonpost.com Retrieved from http://www.huffingtonpost.com/2011/06/12/anonymous-spain-police-website-hacker-arrests_n_875527.html

[106] Hoffman, S. (2011, Sept. 2). *10 biggest cyber attacks in August.* www.crn.com Retrieved from http://www.crn.com/slide-shows/security/231600608/10-biggest-cyber-attacks-in-august.htm?pgno=4

[107] Ibid.

VI. NATO Responses to Cyber Threats

A. Overview

NATO is utilizing various strategies to confront the vast cyber threats that target the Alliance's networks. NATO's Strategic Concept and the 2010 Lisbon Summit Declaration appreciate that complex cyber attacks necessitate strong protections for the Alliance's information and communications systems.[108] On June 8, 2011, NATO Defense Ministers approved a revised NATO Policy on Cyber Defense, one that delineates cyber defense measures throughout the Alliance.[109]

The modified policy offers a coordinated approach to cyber defense across the Alliance with a focus on preventing cyber attacks and building resilience. NATO structures will be protected by a centralized scheme, encompassing new requirements. The policy incorporates cyber defense into NATO's Defense Planning Process. [110]

---

[108] (2010, Nov. 20). *Lisbon summit declaration*. North Atlantic Treaty Organization. Retrieved from http://www.nato.int/cps/en/natolive/official_texts_68828.htm ; *Defending the Networks: The NATO Policy on Cyber Defence*. (2011). NATO Public Diplomacy Division. Retrieved from www.nato.int/nato.../20111004_110914-policy-cyberdefence.pdf; Defense Management. (2011, Nov. 17). *NATO: getting serious about cyber securi*ty. Retrieved from http://www.defencemanagement.com/feature_story.asp?id=18166 ; Healey, J. & Van Bochoven. (n.d.). *NATO cyber capabilities: yesterday, today, and tomorrow*. Atlantic Council. Retrieved from http://www.acus.org/publication/natos-cyber-capabilities-yesterday-today-and-tomorrow ; Kempf, A. (2011, Mar. 24). *Considerations for NATO strategy on collective cyber defense*. Center for Strategic & International Studies. Retrieved from http://csis.org/blog/considerations-nato-strategy-collective-cyber-defense ; (2011, June 10). *Cyber defence: Next steps*. North Atlantic Treaty Organization. Retrieved from http://www.nato.int/cps/en/SIDFF200A97BAB17CB7/natolive/news_75358.htm?selectedLocale=en ; n.d.). *Defending against cyber attacks*. North Atlantic Treaty Organization. Retrieved from http://www.nato.int/cps/en/natolive/75747.htm; (n.d.). *Defending the networks: the NATO policy on cyber defence*. North Atlantic Treaty Organization. Retrieved from www.nato.int/nato.../20111004_110914-policy-cyberdefence.pdf ; Hale, J. (2010, May 23). *NATO official: cyber attack systems proliferating.* Retrieved from http://www.defensenews.com/article/20100323/DEFSECT04/3230304/NATO-Official-Cyber-Attack-Systems-Proliferating ; McGee, J. (2011, July 8). *NATO and Cyber Defense: A Brief Overview and Recent Events*. Center for Strategic & International Studies. Retrieved from http://csis.org/blog/nato-and-cyber-defense-brief-overview-and-recent-events ; (2012, May 10). *NATO and cyber defence*. North Atlantic Treaty Organization. Retrieved from http://www.nato.int/cps/en/SID-D356AF5A-950BFC5F/natolive/topics_78170.htm; (2012, March 13). *NATO rapid reaction team to fight cyber attack*. North Atlantic Treaty Organization. Retrieved from http://www.nato.int/cps/en/natolive/news_85161.htm

[109] Ibid.

[110] Ibid.

The new policy will also assist Allies in their own cyber defense efforts. Among the themes that will be highlighted include optimizing information sharing and situational awareness, collaboration and secure interoperability based on NATO agreed standards. Lastly, the policy provides a framework for NATO's cyber defense collaboration with various entities, including nations, international organizations, the private sector and academia.[111]

B. Context and Evolution

The 2002 Prague Summit introduced cyber defense on the Alliance's political agenda. Subsequently, Allied leaders reiterated the need to offer further protection to these information systems at their Summit in Riga, Latvia, in November 2006.[112]

The 2008 cyber attacks on Estonian public and private institutions spurred NATO to expand its attention to its cyber defenses. In June 2007, the NATO Defense Ministers determined that greater efforts were need in this realm.[113]

