THE CYBER DOGS OF WAR: JOINT EFFORTS OF FUTURE WORLD LEADERS IN THE PREVENTION OF CYBERWARFARE

Nadiya Kostyuk & Marielle Ali
New York University
839 Riverside Drive Apt 4E
New York, NY 10032
nk1220@nyu.edu, ma2850@nyu.edu

ABSTRACT

Cyberwarfare is best viewed as "old wine in a new bottle" as the exigencies of the traditional laws of war remain unchanged. Using this paradigm, this article analyzes the challenges of warfare in cyberspace caused by the thin line between crime and warfare. As cyber-offenders begin using *stepping stone* countries as homebases for assaults, their prosecution becomes more challenging. To overcome this hurdle, this article recommends that governments promote domestic and international cooperation in modernizing the existing legal framework so that cybersphere is viewed as a dimension of war, thus leading to the creation of a strong legal base. On a micro level, community-based approaches remain crucial to cyberwarfare prevention and should be combined with a macro level approach of international technical and financial assistance to stepping stone nations in dealing with future advanced persistent threats that might find safe haven within their borders.

KEYWORDS

Cyberwarfare, laws of war, stepping stone countries, advanced persistent threat, cyber-offenders.

1. INTRODUCTION

In 2007, the Baltic state of Estonia, a "pioneer in the development of e-government" [1], was left reeling as a result of three weeks of continuous cyberattacks that disabled "the websites of government ministries, political parties, newspapers, banks, and companies" with only a click of the mouse [2]. The impetus for these attacks was Estonia's removal "of the Bronze Soldier Soviet war memorial" in its capital Tallinn [3]. It is cyberattacks like the event in Estonia that represent the most significant threat to current and future world leaders in the twenty-first century—a threat that experts have described as *cyberwarfare* [4]. Not only did these attacks showcase the ease and speed in which cyberattacks can occur, but they also raise major concerns for the computer-reliant international community.

This article discusses the complexities involved in defining an act of war and subsequently preventing it. The following section is devoted to comparing traditional war to cyberwarfare. Next, a description of cyberattacks in the twenty-first century is detailed along with a discussion of the lack of coordinated efforts between various governments, which is the main reason for the creation of safe havens for cyber-offenders, specifically in developing countries. The last section will provide recommendations for preventing cyberwarfare and for eliminating offline havens for cyber-offenders [5].

2. COMPLEXITIES AND UNCERTAINTIES OF CYBERWARFARE

Both traditional war and cyberwarfare are similar in that their common aim is to achieve an advantage over a competing nation-state or try to prevent said nation-state from achieving an advantage. Despite occurring in a virtual medium without traditional weapons, cyberwarfare is an act of state aggression with rather complex exigencies [6]. Historically, transnational attacks were associated with a nation-state as only nation-states were able to engage in acts of war, during which soldiers engaged in physical combat. Cyberspace, however, does not have these physical distinctions. In cyberspace, those state and non-state actors with the necessary skills and access can launch "a cross-border virtual attack, not on the territory but on the machinery of an external nation-state." [7] A 19-year old teenager, for example, was deemed responsible for the aforementioned cyberattacks on Estonia and despite his youth he possessed the necessary skills to connect to the Russian security service and bombard the Estonia with cyberattacks. In the Estonian incident, experts are not sure whether the identity of cyber-offenders can be ascertained properly as "it would be difficult to prove the Russian state's responsibility, and that the Kremlin could inflict much more serious cyber-damage if it chose to" [8].

