STATE RESPONSIBILITY FOR CYBER ATTACKS: COMPETING STANDARDS FOR A GROWING PROBLEM

SCOTT J. SHACKELFORD & RICHARD B. ANDRES*

At a time in which the unchecked sovereign authority of States is being challenged across many arenas, State responsibility remains a key component of international security. However, defining State responsibility in cyberspace has proven to be difficult given both the speed and anonymity of cyber attackers. Sponsoring States may, for example, incite groups to commit cyber attacks and then hide behind a (however sheer) veil of plausible deniability to escape accountability. This Article analyzes potential legal regimes of State responsibility to help hold these State sponsors of cyber attacks more accountable, including the effective and overall control standards. Other lesser-known standards are also reviewed, including the governmental awareness and the sliding scale approach. These regimes are then applied to real examples of State sponsorship, from the Estonian cyber militia to cyber criminals in Africa, including instances of neutral States allowing their networks to be used for launching cyber attacks thus giving rise to problems of neutrality and distinction that is analyzed under the Law of Armed Conflict. The Article concludes by arguing for the adoption of a flexible standard of State responsibility for cyber attacks given the extreme difficulties involved with proving the identity of cyber attackers.

TABLE OF CONTENTS

* Scott J. Shackelford is an Assistant Professor of Business Law and Ethics at Indiana University, Kelley School of Business. He is a graduate of Stanford Law School, a Ph.D. candidate in international relations at the University of Cambridge, and author of the forthcoming book *Cyber Peace: Countering Cyber Attacks in International Law, Business, and Relations*, being published by Cambridge University Press. He wishes to thank his lovely wife, Emily, for all of her help and support, as well as his colleagues at Indiana University for their helpful comments including David Fidler and Fred Cate. He would also like to thank Evan Sarosi for his invaluable research support throughout this project, as well as the Indiana University Center for International Business Education and Research, the Center for Applied Cybersecurity Research, the Boren fellowship program, and the fantastic staff at the Institute for National Security Studies. Dr. Richard B. Andres is Professor of National Security Strategy at the U.S. National War College, and Senior Fellow and Chair of EESP at the Institute for National Strategic Studies at National Defense University. The views expressed in this article are those of the author and do not necessarily represent the official policy or position of the U.S. government. © 2011, Scott J. Shackelford and Richard B. Andres..

I. INTRODUCTION

At the height of the Cold War in June 1982, an American early-warning satellite detected a large blast in Siberia. A Soviet gas pipeline had exploded. The explosion was the result of a CIA-sponsored logic bomb planted in software that Soviet spies had stolen from a Canadian software company. The result was "the most monumental non-nuclear explosion and fire ever seen from space."[1] And that was almost thirty years ago.

Flash forward to September 2010 and the discovery of the Stuxnet worm—a sophisticated "cyber weapon" reportedly designed to target Iran nuclear facilities, specifically the centrifuges at its nuclear refinery at Natanz. The worm exploited flaws in Microsoft Windows to disrupt the operation of specific plant processes that were controlled by Siemens-manufactured industrial control systems. However, an estimated 44,000 other computers around the world were also affected and critical infrastructure in systems as far away as Germany and the United

[1] *Cyberwar: War in the Fifth Domain*, ECONOMIST, July 3, 2010, at 25.

States sustained damage.[2] The worm's unusual complexity led some to conclude that the attackers had the backing of one or more national governments, rather than being the work of cyber criminals or terrorists. For example, this cyber shot heard round the world utilized stolen digital certificates to mask its malicious code, modified software to cause the Iranian centrifuges to spin at speeds that reportedly damaged 1,000 of them, and incorporated features to terminate the worm's activities on a set date.[3] Many analysts attributed the attack to Israel or the United States.[4] Stuxnet may be viewed as the first salvo in a new era of cyberwar, which is why James Lewis of the Center for Strategic and International Studies (CSIS) a think-tank in Washington, D.C., labeled this event as potentially "the first act of cyberwarfare."[5] Since the threshold defining armed attacks in cyberspace remain controversial, this statement remains contentious. Others for example maintain that the attack was at most a covert action, as is discussed below.