The cyber attacks against Estonia and Georgia prompted a growing recognition of the baleful effects of cyber attacks on security and stability. Soon, a strategic shift occurred in NATO with a heightened call for a new NATO cyber defense policy.[114]

Against this backdrop, NATO's Strategic Concept adopted at the November 2010 Lisbon Summit highlighted the need for expand efforts in cyber defense. The Lisbon Summit Declaration/New Strategic Concept provides in pertinent part: the growing and evolving sophistication of cyber threats; the need to incorporate the cyber issue in modern conflicts; and the necessity of improving NATO capacity to detect, assess, prevent, defend and recover from cyber attacks NATO and Alliance members. Also, the Strategic Concept provides the goal of the NATO Computer Incident Response Capability achieving full operational capability during 2012.[115]

C. Overview of NATO Policy on Cyber Defense

On June 8, 2011, the NATO Defense Ministers approved the NATO Policy on Cyber Defense. The policy provides that NATO's main focus is to

[111] Ibid.
[112] Ibid.
[113] Ibid.
[114] Ibid.
[115] Ibid.

protect its communication and information systems. Thus, NATO will enhance its capabilities to deal with the vast array of cyber threats it currently faces.[116]

In achieving a coordinated approach to cyber defense, NATO will incorporate and integrate cyber defense across all Alliance missions. Additionally, cyber defense will be incorporated into national defense frameworks. Also, NATO networks will be incorporated under centralized protection. Furthermore, NATO is highly dependent on the Allies' national information systems and networks. Also, NATO works with Allies to develop minimum cyber defense requirements. NATO cyber defense efforts are focused preventing attacks, resilience, and non-duplication.[117]

While NATO will defend itself against cyber threats, it will allow for strategic ambiguity and flexibility, as disparate cyber incidents may not necessarily merit the same level and intensity of response. Should a NATO ally be victimized by a cyber attack, NATO will coordinate assistance. Along those lines, NATO will expand consultation mechanisms, early warning, situational awareness, and information sharing among the Allies.[118]

Among other activities, NATO Military Authorities will investigate the cyber defense aids performing NATO's core tasks, planning for military missions, and carrying out missions. Also, the Cooperative Cyber Defense Center of Excellence in Tallinn, Estonia, will aid NATO and its Allies.[119]

D. NATO's Principal Cyber Defense Activities

With the increased attention garnered by cyber security issues, NATO has assigned various entities to work on such issues, including: the North Atlantic Council (Council), NATO Cyber Defense Management Board (CDMB), the NATO Military Authorities (NMA), NATO Consultation, Control and Command (NC3) Board, and the NATO Communication and Information Services Agency (NCSA). The Council will be made aware of significant cyber incidents and attacks and exercises principal decision-making authority in cyber defense related crisis management. CDMB partakes in coordinating cyber defense throughout NATO Headquarters and its associated commands and agencies.[120]

---

[116] Ibid.
[117] Ibid.
[118] Ibid.
[119] Ibid.
[120] Ibid.

The NC3 Board is the principal consultant on the technical and implementation aspects of cyber defense. Next, the NMA and NC3A focus on the operational requirements and acquisition and implementation of NATO's cyber defense capabilities. Meanwhile, the NCSA, via the NCIRC Technical Center (NCIRC) proffers technical and operational cyber security services throughout NATO. Upon a cyber attack, the NCIRC reports the incident and disseminates incident-connected content to system/security management and users.[121]

VII. Conclusion

This article described the varied and challenging cyber terror threats that exist globally. Subsequently, it centered on cyber threats against NATO and its members. Then, the piece addressed NATO growing recognition of cyber threats and its multi-pronged approach to respond to such challenges.

NATO and its member states—including businesses, non-profits, and non-governmental organizations based in those nations—will continue to be threatened through cyber elements. As such, they must strengthen all phases of counter-cyber threats—technical, legal, and policy—in order to weaken the harmful effects of cyber attackers worldwide.

BIBLIOGRAPHY

Albanesius, C. (2011, July 21). *Anonymous: We hacked NATO*. PC Magazine. Retrieved from http://www.pcmag.com/article2/0,2817,2388823,00.asp

Alexander, D. (2010, July). *The radicalization of extremists/terrorists - why it affects you*. Security Magazine. Retrieved from http://digital.bnpmedia.com/publication/?i=41296&p=42

Amoroso, E. (2010). *Cyber Attacks: Protecting National Infrastructure*. Oxford, UK: Butterworth-Heinemann.

