National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

TODAY'S WEAPON OF MASS DISRUPTION: CYBERTERRORISM

Maj R.T. Montante

JCSP 41

Exercise *Solo Flight*

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 41

Exercice *Solo Flight*

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 41 – PCEMI 41
2014 – 2015

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

TODAY'S WEAPON OF MASS DISRUPTION: CYBERTERRORISM

Maj R.T. Montante

INTRODUCTION

In 2007 a confrontation between Estonia and Russia did not start with a land force invasion, or a devastating air campaign designed to eliminate defense systems, it began with the crippling disruption of the Estonian Presidential and Parliament websites, half of the country's largest news agencies, and two of its main banks.[1] Estonia prides itself as an e-government, utilizing a state-of-the-art electronic administration to conduct 98% of routine operations on-line.[2] The cyber-attacks brought the entire country to a grinding halt for weeks. In 2008 a coordinated distributed denial-of-service (DDoS) attack was launched against Georgia weeks before the armed phase of the conflict began with Russia disrupting the government's ability to communicate with its population and the outside world.[3] And in 2009 a week-long cyber-attack targeted key United States (U.S) and South Korean governmental departments, disrupting the Pentagon, the State Department, the South Korean President's office and National Assembly.[4] Each of these examples demonstrate the vulnerability of critical national infrastructure (CNI), amplified by the fact that these key systems can be infiltrated via the internet.

Cyber-attacks have rapidly become one of the most significant threats to a states' national security, as demonstrated by the United Kingdom (UK) National Security Council elevating a hostile cyberspace attack by other states as one of their four Tier 1 threats, the others being international terrorism, a major accident, and an international

[1] Scott J. Shackelford, "Estonia Three Years Later: A Progress Report on Combating Cyber Attacks," *Journal of Internet Law* 13, no. 8 (02, 2010), 22-23.

[2] Michael Cross, "Whitehall must Learn from Estonia's E-Government," The Guardian, http://www.theguardian.com/technology/2007/may/24/society.insideit (accessed April 2nd, 2015).

[3] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal* (2010), 2-3.

[4] Kevin Roebuck, *Cybersecurity: High-Impact Strategies - what You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors,* Emereo Publishing, 2012), 141.

military crisis.[5] This paper will argue that cyber-attacks pose the greatest threat to a country’s CNI due to inherent internet vulnerabilities and without the adoption of international cyber governance, anchored on universal jurisdiction, a grave threat to a states’ national security will remain. To prove this point, this paper will first analyze the underlying fundamental problems with the internet that led to today’s vast amount of vulnerabilities, followed by a review of current national and international policy and law attempts to counter cyber-attacks, and finally present why universal jurisdiction is the most feasible way to accomplish cyberterrorism deterrence to reduce the threat.

UNDERLYING FUNDAMENTAL INTERNET SECURITY FLAWS

The creation and rapid proliferation of the internet has transformed and interconnected world communications like no other invention has before. The primary conceptual issue of this rapid spread of the internet is the irreversible dependence on technology.[6] With the incredible advantages the internet has produced in both the private and public sectors, it is impossible not to use them at this point. Vinton Cerf, one of the recognized founding fathers of the internet, stated “the internet was designed without any contemplation of national boundaries. The actual traffic in the net is totally unbounded with respect to geography”.[7] In less than a decade, the internet created a limitless global collaboration capability. Unfortunately, the initial internet technical design focused

[5] Cabinet Office: National Security and Intelligence, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (Norwich, UK: TSO,[2010]).

[6] Kelly A. Gable, "Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and using Universal Jurisdiction as a Deterrent," *Vanderbilt Journal of Transnational Law* 43, no. 1 (01, 2010), 63.

[7] Barry Leiner et al., "A Brief History of the Internet," *ACM SIGCOMM Computer Communication Review (ACM Digital Library)* 39, no. 5 (10/01, 2009), 22-31.

primarily on efficiency, security concerns surfaced only after networks had quickly multiplied exposing serious security vulnerabilities. Because of this oversight, major network security vulnerabilities have exposed vital industries critical to national security to devastating cyber-attacks because they are linked via the internet.