Civilian engagement in cyberattacks creates additional complexities in defining cyberwarfare as an increasing number of nation-states are beginning to engage talented civilians in state-sponsored cyberattacks as a way to "save money and gain access to superior technical expertise" and "to operate and maintain sophisticated military equipment and to support combat operations." [9] The integration of civilians in military operations blurs the distinction between civilians and soldiers in the online environment and raises concerns of who should be protected under The Geneva and Hague Conventions. Furthermore, in the absence of an armed military defining a cyberattack as an act of war becomes problematic, especially because digital traffic "[travels] through cyberspace by routine means, the same means used by civilian and government traffic every second of every day," is the only evidence [10]. Mark Galeotti, an expert on Russian organized crime, compares this quagmire to a quote from Shakespeare's *Macbeth*: "Nothing is but what is not." It is quite difficult to differentiate between an attack sponsored by a state and one committed by an individual for private gain [11]. This leads to confusion regarding how virtual attacks should be defined—as cyberwarfare or cybercrime—and how governments should respond. Galeotti continues that "given Russian intelligence's evident interest in cyber-espionage, the claim is that the Kremlin either controls the hackers or, more plausibly, turns a blind eye so long as they step in to help when the government calls" [12].

Response to these attacks depends on how one defines them and wrongly defined attacks may lead to a slower response and greater harm. A cyberattack, for instance, can be mistakenly viewed as cybercrime when its main targets are corporate accounts or personal information though cyberwarfare also focuses on "civilian entities, including financial and infrastructure [units]" [13]. Moreover, considering the significant amount of cyberattacks that occurred during the past decade, some countries have been developing programs to both protect against cyberattacks and to launch them. For instance, in 2012 Iran launched fake cyber

attacks as an educational mechanism to build defenses against future incidents [14]. Thus, in cyberspace, it is hard to differentiate between what is actually happening and what is happening externally, and what then takes place at home [15], which leads to difficulties in finding correct responses to a situation.

Compared to the 1648 Westphalian definition of sovereignty, "a construct based on the concept of sovereign states, each legally entitled to govern its own territory and its own population free of external influence" [16], there are difficulties in defining national borders and sovereignty in cyberspace, another significant challenge of cyberwarfare. The Internet's purpose-built redundancy, usually cited as the World Wide Web's greatest trait, offer attackers a significant degree of obscurity, which therefore complicates efforts to trace the origins of these attacks. Cyberactors' increasing use proxy servers to hide or mask IP addresses serves as a perfect example of plausible deniability. Specifically, while attacks may be routed through Internet servers located in China, it does not necessarily mean that the attack originated from China. For instance, in *Operation Red October*, the advanced, malware-driven espionage network existing from October 2007 until the beginning of January 2013, involved the creation of "more than sixty domain names, mostly in Russia and Germany that worked as proxies to hide the location of their real server" [18]. Even though experts at the Kaspersky Lab believe that the cyber-offenders are most likely located in Russian-speaking countries, the exorbitant use of proxy servers and domain names makes pinpointing the exact location Red October's participants a guessing game with rather low odds, even for security experts.

3. USE OF DEVELOPING NATIONS AS HAVENS FOR CYBER-OFFENDERS

Despite these labeling impediments on cyberspace and cyberwarfare and lack of laws and coordinated efforts between governments, inaction is leading to more brazen cyber-offenders and more costly attacks. In 2008, for instance, Georgia accused Russia of disabling Georgian websites, including the website of the Ministry of Foreign Affairs [19]. No one was deemed responsible for these attacks. In 2009, the Canadian Information Warfare Monitor discovered a large-scale cyber operation in China named *GhostNet* that is speculated to have "infiltrated at least 1,295 computers in 103 countries, including many belonging to embassies, foreign ministries and other government offices" [20]. The Chinese government however denied any responsibility over this project as no conclusive evidence was found to prove its guilt. With the code name *Olympic Games*, the United States and Israel created *Stuxnet*, a worm virus which disrupted the activities at the Nantz Iranian nuclear facility over the course of several weeks in 2010 [21]. As a result, Iran responded by launching a number of cyberattacks on the Israeli establishment and tourists in Azerbaijan, India, and Thailand [22]. In March 2011, the Pentagon reported 24,000 files stolen from their servers and many Pentagon officials, including Deputy Defense Secretary William J. Lynn III, speculated that China was behind the theft [23]. In 2012, the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) responded to 198 cyber incidents with nearly half of them occurring in the energy sector [24]. Other sectors have also been affected by cyberattacks such as major U.S. banks, including Bank of America (BAC), J. P.