Anderson, R. (n.d.). *Countering state-sponsored cyber attacks: Who should lead?* Information as power. Army War College. Retrieved from http://www.csl.army.mil/usacsl/Publications/infoaspowervol2/IAP2%20-%20Section%20Two%20%28Anderson%29.pdf

[121] Ibid.

(2011, June 21). *Anonymous target Spanish national police website after hacker arrests*. www.huffingtonpost.com Retrieved from http://www.huffingtonpost.com/2011/06/12/anonymous-spain-police-website-hacker-arrests_n_875527.html

Apps, P. (2012, Feb. 3). Cyber security specialist: disagreements over hacking risk could mean digital 'cold war'. Retrieved from http://www.huffingtonpost.com/2012/02/03/cyber-security-risk_n_1252889.html

Ashmore, W. (2009, May 21). *Impact of alleged Russian cyber attacks*. US Army Command and General Staff College. Retrieved from http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA504991

Avlon, J. (2009, Oct. 20). *The growing cyberthreat*. Forbes. Retrieved from http://www.forbes.com/2009/10/20/digital-warfare-cyber-security-opinions-contributors-john-p-avlon.html

Ball, J. (2011, Sept. 2). *Wikileaks publishes full cache of unreduced cables*. The Guardian. Retrieved from http://www.guardian.co.uk/media/2011/sep/02/wikileaks-publishes-cache-unredacted-cables

Baocun, W. and Fei, L. (1995, June 13/20). *Information Warfare.* Chinese Academy of Military Science. Retrieved from http://www.fas.org/irp/world/china/docs/iw_wang.htm

Bohn, K. and Todd, B. (2008, Nov. 6). *Obama, McCain campaigns' hacked for policy data*. CNN. Retrieved from http://www.cnn.com/2008/TECH/11/06/campaign.computers.hacked/

Botnets: The new threat landscape white paper. (n.d.). Cisco. Retrieved fromhttp://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns441/networking_solutions_whitepaper0900aecd8072a537.html

Bradbury, D. (2009, Feb. 4). *The fog of cyberwar*. The Guardian. Retrieved from http://www.guardian.co.uk/technology/2009/feb/05/kyrgyzstan-cyberattack-internet-access

British Muslim computer geek, son of diplomat, revealed as al Qaeda's top cyber terrorist. (2008, Jan. 16). Daily Mail. Retrieved from http://www.dailymail.co.uk/news/article-508543/British-Muslim-geek-son-diplomat-revealed-al-Qaedas-cyber-terrorist.html

Bucci, S. (2009, June 12). The confluence of cyber crime and terrorism. Lecture #1123, Heritage Foundation. Retrieved from http://www.heritage.org/research/lecture/the-confluence-of-cyber-crime-and-terrorism

Carr, J. (2011, Aug. 12). *What is cyberwar?* Slate.com. Retrieved from http://www.slate.com/articles/technology/future_tense/2011/08/what_is_cyberwar.html

Charvart, P. *Cyber terrorism: A new dimension in battlespace*. (n.d.). NATO Cooperative Cyber Defence, Centre of Excellence. Retrieved from http://www.ccdcoe.org/publications/virtualbattlefield/05_CHARVAT_Cyber%20Terrorism.pdf

China gone cyber-wild – cyber attacks by China. (2011, Sept. 23). Retrieved from http://uscyberlabs.com/blog/2011/09/23/china-cyber-wild-cyber-attacks-china/

Chinese cyber-attacks: Hello, Unit 61398. (2013, Feb. 19). The Economist. Retrieved from http://www.economist.com/blogs/analects/2013/02/chinese-cyber-attacks

Choinere, P. (2012, Mar. 11). *Lieberman warns of a cyber 9/11.* Retrieved from http://www.theday.com/article/20120311/OP04/303119943

Clapper, J. (2012, Jan. 31). *Unclassified statement for the record on the worldwide threat assessment of the US intelligence community for the Senate Select Intelligence Committee*. Senate Select Intelligence Committee, at 3. Retrieved from http://www.intelligence.senate.gov/120131/clapper.pdf

Context Information Security. (2012, Mar.). *Crouching tiger, hidden dragon, stolen data*. Retrieved from http://www.contextis.co.uk/