Stepping back in time exposes the key technical misstep that resulted in today's cyber threats. The first version of the internet was known as the Advanced Research Projects Agency Network (ARPANET), developed in the 1960s and sponsored by the Pentagon to network organizations for national security purposes.[8] At this point, the limited access points and lack of network-to-network connection capability shielded ARPANET from the threat of an international cyber-attack. With the desire to expand collaboration to major universities throughout the U.S., Transmission Control Protocol/Internet Protocol (TCP/IP) was implemented in 1983 as the standard network communication method between computers. Again, because the agencies linked by this new protocol were known and trusted, security was not a major concern and did not expose the true threat.[9] It was not until 1991 when the first world wide web page was introduced, combined with the 1995 shift of internet oversight to several private entities, that revealed TCP/IP as the primary security weakness of the internet.[10] At this point TCP/IP had become the global standard, with the number of internet users growing from

[8] William M. Stahl, "The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity," *Georgia Journal of International & Comparative Law* 40, no. 1 (Fall2011, 2011), 252-254.
[9] Jonathan L. Zittrain, "The Generative Internet," *Harvard Law Review* 119, no. 7 (05, 2006), 2002-2012.
[10] Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and using Universal Jurisdiction as a Deterrent*, Vol. 43 Vanderbilt Journal of Transnational Law, 2010), 63-64.

less than 10,000 in 1981, to over 700,000 in 1991, and to 36 million in 1996.[11] The continued rapid accessibility of the internet over the past 20 years has uncovered several physical, logical, and software susceptibilities that have significantly contributed to cyber-attack vulnerabilities, but the major underlying issue that experts continue to point back to is the network protocol that dictates the format of all data transfers, TCP/IP.

Today, with more than 2.6 billion internet users, cyber touches every facet of daily life. The internet links control systems to CNI, to include electric power grids, military infrastructure, and water sanitation plants. It also connects routine communication platforms, such as e-mail and social media to conduct business or simply stay in touch. The internet enables global trade and investment, with few restrictions. Unfortunately, the internet is also an effective tool for cyber terrorists, exposing a direct threat to national security.[12] According to Columbia University Computer Science Professor Steven Bellovin, a computer networks and security expert, the internet, with its inherent technical flaws, threatens national security in three major ways.[13] First, the ability of an attacker to easily transfer from one computer or network to another, gaining access to critical data and to elevate privileges to exploit more vulnerable networks. Second, the internet cannot protect data indefinitely from persistent and talented cyber terrorists. And third, the internet has provided cyber terrorists with the tools they need to conduct an attack, while providing the platform to launch their attacks. Professor

[11] Internet World Stats: Usage and Population Statistics, "Internet Growth Statistics: Today's Road to E-Commerce and Global Trade Internet Technology Reports," http://www.internetworldstats.com/emarketing.htm (accessed April 2nd, 2015).

[12] The White House Office of the Press Secretary, https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure (accessed April 3rd, 2015).

[13] S. M. Bellovin, "A Look Back at Security Problems in the TCP/IP Protocol Suite" IEEE Comput. Soc, 01/01, 2004), 7-18.

Bellovin concluded that current internet security flaws can enable a capable cyber terrorist with the right resources to bring a major system crashing down.[14]

Some experts have argued that the solution to the TCP/IP security vulnerability is internet encryption. Corporate think tanks, such as Intel Corporation, have argued that next generation cryptographic solutions can transform the internet into a reliable and secure infrastructure thwarting future cyber-attacks.[15] Few would argue that encryption would not prevent some attacks, but even the strongest algorithms are insufficient to fully secure the internet. According to Doctor Bruce Schneier, a renowned cryptographer, computer security, and privacy specialist, even with encryption in place, cyber-attacks such as password sniffing, Trojan horses, and data modification will still be conducted, ultimately finding a vulnerability to exploit.[16] Even if a solution to secure TCP/IP was developed, Johnny Long, author of *No Tech Hacking*, stated "there will always be a human somewhere who holds the keys to the kingdom and may be scammed or bribed into giving them up".[17] It must be recognized that there is no 100% secure solution to the underlying internet security flaws. Therefore, in an effort to counter cyber terrorists, nations must turn to attempts at prevention and deterrence, primarily through the use of international cyber policy and law.

[14] Ibid.

[15] Michael Kounavis et al., "Encrypting the Internet," *ACM SIGCOMM Computer Communication Review (ACM Digital Library)* 41, no. 4 (10/22, 2011), 135-136.

[16] Jay G. Heiser, "Beyond Cryptography: Bruce Schneier's Beyond Fear: Thinking Sensibly about Security in an Uncertain World," *Computers & Security* 22, no. 8 (12, 2003), 22.