Morgan Chase, and Wells Fargo (WFC). In addition, Japan's Internal Finance Ministry was affected when more than 3,000 confidential documents were compromised as a result of a cyber attack [25]; furthermore, the U.S. Department of Justice (USDOJ) suffered multiple cyber attacks during the past year [26] and in January 2013 [27], respectively.

Due to the dearth of efforts in combating unlawful activities in cyberspace, less technologically developed countries are at greater risk of becoming safe havens for cyber-offenders. With minimal risk and often impunity, cyber-offenders usually operate through cyberspace from these *stepping stone countries*, technologically unsophisticated states which often lack preventive cyber security measures in their police departments, laws that guard cyberspace, and the resources and institutional capacity to prevent attacks occurring in the online environment [28]. A significant example of such a cyber safe haven is the Philippines, where the 2000 *ILOVEYOU* virus originated, causing approximately $10M U.S. in losses in twenty countries [29]. Even after FBI agents identified the perpetrator, a Filipino student, no charges were brought against him due to the lack of Philippine laws prohibiting unlawful cyberactivities. Moreover, the country refused to extradite its citizen to the United States where he could have been prosecuted for his actions as no extradition treaty exists between the two countries. The *ILOVEYOU* virus shows that jurisdictional voids remain in many countries where cybersecurity might not even be on their national agendas, such as the countries of Central and Eastern Europe, Central Asia, and Africa. Nigeria, for example, is *infamous* for its *419 scams* involving advance fee fraud, so named after the Nigerian criminal code that this scam violates [30]. Multiple variations of the 419 scam exist in which scammers offer victims everything from false job promises and inheritance traps to company shares in the public and private sector, all of which cost the victim a nominal fee as a means to receive a greater prize. After a victim supplies the perpetrator with personal information, such as bank account numbers, illegal money transfers occur through companies like Western Union. The Nigerian scam has spread to other countries that have no legal base for this crime, including Togo and Cote d'Ivoire. These safe havens make it difficult for law enforcement even from wealthy, technologically sophisticated nations to follow information trails and thus allow cyber-offenders operate with relative impunity [31].

Our future appears dim with upcoming cyber menace, and according to Intel's McAfee, *Project Blitzkrieg*, a potential cyber attack on the banking industry is set to launch in spring 2013 [32]. In this 'Project,' Russian hackers will target investment and national banks through a fraudulent transaction. This attack, however, is the only one we are aware of. With every passing day, cyber-offenders become increasingly skilled and sophisticated. With this in mind, this article offers the following recommendations to predict and prevent violent acts in the online environment.

4. POLICY RECOMMENDATIONS:

4.1 "Old wine in a new bottle:" Laws of war in the cyberspace. In conjunction with *stepping stone countries*, developed nations should work domestically to establish a legal base for adjudicating cyberattacks. Ernesto Savon, head of the Transcrime Research Center in

Trento, Italy, points out that the creation of laws that punish cyberoffenders and the imposition of similar laws in various countries will help decrease the number of safe havens where cyberperpetrators can operate with impunity [33]. The U.S. can serve as an example for the members of the international community that have already applied laws of war to cyberspace. Some nascent steps have already been undertaken, such as the 1993 White Paper on Growth and the Bangemann Report issued by the then-European Commission, which focused on the importance of computer security [34]; the 2001 Council of Europe Convention on Cybercrime [35], and the 2009 development of the EU's European Network and Information Security Agency (ENISA), which is a "pace-setter" for information security in Europe [36]. There are similar initiatives in other corners of the world. Defence Secretary Gotabhaya Rajapaksa of Sri Lanka, for instance, addressed the role the national government plays in protecting its national information infrastructure and its citizens. In his December 2012 speech, Rajapaksa suggested that the government should "develop cyber strategies that hold true across the state [and private] sectors," and meet international standards [37]. Though all of these initiatives address cybersecurity and cybercrime, none discuss large-scale cyberattacks and cyberwarfare nor establish a legal base for the online environment. Only the forthcoming 2013 Tallinn Manual on the International Law Applicable to Cyber Warfare, to be published by the NATO Cooperative Cyber Defense Centre of Excellence, applies the United Nations Charter, specifically Articles 2 (Section 4 use of force) and 41, 42, 51(self-defense), and the Geneva Conventions to the online environment [38]. The international community thus should work together with Russia, China, Uzbekistan, and Tajikistan—nations that have been pushing the Secretary General for an international code of conduct on information security [39]. Only after world leaders cooperate and compromise will other countries follow their example in applying laws of war to the online environment.