Conway, M. (n.d.). *Hackers as terrorists? Why it does not compute*. Computer Fraud & Security. Retrieved from http://www.arifyildirim.com/ilt510/maura.conway.pdf

Cyber attacks against US government growing at rapid pace (n.d.). Secure128.com. Retrieved from http://www.secure128.com/cyber-attacks-against-us-government-growing-at-rapid-pace.aspx

(2011, June 10). *Cyber defence: Next steps*. North Atlantic Treaty Organization. Retrieved from http://www.nato.int/cps/en/SIDFF200A97BAB17CB7/natolive/news_75358.htm?selectedLocale=en

Cyber Security: a Part 3 Definition. (n.d.). Palo Alto Networks. Retrieved from http://www.paloaltonetworks.com/community/learning-center/what-is-cyber-security.html

Daly, J. (2007, June 5). *LTTE: Technologically innovative rebels*. ISN Eth Zurich. Retrieved from http://isn.ch/isn/Digital-Library/Articles/Detail/?ots783=4888caa0-b3db-1461-98b9-e20e7b9c13d4&lng=en&id=53217

(n.d.). *Defending against cyber attacks*. North Atlantic Treaty Organization. Retrieved from http://www.nato.int/cps/en/natolive/75747.htm

(2011). *Defending the Networks: The NATO Policy on Cyber Defence*. NATO Public Diplomacy Division. Retrieved from www.nato.int/nato.../20111004_110914-policy-cyberdefence.pdf

Definition of cyberwarfare (n.d.). Retrieved from http://dictionary.reference.com/browse/cyberwarfare

Denning, D. (2009). *Terror's web: How the Internet is transforming terrorism.* Handbook on Internet Crime (Y. Jewkes and M. Yar, eds.), Willan Publishing. Retrieved from http://faculty.nps.edu/dedennin/publications/Denning-TerrorsWeb.pdf

Duell, M. (2012, Feb. 3). *'What about McDonald's in the Pentagon?: Extraordinary top secret call between FBI and Scotland Yard 'tapped' by Anonymous.* Daily Mail. Retrieved from http://www.dailymail.co.uk/news/article-2096035/Secret-FBI-Scotland-Yard-tapped-Anonymous--trying-catch.html

*Estonia fines man for 'cyber war.' (*2008, Jan. 25). BBC news, Retrieved from http://news.bbc.co.uk/2/hi/technology/7208511.stm

Evans. M. et al. (2012, Apr. 12). *Two arrested after hackers attacked anti-terror hotline*. The Telegraph. Retrieved from http://www.telegraph.co.uk/news/9201621/Two-arrested-after-hackers-attacked-anti-terror-hotline.html

Examining the cyber threat to critical infrastructure and the American economy. (2011, Mar. 16). Subcommittee on cyber security, infrastructure protection, and security technologies, Committee on homeland security, U.S. House of Representatives. Retrieved from http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg72221/html/CHRG-112hhrg72221.htm

Executive order - - Improving critical infrastructure cybersecurity. (2013, Feb. 12). Office of the Press Office, White House. Retrieved from http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Federal Bureau of Investigation. (2012, May 11). *Economic espionage: how to spot a possible insider threat.* Retrieved from http://www.fbi.gov/news/stories/2012/may/insider_051112/insider_051112

(2011, Oct.). *Foreign spies stealing U.S. economic secrets in cyberspace.* Office of the National Counterintelligence Executive. Retrieved fromhttp://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

Fox News. (2011, Aug. 3). *Massive global cyberattack targeting U.S., U.N. discovered; experts blame China*. Retrieved from http://www.foxnews.com/scitech/2011/08/03/massive-global-cyberattack-targeting-us-un-discovered-experts-blame-china/

Germany, W. (2012, Feb. 29). *What is 'Anonymous' and How Does it Operate?* Radio Free Europe/Radio Liberty. Retrieved from http://www.rferl.org/content/explainer_what_is_anonymous_and_how_does_it_operate/24500381.html

Glenny, M. (2010, May 24). *The countdown to cybergeddon*. FT.com. Retrieved from http://www.ft.com/cms/s/0/47b390e4-66ca-11df-aeb1-00144feab49a.html#axzz2T6t8My9N

Goldman, D. (2011, July 28). *China v. U.S.: The cyber cold war is raging*. Retrieved from http://money.cnn.com/2011/07/28/technology/government_hackers/index.htm