[17] Amanda N. Craig and Scott J. Shackelford, "Hacking the Planet, the Dalai Lama, and You: Managing Technical Vulnerabilities in the Internet through Polycentric Governance," *Fordham Intellectual Property, Media and Entertainment Law Journal* 24, no. Winter 2014 (2014), 12.

CURRENT POLICY ATTEMPTS TO COMBAT CYBERTERRORISM

Cyberterrorism has forced many nations into developing new laws and policies in an attempt to secure their critical infrastructure. The primary focus is on governance, rather than a purely technical solution, because states quickly realized it is more difficult, if not impossible, to reengineer information technology (IT) networks and CNI with security measures after the fact, compared to developing and implementing them with security in mind from the start. Additionally, the attacks on Estonia, Georgia, and the U.S. have proven cyber-attacks are an effective method to threaten a country's national security, especially since the international community does not currently have an effective process to respond with.[18]

The diverse nature of cyber-attacks, and the fact no nation is immune to the threat, has thrust the difficult task of developing prevention methods before national governments and international establishments.[19] A number of far-reaching organizations, such as NATO, the European Union (EU), the United Nations, and the Organization for Security and Cooperation of Europe (OSCE), have taken the initial actions to advance international collaboration to combat cyberterrorism. For example, the OSCE formation of the Action Against Terrorism Unit in 2002, now a part of the Transnational Threats Department, was stood-up as a key centralized information center for counter-terrorism activates, to include disrupting terrorist use of the internet.[20] Another noteworthy

[18] Stahl, *The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity*, Vol. 40University of Georgia School of Law, Georgia Journal of International & Comparative Law, 2011), 247-252.

[19] Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and using Universal Jurisdiction as a Deterrent*, Vol. 43 Vanderbilt Journal of Transnational Law, 2010), 63-65.

[20] OSCE Transnational Threats Department, *OSCE Anti-Terrorism Reference*,[2015]) 19-21.

example is the Council of Europe formation of the Convention of Cybercrime in 2001, a resource accessible by any state government developing national cybercrime legislation; it also provides a framework for international cooperation between nations.[21] The two examples are just the beginning and are not enough to deter cyberterrorism. Many nations are facing a cybersecurity crisis, and in the absence of actionable international governance cyber powers, to include China, Russia, UK, and the U.S. have developed and implemented national measures to confront this formidable threat.

As the predominate pioneer of the internet, the U.S. has taken the development of national cyber policy and law seriously in an attempt to secure its CNI. It started with the 1995 White Paper on Information Infrastructure Assurance. This document singled out banking and finance, energy services, and the defense industry base dependence on the internet making it vulnerable to disruptive cyber-attacks.[22] President Clint followed up on this foundation component with Presidential Decision Directive 63 to document specific facilities as CNI to take action to protect them. Section one of the directive stated

> …many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failure, human error, weather and other natural causes, and physical and cyber-attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security.[23]

[21] Council of Europe, "Action Against Economic Crime: Cybercrime," http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp (accessed April 4th, 2015).

[22] United States Government, *The National Strategy to Secure Cyberspace*,[2003]) 5-11.

[23] The White House, "PRESIDENTIAL DECISION DIRECTIVE/NSC-63: Critical Infrastructure Protection," http://fas.org/irp/offdocs/pdd/pdd-63.htm (accessed April 4th, 2015).

Successive Presidential administrations built on the progress made from these documents, in particular former President George W. Bush who formed the Department of Homeland Security in 2003 charging them with the task of national cybersecurity. At the end of his second term, President Bush also launched the Comprehensive National Cybersecurity initiative based on Homeland Security Presidential Directive 23 and National Security Presidential Directive 54.[24] The initiative goals were to identify current and potential cyber threats, protect CNI, and determine a response process to a cyber-attack. President Obama has proven to be a proactive cybersecurity leader, starting with signing of the Cybersecurity Act of 2009. The legislation formed a Cybersecurity Advisory Panel and declared the Department of Commerce to “serve as the clearinghouse of cybersecurity threats and vulnerability information”.[25] The President also tasked the Department of Defense to create an organization responsible for the planning, integrating, and if called upon, defense of military networks utilizing a full spectrum of cyberspace operations.[26] That organization is U.S. Cyber-Command, a force of more than 5,000 active duty cyber specialists working in parallel with the National Security Agency. Finally, the 2013 National Infrastructure Protection Plan fulfilled the President directive to update the 2009 plan. The mission of the document is to strengthen the security and resilience of CNI by proactively managing cyber risk through a collaborative effort from Federal, State, local, and other regional entities.[27]

[24] Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and using Universal Jurisdiction as a Deterrent*, Vol. 43Vanderbilt Journal of Transnational Law, 2010), 72-75.