While there is a good deal of agreement on the likely identity of the Stuxnet attackers, that is not the case in the vast majority of cyber attacks.[6] The "Conficker" worm, for instance, was a global malware program starting in late 2008 that infected millions of computers including systems in the French Navy, the Bundeswehr (German Federal Defense Force), and the U.K. Ministry of Defense, but it is still not known publically who launched the attacks, why, and whether the malware has even been fully removed.[7] (If governments know who released the worm they are not talking.) Situations such as this highlight the fundamental problem of attribution in cyberspace.

Stuxnet lays bare the open question of what the true potential of a

[2] Sharon Weinberger, *U.S. Also Vulnerable to Stuxnet Virus, Official Warns*, AOL NEWS (Dec. 7, 2010), http://www.aolnews.com/nation/article/us-also-vulnerable-to-stuxnet-virus-official-warns/19750249; *see also* William Jackson, *In Cyberspace, a Good Offense is NOT Always the Best Defense*, GOV'T COMPUTER NEWS (Nov. 29, 2010), http://gcn.com/articles/2010/11/29/stuxnet-reveals-cyber-war-folly.aspx.

[3] *See* Nicolas Falliere, Liam O. Murchu, & Eric Chien, W32: Stuxnet Dossier (Symantic Security Response, Version 1.4, Feb. 2011).

[4] *See, e.g.*, William J. Broad, John Markoff & David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES, Jan. 16, 2011, at A1.

[5] *See Are 'Stuxnet' Worm Attacks Cyberwarfare?*, NPR SCI. FRIDAY (Oct. 1, 2010), http://www.npr.org/templates/story/story.php?storyid=130268518; *see also The Meaning of Stuxnet*, ECONOMIST, Oct. 2, 2010, at 14.

[6] In this Article, the term "cyber attack" is used broadly to refer to a broad range of computer network intrusions including cyber exploitation.

[7] *See* THE RENDON GRP., CONFICKER WORKING GROUP: LESSONS LEARNED 2 (2011), *available at* http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf.

logic bomb or other cyber attacks is today now that everything from stock exchanges to national power grids are connected to a ubiquitous Internet. And it is not just cyberwarfare that is a growing problem: cyber espionage, terrorism, and cybercrime are also on the rise. President Obama has stated that $1 trillion was lost to cybercrime in 2009, a figure greater than the global market in illegal drugs.[8] This revelation prompted Rhode Island Democrat Sheldon Whitehouse to argue, "I believe we are suffering what is probably the biggest transfer of wealth through theft and piracy in the history of mankind."[9] The array of threats facing cyberspace has caused it to become the fifth domain of combat, after land, sea, air, and space.[10] But determining an appropriate legal regime to regulate this new domain incorporating *jus ad bellum* (the right to wage war) and *jus in bello* (justice in war) elements has proven to be elusive, particularly with regards to the central problem of proving attribution and State responsibility.

At a time in which the unchecked sovereign authority of States is being challenged across many arenas, State responsibility remains a key bulwark of international security.[11] But the speed and anonymity of cyber attacks makes proving State responsibility and "distinguishing among the actions of terrorists, criminals, and nation states difficult."[12] As the 2007 cyber attacks on Estonia demonstrated, a State hosting groups that make attacks for reasons that benefit the State rarely cooperates in the investigation, apprehension, and extradition of those who committed that attack.[13] Moreover, there is an open question as to

[8] *See Cyberwar*, *supra* note 1, at 25.

[9] Tim Starks, *Cybersecurity: Learning to Share*, CQ POLITICS (Aug. 1, 2010), http://www.cqpolitics.com/wmspage.cfm?docID=weeklyreport-000003716158&cpage=1.

[10] *See* JAMES A. LEWIS, CTR. FOR STRATEGIC & INT'L STUDIES, THE "KOREAN" CYBER ATTACKS AND THEIR IMPLICATIONS FOR CYBER CONFLICT 2 (2009). Note, the Department of Defense labeled cyberspace a military domain in 2006. *See* PETER PAGE, CHAIRMAN OF THE JOINT CHIEFS OF STAFF, THE NATIONAL MILITARY STRATEGY FOR CYBERSPACE OPERATIONS 2 (2006), *available at* http://www.dod.mil/pubs/foi/ojcs/07-F-2105doc1.pdf.