4.2. Joint efforts between the public and private sectors. U.S. Congressmen Michael McCaul, Co-Chair of the Cybersecurity Caucus Committee, said the enactment of comprehensive cybersecurity legislation would "be one of [the] Committee's top priorities." [40] McCaul noted that 85 percent of the nation's critical infrastructure is privately owned, and private industry must be part of the solution [41]. A similar concern was expressed by Richard Horne, the director of cyber security at Barclays, also stresses the importance of transparent sharing of information and intelligence between public and private sectors [42]. This cooperation can be achieved through training programs and joint workshops as major soft targets for cyber attacks include national power grids, water facilities, and other critical but poorly cyber-guarded infrastructure. The Network Security Innovation Center at Lawrence

Livermore National Laboratory [43], for instance, is a successful example of public-private initiative to counter the persistent attack on infrastructure and national security networks and protect critical operations. Its Secure Operations program aids private partners in keeping critical operations safe. Moreover, the United Nation's International Telecommunication Union (ITU) launched a new coalition with the International Multilateral Partnership Against Cyber Threats (IMPACT) in 2011, whose main focus is bringing together governments, academic experts, and industry experts such as Microsoft, Kaspersky Lab and Symantec in order to enhance the global community's capability in dealing with cyber threats [44]. In 2012, India's National Security Agency released a report titled "Recommendations of Joint Working Group on Engagement with Private Sector on Cyber Security," which became another successful initiative that stresses a need for capacity building and public-private cooperation [45]. Other governments should follow these examples and establish working agreements with anti-virus companies such as Kaspersky Lab, Computer Associates and Symantec who have for decades shared virus definitions as part of a comprehensive public-private cybersecurity initiative. Moreover, public-private initiatives should be expended through joint programs, training, and conferences.

4.3 Corporeal Security as a Priority. Because a motivated cyberoffender physically installed malware at a nuclear facility that lacked adequate security measures, the Stuxnet incident revealed the importance of physically guarding locations such as power grids, hospitals, transportation hub, among others. The Stuxnet breech illustrates the necessity of effective physical security measures as not all cyberattacks originate through the Internet. Critical national infrastructure, including "any physical assets that is capable of being used to produce services or other benefits for a number of years," should be equipped with adequate security measures to prevent easy access to cyber-offenders [46]. Even though the U.S. Department of Homeland Security's (DHS) Federal Emergency Management Agency (FEMA) highlights the need for citizens to stay protected in their online environment, it does not mention physical security of infrastructure during manmade or natural emergencies [47]. When Hurricane Sandy hit the Northeastern part of the United States, for instance, the physical security of power grids and transportation was jeopardized, which was labeled an ideal scenario for a potential cyberattack by department Secretary Janet Napolitano [48]. There is a need therefore for FEMA and similar agencies worldwide to address the physical security of national infrastructure, which can become significantly vulnerable.