[25] Ibid. 86-89.

[26] G. Roesener, Carl Bottolfson and Gerry Fernandez, "Policy for US Cybersecurity," *Air & Space Power Journal* 28, no. 6 (Nov, 2014), 38-45.

[27] Department of Homeland Security, *NIPP 2013 Partnering for Critical Infrastructure Security and Resilience* United States Government,[2013]) 1-5.

As expected, the U.S. is not the only nation or association concerned with and developing national-level or regional cybersecurity policy. The UK has elevated cyber-attacks as a grave threat to national security. To counter this aggression, the 2011 UK Cyber Security Strategy created the Center for the Protection of National Infrastructure, an organization designed to create and implement thorough standards while partnering with key private and public industry to enhance cybersecurity.[28] The end goal of this strategy is a comprehensive framework to protect CNI while providing guidance to both the private and public sectors. Expanding beyond the UK, the EU has recognized their unique situation and in 2008 established the European Programme for Critical Infrastructure Protection, a group charged with outlining a process to secure CNI. They followed up with the 2013 EU Cybersecurity Strategy with the priorities of cyber resilience, a reduction of cybercrime, the development of new policy, creating technological resources to support cybersecurity, and instituting an internationally recognized EU cyberspace policy.[29] Moving away from Europe, China has been active in cyber policy since the mid-1990s. The salient developments are the 2003 State Information Leading Group document 27 and the 2007 multi-level protection scheme articulating the plan to adopt a national assurance system designed with rigid domestic management.[30] As expected, the further development of this plan has been a source of tension with proponents of internet freedom promoters, as witnessed recently by China’s cybersecurity policy group demanding IT companies that supply Chinese financial

[28] Ministry of Defence, *Cyber Primer* Development, Concepts and Doctrine Centre,[2013]) 1-20.

[29] European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe, and Secure Cyberspace* (Brussels: High Representative of the European Union for Foreign Affairs and Security Policy,[2013]) 4-16.

[30] Amanda N. Craig and Scott J. Shackelford, "Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity," *Stanford Journal of International Law* 50, no. 1 (Winter2014, 2014), 157-165.

institutions to provide highly-sensitive source code to Chinese regulators and mandating the use of their encryption.[31]

It’s clear that nations are taking steps to address cybersecurity, but if the prevailing trend to develop domestic policy remains, the threat of international legal fragmentation remains high. According to Robert Knake, the 2011-2015 U.S. Director for Cybersecurity Policy at the National Security Council, what is clear is “states will play a significant role in shaping twenty-first century cyberspace”.[32] Although states have taken positive steps to combat cyberterrorism, according to U.S. National Security Advisor James Jones, while making remarks at the Munich Conference on Security Policy, “the steps taken to date are insufficient, greater international cooperation is needed”.[33] The advancements in national-level law, policy, and technology are important, but even the U.S. realizes that the need for a cybersecurity strategy intended to sculpt the international environment that brings nations together to tackle key common issues relating to technical criteria, legal foundation for territorial jurisdiction, and the use of force to counter cyberterrorism is needed.

[31] Krista Hughes, "U.S. Businesses Urge China to Postpone New Cybersecurity Policies," Reuters, http://www.reuters.com/article/2015/01/29/us-china-tech-security-idUSKBN0L12SQ20150129 (accessed April 5th, 2015).

[32] Shackelford and Craig, *Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity*, Vol. 50 Stanford Journal of International Law, 2014), 136-137.

[33] Council of Foreign Relations, "Remarks by National Security Adviser Jones at 45th Munich Conference on Security Policy," Primary Sources, http://www.cfr.org/world/remarks-national-security-adviser-jones-45th-munich-conference-security-policy/p18515 (accessed April 5th, 2015).