Gorman, S. et al. (2009, Apr. 21). *Computer spies breach fighter-jet project*. Wall Street Journal. Retrieved from http://online.wsj.com/article/SB124027491029837401.html.html

Graham, D. (2010). *Cyber threats and the laws of war*. 4 Journal of national security law and policy 84. Retrieved from http://jnslp.com/wp-content/uploads/2010/08/07_Graham.pdf

Grauman, B. (2012, Feb.). *Cyber-security: the vexed question of global rules*. Retrieved from http://www.securitydefenceagenda.org/Contentnavigation/Library/Libraryoverview/tabid/1299/articleType/ArticleView/articleId/3064/SDA-cybersecurity-report.aspx

Hale, J. (2010, May 23). *NATO official: cyber attack systems proliferating.* Defense News. Retrieved from http://www.defensenews.com/article/20100323/DEFSECT04/3230304/NATO-Official-Cyber-Attack-Systems-Proliferating

Healey, J. & Van Bochoven. (n.d.). *NATO cyber capabilities: yesterday, today, and tomorrow*. Atlantic Council. Retrieved from http://www.acus.org/publication/natos-cyber-capabilities-yesterday-today-and-tomorrow

Hellman, Z. (2012, Feb. 22). *Hackers or terrorists*. Jpost.com.Retrieved from http://m.jpost.com/Headlines/Article.aspx?id=86258350&cat=2

(2012, Mar. 11). *Hidden Chinese Hackers Crouching Dragon, Stolen Data*. Cyber War Zone Retrieved from http://www.cyberwarzone.com/cyberwarfare/hidden-chinese-hackers-crouching-dragon-stolen-data?page=4

Hoffman, S. (2011, Aug. 1). *Anonymous hackers target FBI cybersecurty [sic] contractor Mantech*. www.crn.com. Retrieved from http://www.crn.com/news/security/231003077/anonymous-hackers-target-fbi-cybersecurty-contractor-mantech.htm

Hoffman, S. (2011, Sept. 2). *10 biggest cyber attacks in August*. www.crn.com Retrieved from http://www.crn.com/slide-shows/security/231600608/10-biggest-cyber-attacks-in-august.htm?pgno=4

Hopkins, N. (2012, Mar. 10). *China suspected of facebook attack on Nato' s supreme allied commander*. The Guardian. Retrieved from http://www.guardian.co.uk/world/2012/mar/11/china-spies-facebook-attack-nato

Hosenball, M. and Zengerle, P. (2013, Mar. 12). *Cyber attacks leading threat against U.S.: Spy agencies*. Reuters.com. Retrieved from http://www.reuters.com/article/2013/03/12/us-usa-threats-idUSBRE92B0LS20130312

Insider security threats: State CIOs take action now. (2007). National Association of Chief Information Officers of States. Retrieved from http://www.nascio.org/publications/documents/NASCIO-InsiderSecurityThreats.pdf

Jajodia, S. et al. (1999, Apr.). *Surviving information warfare attacks*. Mitre. Retrieved from http://www.mitre.org/work/best_papers/99/jajodia_surviving/jajodia_surviving.pdf

Jones, T. (2012, Apr. 2). *Anonymous again targets Czech ruling party*. Czechposition.com. Retrieved from http://www.ceskapozice.cz/en/news/politics-policy/anonymous-again-targets-czech-ruling-party

Kempf, A. (2011, Mar. 24). *Considerations for NATO strategy on collective cyber defense*. Center for Strategic & International Studies. Retrieved from http://csis.org/blog/considerations-nato-strategy-collective-cyber-defense

Kirk, J. (2007, May 17). *Estonia recovers from massive denial-of-service attack*. Infoworld. Retrieved from http://www.infoworld.com/d/security-central/estonia-recovers-massive-denial-service-attack-188 (hereinafter Kirk 2007)

Kirk, J. (2008, July 4). *Lithuania: Attacks focused on hosting company*. PC World. Retrieved from http://www.pcworld.com/article/147960/article.html (hereinafter Kirk 2008)

Kovacs, E. (2012, Apr. 3). Site of NATO Croatia hacked and defaced by TeaMp0ison. Softpedia. Retrieved from http://news.softpedia.com/news/Site-of-NATO-Croatia-Hacked-and-Defaced-by-TeaMp0isoN-262429.shtml

Kretsinger, Sony hacker Recrusion, jailed for year. (2013, Apr. 13). BBC News. Retrieved from http://www.bbc.co.uk/news/technology-22214506