4.4. Education for cybersecurity professionals. Some nations are making significant progress in educating future cybersecurity professionals. The U.S. DHS, together with the National Initiative

for Cybersecurity Education, the Department of Education, and the National Science Foundation, announced a new initiative that focuses on the implementation of cybersecurity education programs from kindergarten through postgraduate studies [49]. On the other side of the Atlantic, the Kaspersky Lab in Russia is encouraging academic growth in the field of cybersecurity by holding annual academic conferences for a new generation of cyberleaders [50]. After being attacked by viruses like Flame, Stuxnet and Gauss, Iran began developing military and civil cyber units to prevent future cyber attacks. In 2012, Iran launched fake cyber attacks as an educational mechanism to build defense for future incidents [51]. Moreover, in 2013, the Israeli government will launch a cyberwarfare awareness program for teenagers titled *Magshimim Le'umit* [52]. While these initiatives are steps forward in the right direction, even more can and should be done. Even though the number of cybersecurity professionals has increased recently, the demand for more professionals is high and will continue to grow as cybersecurity is an ever-changing industry that requires high-skilled, adaptable individuals, and cyberwarfare is a continuing potential threat that must be adequately addressed. Last year, the UK government announced their plan to recruit 'Cyber Reservists' for the Ministry of Defense with the objective of attracting more cyber professionals towards supporting the work of the government against cyber attacks [53]. The Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM) certificates are the minimum requirements in the U.S. for every future cyber warrior [54], but they are just first steps. Considering the need for the future cyber specialists, New York University created a Masters of Science in Cybersecurity, a program that provides IT leaders with cybersecurity expertise. Likewise, many courses on cybersecurity and hacking have been added to UK universities [55]. Other universities worldwide should follow these examples.

4.5. Civilian policing of cyberspace.

Referring to cybersecurity challenges, British Army General Rupert Smith argues, "Military organizations need to rethink and restructure their approach to warfare in order to accommodate the realities of this century" [56]. Through online programs, military personnel will be able to gain a high level of cyber security knowledge and provide valuable support to government agencies [57]. Militaries and law enforcement, however, should not be the only entities responding to the acts of cyber-offenders. Civilians who have appropriate skills should take an active part in this process, as the rationale of excluding them—the protection from retaliatory attacks by an opposing military force—is not pragmatic in cyberwarfare [58]. The prospect of vigilantism, the idea of civilians "taking the law into [their] own hands," give credence against involving civilians in law enforcement because "While vigilantes claim to be acting on behalf of the law, their conduct

actually erodes the fabric and integrity of the law" [59]. Properly trained civilian participation however, could be a valuable asset for assisting law enforcement in policing the online environment. Thus, civilian policing could be completed in a formal way by creating a new social institution or an informal way through voluntary, ad hoc participation [60]. In both cases, civilians should be under direct supervision of law enforcement or military officials. Some steps in this direction have already been completed by the Pentagon, which quadrupled the Department of Defense's Cyber Command personnel from 900 to 4900 troops and civilians [61]. Through such cooperation, world leaders can establish links between civilians and the national cybersecurity apparatuses of global society as plugging security gaps in one-entity increases the protection of all.

5. CONCLUSION

The Internet adds a new dimension for conflict, and this cyber dimension desperately needs to be regulated via a legal framework. Current and future leaders should take a proactive approach to cyberwarfare instead of a reactive one and unite in adjusting the laws of war to cyberspace. As U.S. Defense Secretary Leon Panetta rightfully pointed out, "Since China and the United States have advanced cyber capabilities, it is important to develop better co-operation… it's extremely important that we work together to develop ways to avoid any miscalculation or misperception that could lead to crisis in this area." [62] With this cooperative spirit, global society is taking a step in the right direction. Not only does cooperation help prevent cyberattacks, but it also addresses the complexities of cyber warfare. It is hoped that other nation states follow suit.

Such cooperation will additionally serve as an example for other nations, resulting in fewer stepping stone countries becoming safe havens for future cyber-offenders. Moreover, world-leading nations should use this narrow window of opportunity to increase prevention efforts by engaging civilians through education and implementing better cybersecurity programs in developing countries. Despite the diversity of opinions and ideas present in the global information society, nations should work in concert to address the exigencies of cyberwarfare and establish the means to mitigate it. It is of paramount importance that nation leaders act swiftly because cyber-offenders remain resolute in their mission to disrupt an ever-increasingly technology-dependent society. Cyberoffenders are already several steps ahead of the international community and are increasing in sophistication by the minute.