THE NEED FOR UNIVERSAL CYBERTERRORISM JURISDICTION

Significant national government and international organization progress has been made to confront the challenge of cyberterrorism, but much more must be done. At this point a comprehensive international legal framework to combat cyber aggression does not exist, therefore nations must work together to identify the various levels of cyberterrorism and to structure an international process to deal with this grave threat. To obtain an acceptable legal response to a cyber-attack, nations must first agree on a definition of cyberterrorism, in addition to the implementation of an international institute with the authority to examine and prosecute cyberterrorism acts regardless of the source of the attack.[34] Because nations currently turn to territorial jurisdiction and legal systems to respond to cyberterrorism, the process hinders an effective counteraction to stop current and future attacks. For example, the 2000 “Lovebug” virus creator affected 20 nations and cost an estimated 10 billion dollars in damage globally, but could not be prosecuted due to the Philippines, his home nation, did not outlaw this action and without an international recognized process the victim countries did not have a legal method to pursue charges.[35]

With the inherent internet architecture insecurities a practical prevention option is not possible, therefore deterrence is the best choice. Due to its ability to incapacitate a nation’s CNI with significantly less resources of traditional weapons of mass destruction, cyberterrorism will remain a weapon-of-choice. A key issue is cyber is a borderless

[34] Stahl, *The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity*, Vol. 40 University of Georgia School of Law, Georgia Journal of International & Comparative Law, 2011), 260-262.

[35] Mike Ingram, ""Love-Bug" Virus Damage Estimated at $10 Billion," World Socialist Web Site, https://www.wsws.org/en/articles/2000/05/bug-m10.html (accessed April 5th, 2015).

entity, an attack often comes from multiple computers located around the world, simultaneously launched impeding the attacked nations ability to pursue a legal remedy due to jurisdictional barriers.[36] Because of the restrictions of territorial jurisdiction, it serves as little to no deterrence to cyberterrorism. To overcome this hurdle, the use of universal cyberterrorism jurisdiction would be a much more effective deterrent because it "confers on any nation the authority to prosecute alleged international crimes, even when the prosecuting nation has no connection whatsoever with the offense".[37]

Supporting this argument is Doctor Mahmoud Bassiouni, a founding member of the International Human Rights Law Institute at DePaul University and the International Institute of Higher Studies in Criminal Sciences. He believes that due to the far-reaching capability of this method and the challenges of terrorists utilizing cyber as a global weapon, that the best way to deter cyberterrorism is through the use of universal jurisdiction.[38] Doctor Bassiouni points out treaties already recognize terrorism as an international crime, such as the Convention to Prevent and Punish Acts of Terrorism Taking the Form of Crimes Against Persons, therefore utilizing existing treaty law is one method with a strong basis to expand universal jurisdiction over cyberterrorism.[39] Additionally, widely published counterterrorism expert and Penn State University humanities and law Professor Jonathan Marks analyzed the extension of universal jurisdiction to deter cyberterrorism and documented several justifications. The first he

[36] The White House, *Cyber Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*,[2009]) 1-5.

[37] Luc Reydams, "Universal Jurisdiction: International and Municipal Legal Perspectives. Oxford: Oxford University Press, 2003, 258pp +xxvii. ISBN 0-19-925162-2," *Journal of Conflict & Security Law* 9, no. 1 (03, 2004), 127-132.

[38] Cherif Bassiouni, "Universal Jurisdiction for International Crimes: Historical Perspectives and Contemporary Practice," *Virginia Journal of International Law* 42, no. 81 (2001), 81.

[39] Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and using Universal Jurisdiction as a Deterrent*, Vol. 43 Vanderbilt Journal of Transnational Law, 2010), 100-104.

labeled “the common interest rational” which he states that nations are authorized to apply jurisdiction over acts of aggression that threaten national interests.[40] Another justification he calls “the agency rational”. The basis of this point is the prosecuting nation is representing the international community because the violations themselves represent an action that could be applied to any country.[41] And finally, Professor Marks presented “the harm rational”, what he thinks is the strongest support for universal jurisdiction, because the heinousness of the global exploits that result in physical and societal damage, to include psychological impairment, have the potential to disrupt entire governments and can be carried out again.[42]

Some would argue, such as Harvard Law School Professor and extensive writer in the field of international and cyber law, Jack Goldsmith, along with his colleague, Columbia Law School Professor and author of *The Master Switch*, named one of the top 100 books of 2010, Timothy Wu, that the internet is not a borderless realm or that it does fall within the control of territorial jurisdiction because the internet is slowly conforming to national regulations thus losing its traits that have traditionally been beyond state control.[43] Although national and international laws have begun to sprout, state control is limited to only certain aspects, such as limiting domain naming conventions and filtering content, no nation can control or prevent cyberterrorism from a national jurisdiction perspective. Additionally, cyberterrorist do not conform to state rules, they operate outside the “borders” to obtain their objectives. Therefore the best solution to counter

[40] Jonathan Marks, "Mending the Web: Universal Jurisdiction, Humanitarian Intervention, and the Abrogation of Immunity by the Security Council," *Columbia Journal of Transnational Law* 42, no. 2 (2004), 465-470.