Krupnick, S. (2011, Aug. 16). *Freedom fighters or vandals? No consensus on Anonymous.* Contra Costa Times. Retrieved from http://www.mercurynews.com/top-stories/ci_18686764

Lewis, J. (2002, Dec.). *Assessing the risks of cyber terrorism, cyber war, and other cyber threats*. Center for Strategic and International Studies at 9.Retrieved from http://www.steptoe.com/publications/231a.pdf

Lewis, J. (2012, Mar. 10). *How spies used to steal Nato chief's details*, Daily Telegraph. Retrieved from http://www.telegraph.co.uk/technology/9136029/How-spies-used-Facebook-to-steal-Nato-chiefs-details.html

(2010, Nov. 20). *Lisbon summit declaration*. North Atlantic Treaty Organization. Retrieved from http://www.nato.int/cps/en/natolive/official_texts_68828.htm

Lithuanian tax office website hit by cyber attack. (2008, July 21). Reuters. Retrieved from http://www.reuters.com/article/2008/07/21/lithuania-web-attacks-idUSMAR14153920080721

Mackey, R., (2009, Feb. 9). *Are 'cyber-militias' attacking Kyrgyzstan?* NY Times. Retrieved from http://thelede.blogs.nytimes.com/2009/02/05/are-cyber-militias-attacking-kyrgyzstan/

Markoff, J. (2008, Aug. 13). *Before the gunfire, cyberattacks*. Retrieved from http://www.nytimes.com/2008/08/13/technology/13cyber.html

Masters, J. (2011, May 23). Confronting the cyber threat. Council on Foreign Relations Backgrounder. Retrieved from http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577

McAfee. (2009). *In the Crossfire: Critical Infrastructure in the Age of Cyber War.* Retrieved from http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf

McCusker, R. (2006). *Transnational organised cyber crime: distinguishing threat from reality*. Crime, Law and Social Change, 46 (4-5), pp. 257-273. Retrieved from http://tees.openrepository.com/tees/bitstream/10149/115450/2/115450.pdf

McGee, J. (2011, July 8). *NATO and Cyber Defense: A Brief Overview and Recent Events*. Center for Strategic & International Studies. Retrieved from http://csis.org/blog/nato-and-cyber-defense-brief-overview-and-recent-events

Moore, D. et al. (2003, July/Aug.). *Inside the slammer worm*. IEEE Security & Privacy, at 33. Retrieved from http://cseweb.ucsd.edu/~savage/papers/IEEESP03.pdf

Mueller III, R. (2012, Mar. 1). Speech at RSA cyber security conference. FBI press release. Retrieved fromhttp://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

Murphy, D. (2011, June 19). *Three reasons to fear Lulzsec: Sites, skills, and slant*. PC Magazine. Retrieved from http://www.pcmag.com/article2/0,2817,2387219,00.asp

Nakashima, E. (2011, July 21). *Anonymous claimed it hacked NATO web site, tells FBI we're back.* Washington Post. Retrieved from http://articles.washingtonpost.com/2011-07-21/world/35266809_1_ anonymous-claims-richard-stiennon-hackers-group

Nakashima, E. (2012, Mar. 7). *China testing cyber-attack capabilities, report says*, Washington Post. Retrieved from http://www.washingtonpost .com/world/national-security/china-testing-cyber-attack-capabilities-report-says/2012/03/07/gIQAcJwDyR_story. html

(2012, May 10). *NATO and cyber defence*. North Atlantic Treaty Organization. Retrieved from http://www.nato.int/cps/en/SID-D356AF5A-950BFC5F/natolive/topics_78170.htm

(2011, Nov. 17). *NATO: getting serious about cyber securi*ty. Defense Management. Retrieved from http://www.defencemanagement.com/feature_story.asp?id=18166

(2012, March 13). *NATO rapid reaction team to fight cyber attack*. North Atlantic Treaty Organization. Retrieved from http://www.nato.int/cps/en/natolive/news_85161.htm

(2011, Dec. 5). *NATO under cyber attack, 50+ sites hacked by pak cyber combat squad.* Retrieved from http://www.voiceofgreyhat.com/2011/12/nato-under-cyber-attack-50-sites-hacked.html

Newton, S. (2001, Nov.). *Can cyberterrorists actually kill people?* SANS Institute. Retrieved from http://www.sans.org/reading_room/whitepapers /warfare/cyberterrorists-kill-people_820