6. REFERENCES

1. Ruus, Kertu. "E-Stonia: Pioneer of Internet Innovation and e-Government." *European Affairs*. 8.1 (2007). Web. 14 Nov. 2012. <http://www.europeaninstitute.org/20070302100/Spring-2007/estonia-pioneer-of-internet-innovation-and-e-goverment.html>.
2. Traynor, Ian. "Russia accused of unleashing cyberwar to disable Estonia." *Guardian* [Brussels] 16 May 2007. Web. 14 Nov. 2012. <http://www.guardian.co.uk/world/2007/may/17/topstories3.russia>.
3. Swaine, Jon. "Georgia: Russia 'conducting cyber war'." *Telegraph* 11 Aug 2008. Web. 14 Nov. 2012.

<http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html>.

4. Nils Melzer, Research Director of the Center for Business and Human Rights at the University of Zurich and former Legal Adviser of the International Committee of the Red Cross defines cyberwarfare as "warfare conducted in cyberspace through cyber means and methods." Fore more information, *see* Melzer, Nils. "Cyberwarfare and International Law." *United Nations Institute for Disarmament Research*. United Nations. Web. 14 Nov 2012. <http://unidir.org/pdf/activites/pdf2-act649.pdf>.
5. William , Hague. "Arming the information highway patrol." *World Today*. (Dec 2012 & Jan 2013): 35. Print.
6. Brenner, Susan. "'At Light Speed' – Attribution and Reponse to Cybercrime/Terrorism/Warfare." *Journal of Criminal Law and Criminology*. 97. (2007): 110-111. Print.
7. *Ibid*, p. 412.
8. *Guardian, supra* n 2.
9. Power, Richard. Tangled Web: Tales of Digital. Que , 2000. Print.
10. Brenner, *supra* n 7, p. 426.
11. Galeotti, Mark. "The Cyber Menace." *World Today*. (Dec 2012 & Jan 2013): 34. Print.
12. Galeotti, Mark. "Why are Russians excellent cybercriminals?." *Moscow News*, 21 Nov 2011. Web. 23 Feb. 2013. <http://themoscownews.com/siloviks_scoundrels/20111121/189221309.html>.
13. Wilson, Clay. "Information Operations and Cyberwarfare: Capabilities and Related Policy Issues CRS-1 to CRS-8 (2006)." *CRS Report for Congress*. Web. 14 Nov 2012. <http://www.fas.org/irp/crs/RL31787.pdf>. This congressional report described China's commitment to cyberwarfare: "China is actively improving its non-traditional military capabilities. . . . China's approach to exploiting the technological vulnerabilities of adversaries extends beyond destroying or crippling military targets. Chinese military writings refer to attacking key civilian targets such as financial systems. The Commission believes Chinese intelligence services are capable of doctoring computer systems. It has seen clear examples of computer network penetrations coming from China, some of which were publicized in the "Titan Rain" expose that received substantial press coverage…."
14. "Iran stages cyber warfare drill alongside Hormuz naval exercise." *RT News* 31 Dec 2012. Web. 20 Jan. 2013. <http://rt.com/news/iran-cyber-drill-hormuz-154/>.
15. Galeotti, *supra* n 11, p.35.
16. Janis, Mark. "Religion and International Law." *American Society of International Law*. (2002). Print.
17. Maras, Marie-Helen. *Computer Forensics: Cybercriminals, Laws, and Evidence*. 1st ed, 261. Jones & Bartlett Learning, 2011. Print.
18. Gutterman, Steve. "Russia beefs up Internet security after spy attacks." *MSN News* 21 Jan 2013. Web. 23 Feb. 2013. <http://news.msn.com/science-