[41] Ibid.

[42] Ibid.

[43] Jack Goldsmith, "Who Controls the Internet? Illusions of a Borderless World," *Strategic Direction* 23, no. 11 (10/23, 2007) 23.

cyberterrorism is the evolution of international law anchored in universal jurisdiction enabling a legal and measured response to a cyber-attack on a nation's CNI. Cyberterrorism will thrive if left undeterred. Although prosecution will be difficult, the complete lack of credible international law and jurisdiction will allow cyberterrorists to continue to operate without fear of being held accountable or facing repercussion.

CONCLUSION

Purdue University Professor Doctor Gene Spafford, the only person to receive all three U.S. National Computer Security Awards, stated "the only true secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards--and even then I have my doubts".[44] Cyberterrorism is today's weapon of mass disruption, a tactic capable of threating a nation's national security by targeting its CNI. As the internet continues to expand, intertwining economies and societies, cyber aggression will grow as a weapon-of-choice due to its ability to impact national governments globally. States and international organizations have taken this threat seriously and have developed significant cybersecurity products, but much more must be done. Through an international effort, states must deliberate approaches to create and implement cyber policy, to include adopting global cyber standards, to protect CNI while deterring cyberterrorist.

Unfortunately, because of inherent internet security vulnerabilities, complete prevention of cyberterrorism is not possible. Therefore, by conducting an analysis of the

[44] Craig and Shackelford, *Hacking the Planet, the Dalai Lama, and You: Managing Technical Vulnerabilities in the Internet through Polycentric Governance*, Vol. 24, 2014), 2-4.

underlying fundamental problems of the internet, identifying the evolution of key national and international cybersecurity policy and laws, and presenting a case for universal jurisdiction, this paper has clearly argued a feasible method to deter cyberterrorism. Amongst many vital issues, global economic growth and prosperity has become more dependent on internet commerce, therefore cyber has a direct impact on national security concerns. Because of this linkage states cannot afford to mold cybersecurity policy solely around national interests, an international inclusive effort must be made to create globally accepted cyber laws in addition to a process allowing effected nations to have legal recourse. Due to the unquestionable weaknesses of the internet, until the international community is willing to utilize universal jurisdiction to deter cyberterrorist as part of a layered cyber defense, cyberterrorist will continue to be undeterred enabling the development and release of cyber-attacks with the likelihood of increasing success.

BIBLIOGRAPHY

Bassiouni, Cherif. "Universal Jurisdiction for International Crimes: Historical Perspectives and Contemporary Practice." *Virginia Journal of International Law* 42, no. 81 (2001): 1.

Bellovin, S. M. "A Look Back at Security Problems in the TCP/IP Protocol Suite". IEEE Comput. Soc, 01/01, 2004.

Cabinet Office: National Security and Intelligence. *A Strong Britain in an Age of Uncertainty: The National Security Strategy*. Norwich, UK: TSO, 2010.

Council of Europe. "Action Against Economic Crime: Cybercrime." . Accessed April 4th, 2015. http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp.

Council of Foreign Relations. "Remarks by National Security Adviser Jones at 45th Munich Conference on Security Policy." Primary Sources. Accessed April 5th, 2015. http://www.cfr.org/world/remarks-national-security-adviser-jones-45th-munich-conference-security-policy/p18515.

Craig, Amanda N. and Scott J. Shackelford. "Beyond the New Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity." *Stanford Journal of International Law* 50, no. 1 (Winter 2014, 2014): 119-184.

Craig, Amanda N. and Scott J. Shackelford. "Hacking the Planet, the Dalai Lama, and You: Managing Technical Vulnerabilities in the Internet through Polycentric Governance." *Fordham Intellectual Property, Media and Entertainment Law Journal* 24, no. Winter 2014 (2014): 381.