Olsen, K. (2009, July 9). *Massive cyber attack knocked out government websites starting on July 4th*. Retrieved fromhttp://www.huffingtonpost .com/2009/07/07/massive-cyber-attack-knoc_n_227483.html

Ottis, R. & P. Lorents. (n.d.). *Cyberspace: definition and implications*. Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia. Retrieved from www.ccdcoe.org/articles/.../Ottis_Lorents_CyberspaceDefinition.pdf

Paganini, P. (n.d.). *The rise of cyber weapons and relative impact of cyber space*. Infosec Institute Resources. Retrieved from http://resources.infosecinstitute.com/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace/

Pellerin, C. (2011, Sept. 14). *Panetta: Regional defense, cyber highlight AUSMIN talks.* American Forces Press Service. Retrieved from http://www.defense.gov/News/NewsArticle.aspx?ID=65337

PKK attacks Turkey's finance ministry website. (2011, Nov. 9)Today's Zaman. Retrieved from http://www.todayszaman.com/news-262152--pkk-attacks-turkeys-finance-ministry-website.html

(2011, June 23). *Probable data breach from a NATO-related site*. NATO. Retrieved from http://www.nato.int/cps/en/natolive/news_75729.htm

Puran, R. (2003, Feb. 28). *Beyond conventional terrorism … the cyber assault*. SANS Institute. Retrieved from http://www.sans.org/reading_room/whitepapers/threats/conventional-terrorismthe-cyber-assault_931

Rafter, M. (2010). *New security risks from USB flash drives*. Norton. Retrieved from http://us.norton.com/yoursecurityresource/detail.jsp?aid=usbdrives

Rhodin, S. (2008, July 1). *Hackers tag Lithuanian website with Soviet symbols*. NY Times. Retrieved from http://www.nytimes.com/2008/07/01/world/europe/01baltic.html?_r=1&scp=3&sq=lithuania&st=nyt&oref=slogin

Riley, M. & J. Walcott. (2011, Dec. 12). *China-based hacking of 760 companies shows cyber cold war*. Businessweek. Retrieved from http://www.businessweek.com/news/2011-12-22/china-based-hacking-of-760-companies-shows-cyber-cold-war.html

Rogin, J. (2010, Jan. 22). *The top 10 Chinese cyber attacks that we know of*. Foreign Policy. Retrieved from http://thecable.foreignpolicy.com/posts/2010/01/22/the_top_10_chinese_cyber_attacks_that_we_know_of

Rollins, J. and Wilson, C. (2007, Jan. 22). *Terrorist capabilities for cyberattack: Overview and policy issues*. Congressional research service. Retrieved from http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-024.pdf

Savage, C. (2013, Feb. 28). *Soldiers admits providing files to WikiLeaks*. NY Times. Retrieved from http://www.nytimes.com/2013/03/01/us/bradley-manning-admits-giving-trove-of-military-data-to-wikileaks.html?pagewanted=all&_r=0

Schwartz, M. (2011, June 16). *LulzSec claims credit for CIA site takedown*. Information Week. Retrieved from http://www.informationweek.com/security/cybercrime/lulzsec-claims-credit-for-cia-site-taked/230800019

Schwartz, M. (2011, June 27). *LulzSec hackers retire: time to rethink risk*. Information Week. http://www.informationweek.com/security/attacks/lulzsec-hackers-retire-time-to-rethink-r/231000472

Silicon Republic. (2012, Jan. 9). *Anonymous attack reveals US, UK and Nato email passwords*. Retrieved from http://www.siliconrepublic.com/strategy/item/25247-anonymous-attack-reveals-us

Snow, G. (2011, Sept. 11). *Statement before the House Financial Services Committee*. *Subcommittee on Financial Institutions and Consumer Credit*. Retrieved from http://www.fbi.gov/news/testimony/cyber-security-threats-to-the-financial-sector

Snow, G. (2011, Apr. 12). *Statement before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism*, at 3. Retrieved from http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism

Social engineering using a USB drive. (n.d.). Carnegie Mellon University. Retrieved from http://www.cmu.edu/iso/aware/be-aware/usb.html

Spiegel Online International. (n.d.). WikiLeaks *Diplomatic Cables.* Retrieved from http://www.spiegel.de/international/topic/wikileaks_diplomatic_cables/

Sterner, E. (2012, Apr.). *The paradox of cyber protest*. Marshall Policy Institute Outlook. Retrieved from http://www.marshall.org/pdf/materials/1087.pdf