technology/russia-beefs-up-internet-security-after-spy-attacks>.
19. Gorman, Siobhan. "Georgia States Computers Hit By Cyberattack." *Wall Street Journal* 12 Aug 2008. Web. 14 Nov. 2012. <http://online.wsj.com/article/SB121850756472932159.html>.
20. Markoff, John. "Vast Spy System Loots Computers in 103 Countries." *New York Times*. 28 2009. Web. 14 Nov. 2012. <http://www.nytimes.com/2009/03/29/technology/29spy.html?pagewanted=all>.
21. Sanger, David. "Obama Order Sped Up Wave of Cyberattacks Against Iran." *New York Times* [New York] 01 Jun 2012. Web. 14 Nov. 2012. <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all>.
22. Parthasarathy, G. "Watch Out for Instability in West Asia." Hindu Business Line [Chennai] 07 Jul 2012. Web. 14 Nov. 2012. <http://www.thehindubusinessline.com/opinion/columns/g-parthasarathy/watch-out-for-instability-in-west-asia/article4074545.ece?homepage=true>.
23. Smith, Gerry. "Foreign Hackers Stole 24,000 Military Files, Pentagon Says." *Huffington Post* 13 Sep 2011. Web. 14 Nov. 2012. <http://www.huffingtonpost.com/2011/07/14/foreign-hackers-stole-240_n_899304.html>.
24. Rashid, Fahmida. "ICS-CERT: Response to Cyber 'Incidents' Against Critical Infrastructure Jumped 52 Percent in 2012." *Security Week* 10 Jan 2013, n. pag. Web. 20 Jan. 2013. <http://www.securityweek.com/ics-cert-response-cyber-incidents-against-critical-infrastructure-jumped-52-percent-2012>.
25. *AsiaOne. Science and Tech. Asia News Network* [Cyber-attack malware in Japan identified] 04 Jan 2013. Web. 20 Jan. 2013. <http://www.asiaone.com/News/Latest+News/Science+and+Tech/Story/A1Story20130104-393309.html>.
26. Egan, Matt. "PNC warns Customers About Ongoing Cyber Attack." *Fox Business*, 04 Jan 2013. Web. 20 Jan. 2013. <http://www.foxbusiness.com/industries/2013/01/04/pnc-warns-customers-on-likely-ongoing-cyber-attack/>.
27. "Cyber attack shuts down US Justice Department's website." *PressTV* 27 Jan 2013. Web. 23 Feb. 2013. <http://www.presstv.ir/detail/2013/01/27/285801/us-justice-department-website-hacked/>.
28. Computer Crime Research Center. 2010. 9 Nov. 2012.< http://www.crime-research.org/
29. ""ILOVEYOU" Virus: Lessons Learned Report." *Assured Information for America's Power Projection Army*. Department of the Army, 25 Jun 2003. Web. 14 Nov 2012. <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA415104&Location=U2&doc=GetTRDoc.pdf>.
30. Maras, *supra* n 17, p. 137.
31. Computer Crime Research Center. 2010. 9 Nov. 2012.< http://www.crime-research.org/
32. Egan, 2013, *supra* n 26.
33. Computer Crime Research Center, *supra* n 31.
34. For the full version of this report, *see* http://www.telework-