Cross, Michael. "Whitehall must Learn from Estonia's e-Government." The Guardian. Accessed April 2nd, 2015. http://www.theguardian.com/technology/2007/may/24/society.insideit.

Department of Homeland Security. *NIPP 2013 Partnering for Critical Infrastructure Security and Resilience*: United States Government, 2013.

European Commission. *Cybersecurity Strategy of the European Union: An Open, Safe, and Secure Cyberspace*. Brussels: High Representative of the European Union for Foreign Affairs and Security Policy, 2013.

Gable, Kelly A. "Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and using Universal Jurisdiction as a Deterrent." *Vanderbilt Journal of Transnational Law* 43, no. 1 (01, 2010): 57-118.

Goldsmith, Jack. "Who Controls the Internet? Illusions of a Borderless World." *Strategic Direction* 23, no. 11 (10/23, 2007).

Heiser, Jay G. "Beyond Cryptography: Bruce Schneier's Beyond Fear: Thinking Sensibly about Security in an Uncertain World." *Computers & Security* 22, no. 8 (12, 2003): 673.

Hollis, David. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal* (2010): 1.

Hughes, Krista. "U.S. Businesses Urge China to Postpone New Cybersecurity Policies." Reuters. Accessed April 5th, 2015. http://www.reuters.com/article/2015/01/29/us-china-tech-security-idUSKBN0L12SQ20150129.

Ingram, Mike. ""Love-Bug" Virus Damage Estimated at $10 Billion." World Socialist Web Site. Accessed April 5th, 2015. https://www.wsws.org/en/articles/2000/05/bug-m10.html.

Internet World Stats: Usage and Population Statistics. "Internet Growth Statistics: Today's Road to e-Commerce and Global Trade Internet Technology Reports". Accessed April 2nd, 2015. http://www.internetworldstats.com/emarketing.htm.

Kounavis, Michael, Xiaozhu Kang, Ken Grewal, Mathew Eszenyi, Shay Gueron, and David Durham. "Encrypting the Internet." *ACM SIGCOMM Computer Communication Review (ACM Digital Library)* 41, no. 4 (10/22, 2011): 135-146.

Leiner, Barry, Vinton Cerf, David Clark, Robert Kahn, Leonard Kleinrock, Daniel Lynch, Jon Postel, Larry Roberts, and Stephen Wolff. "A Brief History of the Internet." *ACM SIGCOMM Computer Communication Review (ACM Digital Library)* 39, no. 5 (10/01, 2009): 22-31.

Marks, Jonathan. "Mending the Web: Universal Jurisdiction, Humanitarian Intervention, and the Abrogation of Immunity by the Security Council." *Columbia Journal of Transnational Law* 42, no. 2 (2004): 445.

Ministry of Defence. *Cyber Primer*: Development, Concepts and Doctrine Centre, 2013.

OSCE Transnational Threats Department. *OSCE Anti-Terrorism Reference*, 2015.

"PRESIDENTIAL DECISION DIRECTIVE/NSC-63: Critical Infrastructure Protection". Accessed April 4th, 2015. http://fas.org/irp/offdocs/pdd/pdd-63.htm.

Reydams, Luc. "Universal Jurisdiction: International and Municipal Legal Perspectives. Oxford: Oxford University Press, 2003, 258pp +xxvii. ISBN 0-19-925162-2." *Journal of Conflict & Security Law* 9, no. 1 (03, 2004): 127-132.

Roebuck, Kevin. *Cybersecurity: High-Impact Strategies - What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors*: Emereo Publishing, 2012.

Roesener, G., Carl Bottolfson, and Gerry Fernandez. "Policy for US Cybersecurity." *Air & Space Power Journal* 28, no. 6 (Nov, 2014): 38-54.

Shackelford, Scott J. "Estonia Three Years Later: A Progress Report on Combating Cyber Attacks." *Journal of Internet Law* 13, no. 8 (02, 2010): 22-29.

Stahl, William M. "The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity." *Georgia Journal of International & Comparative Law* 40, no. 1 (Fall2011, 2011): 247-273.

The White House. *Cyber Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, 2009.

The White House Office of the Press Secretary. Accessed April 3rd, 2015. https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

United States Government. *The National Strategy to Secure Cyberspace* , 2003.

Zittrain, Jonathan L. "The Generative Internet." *Harvard Law Review* 119, no. 7 (05, 2006): 1975-2040.