Tafoya, W. (2011, Nov.). *Cyber Terror*. FBI Law Enforcement Bulletin. Retrieved from http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/cyber-terror

Taliharm, A.M. (2010, Fall). *Cyberterrorism: In theory or in practice?* Defence Against Terrorism Review. 3 (2). pp. 59-71. Retrieved from http://www.coedat.nato.int/publications/datr6/DATR_Fall2010.pdf

Thachuk, K. (2008, Spring). Countering terrorist support structures. Defence Against Terrorism Review. 1 (1), pp. 13-28. Retrieved from http://www.coedat.nato.int/publications/datr/02.Kimberley%20THACHUK.pdf

Three admit inciting terror acts. (2007, July 4). BBC News. Retrieved from http://news.bbc.co.uk/2/hi/uk_news/6268934.stm

Tikk, E. et al. (2008, Nov.). Cyber attacks against Georgia: Legal lessons identified. Cooperative Cyber Defence Centre of Excellence. Retrieved from http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf

Tikk, E. et al. (2010). International cyber incidents legal considerations. Cooperative Cyber Defence Centre of Excellence. Retrieved from http://www.ccdcoe.org/publications/books/legalconsiderations.pdf

Traynor, I. (2007, May 16). *Russia accused of unleashing cyberwar to disable Estonia*. The Guardian. Retrieved from http://www.guardian.co.uk/world/2007/may/17/topstories3.russia

UN Office on Drugs and Crime. (2012, Sept.). *The use of the Internet for terrorism purposes*. Retrieved from http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

U.S. Army Training and Doctrine Command, Cyber Operations and Cyber Terrorism Handbook. No. 1.02, P.II-1 and II-3. (2005, Aug. 15). Retrieved from http://www.au.af.mil/au/awc/awcgate/army/guidterr/sup2.pdf

Wagensall, P. (2011, Feb. 16). *Cyberwarfare called the fifth domain of battle by pentagon.* Technewsdaily.com. Retrieved from http://www.technewsdaily.com/6620-cyberwarfare-called-fifth-domain-of-battle-by-pentagon.html

War in the fifth domain. (2010, July 1). The Economist. Retrieved from http://www.economist.com/node/16478792

War of the worms: cyber-attacks pose increasing danger to Israeli society (n.d.). Wharton. Retrieved from http://kw.wharton.upenn.edu/israel/war-of-the-worms-cyber-attacks-pose-increasing-danger-to-israeli-security/

War redefined. (2008, Aug. 17). LA Times. Retrieved from http://articles.latimes.com/2008/aug/17/opinion/ed-cyberwar17

Waugh, R. (2011, Dec. 29). *Computer hackers 'could bring rail network to a standstill' warns security expert – but would we even notice?* Daily Mail. http://www.dailymail.co.uk/sciencetech/article-2079449/Computer-hackers-bring-rail-network-standstill-warns-security-expert--notice.html

Whitlock, C. and Hsu, S. (2007, July 6). *Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070502120.html

Wilson, C. (2008, Jan. 29). *Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for Congre ss.* Congressional Research Service. Retrieved from http://www.au.af.mil/au/awc/awcgate/crs/rl32114.pdf

Wilson, C. (2005, Apr. 1). *Computer attack and cyberterrorism: Vulnerabilities and policy issues for Congre ss.* Congressional Research Service at 20. Retrieved from http://www.history.navy.mil/library/online/computerattack.htm

Özet

Bu makale, küresel olarak var olan çeşitli ve zorlu siber terör tehditlerini tanımlamaktadır. Bilahare, NATO ve üyelerine karşı yapılan siber tehditler noktasına odaklanmaktadır. Daha sonra, makale, NATO'da siber tehditlerle ilgili bilinçlenmenin artması ve NATO'nun bu gibi sorunlara karşılık verebilme adına çok yönlü yaklaşımı konularına değinmiştir.

NATO, üye devletler ve bu devletlerde bulunan işletmeler, kar amacı gütmeyen kuruluşlar ve sivil toplum örgütleri, siber öğeler kanalıyla tehdit edilmeye devam edileceklerdir. Durum böyle olunca, bu kuruluşlar, siber saldırganların dünya çapında yarattığı zararlı etkileri zayıflatabilmek adına siber tehditlere karşı bütün evreleri (teknik, kanuni ve politika) güçlendirmek zorundadırlar.