mirti.org/english/invent/invent.htm#2.
35. For the full version of this convention, *see* "Council of Europe Convention on Cybercrime." *The Council of Europe*. 23 Nov 2001. Web. 14 Nov 2012.
36. ENISA. "About US." European Network and Information Security Agency. ENISA. Web. 14 Nov 2012. <http://www.enisa.europa.eu/about-enisa>
37. "Gearing for cyber attacks - Defence Secretary." *Daily News. Sri Lanka's Daily Newspaper* 18 Dec 2012. Web. 20 Jan. 2013. <http://www.dailynews.lk/2012/12/18/fea01.asp>.
38. "The Tallinn Manual." *CCDCOE*. NATO Cooperative Cyber Defense Centre of Excellence. Web. 14 Nov 2012. <https://www.ccdcoe.org/249.html>.
39. General Assembly, . United Nations. United Nations. Developments in the field of information and telecommunications in the context of international security. New York: , 2011. Web. <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/496/56/PDF/N1149656.pdf?OpenElement
40. Martinez, Jennifer. "McCaul: Cybersecurity Legislation is 'Top' Priority Next Congress." *The Hill* 05 Dec 2012. Web. 25 Feb. 2013. <http://thehill.com/blogs/hillicon-valley/technology/271251-mccaul-cybersecurity-legislation-is-qtopq-priority-next-congress>
41. *PressTV, supra* n 27.
42. Warren, Peter. "Russia proposes new plan to defeat online hackers." *Telegraph* 22 Dec 2011. Web. 23 Feb. 2013. <http://www.telegraph.co.uk/sponsored/russianow/technology/8972805/Russia-plan-defeat-online-hackers.html>.
43. For more information, *see:* https://nsic.llnl.gov/
44. For more information, *see:* http://www.impact-alliance.org/home/index.html
45. Singh, Shalini. "NSA announces cyber security cooperation with private sector." *Hindu* 12 Oct 2012. Web. 20 Jan. 2013. <http://www.thehindu.com/news/national/nsa-announces-cyber-security-cooperation-with-private-sector/article4000136.ece>.
46. "Critical Infrastructure and Key Assets:Definition and Identification. ." *CRS Report for Congress*. The Library of Congress, 01 2004. Web. 14 Nov 2012. <http://www.fas.org/sgp/crs/RL32631.pdf>.
47. "Cyber Attack." *Federal Emergency Management Agency*. Department of Homeland Security, 27 Sep 2012. Web. 20 Jan 2013. <http://www.ready.gov/cyber-attack>
48. Garrett, David. "Cyber attack is imminent, says DHS Secretary Napolitano." *Examiner* 25 Jan 2013. Web. 23 Feb. 2013. <http://www.examiner.com/article/cyber-attack-is-imminent-says-dhs-secretary-napolitano>.
49. Department of Homeland Security, . "Inspiring the Next Generation of Cyber Professionals." Department of Homeland Security. Department of Homeland Security, 26 2012. Web. Web. 5 Nov. 2012.
50. "Cybersecurity for the Next Generation. European Round 2013." *Conference for Young Professionals*. Kaspersky Lab. Web. 14 Nov 2012.

< http://www.kaspersky.com/images/European Round 2013_info brochure.pdf>.
51. "Iran stages cyber warfare drill alongside Hormuz naval exercise." *RT News* 31 Dec 2012. Web. 20 Jan. 2013. <http://rt.com/news/iran-cyber-drill-hormuz-154/>.
52. Phneah, Ellyne. "Israel launches cyber warfare training program." *ZDNet* 02 Jan 2013. Web. 20 Jan. 2013. <http://www.zdnet.com/israel-launches-cyber-warfare-training-program-7000009264/>.
53. Perks, Aleyx. "Cyber Security in the UK Needs to Be Improved ." *Business 2 Community* 23 Jan 2013, http://www.business2community.com/tech-gadgets/cyber-security-in-the-uk-needs-to-be-improved-0385687
54. Talley, Sue. "In Cyber Warfare, Education is Our Most Powerful Weapon." *Huffington Post* 12 Dec 2012. Web. 20 Jan. 2013. <http://www.huffingtonpost.com/sue-talley-edd/in-cyber-warfare-education_b_2244950.html>.
55. *Business 2 Community*, *supra* n 52.
56. Brenner, *supra* n 6, p. 455.
57. Talley, *supra* n 53.
58. Brenner, *supra* n 6, p. 444.
59. *Ibid*, p. 448.
60. *Ibid*, p. 467.
61. Nakashima, Ellen. "Pentagon to create cyber attack wing." *Sydney Morning Herald* 28 Jan 2013. Web. 23 Feb. 2013. <http://www.smh.com.au/world/pentagon-to-create-cyber-attack-wing-20130128-2dg40.html>.
62. Pellerin, Cheryl. "U.S., China Must Work Together on Cyber, Panetta Says." *American Forces Press Service*. 7 May 2012. Web. 25 Feb. 2013.<http://www.defense.gov/News/NewsArticle.aspx?ID=116235>