[11] DAVID HELD, MODELS OF DEMOCRACY 293–97 (2006); *see generally* ROBERT B. REICH, THE WORK OF NATIONS: PREPARING OURSELVES FOR 21ST-CENTURY CAPITALISM (1991). On the problems with attribution see, for example, Christopher C. Joyner & Wayne P. Rothbaum, *Libya and the Aerial Incident at Lockerbie: What Lessons for International Extradition Law?*, 14 MICH. J. INT'L L. 222, 229 (1993). *But see* Susan W. Brenner & Anthony C. Crescenzi, *State-Sponsored Crime: The Futility of the Economic Espionage Act*, 28 HOUS. J. INT'L L. 389 (2006); Douglas R. Burgess, Jr., Hostis Humani Generi: *Piracy, Terrorism and a New International Law*, 13 U. MIAMI INT'L & COMP. L. REV. 293, 302–03 (2006).

[12] WHITE HOUSE, NATIONAL STRATEGY TO SECURE CYBERSPACE, at viii (2003).

[13] *See, e.g.*, Agreement on Legal Assistance and Legal Relations in Civil, Family and Criminal Matters, Est.-Russ., Jan. 26, 1993, Riigi Teataja II 1993, at 16, 27.

whether these attacks should be characterized as: cybercrimes, with Russian Nashi hackers orchestrating a coup; cyber terrorism by a group pursuing idiosyncratic ideological goals; cyberwarfare, a virtual sortie by Russian intelligence operatives; or merely a cyber riot? Determining these classifications and the distinctions between them shapes responses and retaliation, including the proper involvement of civilian law enforcement or the military if necessary.

Given the secretive nature of cyber conflict, States may incite civilian groups within their own borders to commit cyber attacks and then hide behind a (however sheer) veil of plausible deniability, thus escaping accountability. The well-documented use of patriotic hackers by several governments, including China and Russia, as well as the rise of cyber militias in countries such as Estonia speaks to the urgent necessity of resolving the critical question of State responsibility. This Article analyzes potential legal regimes of State responsibility for cyber attacks, including the effective and overall control standards. In brief, the effective control doctrine, originating in the International Court of Justice (ICJ) *Nicaragua* case, recognizes a country's control over paramilitaries or other non-State actors only if the actors in question act in "complete dependence" on the State.[14] In contrast, the overall control doctrine, illustrated in the International Criminal Tribunal for the Former Yugoslavia *Tadic* case, held that where a State has a role in organizing and coordinating, in addition to providing support for a group, it has sufficient overall control so that the group's acts are attributable to the State.[15] Other lesser known standards will also be reviewed, including the governmental awareness and the sliding scale approaches.[16] These regimes will then be applied to real examples of State-sponsored cyber attacks, including Russia's alleged attacks on Estonia. The applications focus on instances of neutral States that allow their networks to be used as launching points for cyber attacks, thus giving rise to the problems of neutrality and distinction that will be analyzed under the Laws of Armed Conflict.

[14] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 110 (Jun. 27) [hereinafter "Nicaragua"].

[15] Prosecutor v. Tadic, Case No. IT-94-1-I, Decision on Defense Motion for Interlocutory Appeal on Jurisdiction (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995) [hereinafter "Tadic"].

[16] *See generally* Scott J. Shackelford, State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem (Jan. 12, 2010) (unpublished conference paper presented at the CCD NATO Conference on Cyber Conflict held in Tallinn, Estonia, July 15–18, 2010), *available at* http://ssrn.com/abstract=1535351.

The Article is structured as follows. In section II, we construct a brief literature review on the question of appropriate standards governing State responsibility for cyber attacks before summarizing some of the myriad technical challenges raised by tracing cyber attacks in section III. Section IV discusses the fundamental problem of attribution in cyberspace as well as the cases for and against various legal regimes of State responsibility as applied to cyber attacks, including the effective and overall control standards. Finally, section V analyzes the debate on the applicability of the Law of Armed Conflict to cyberspace, particularly efforts aimed at defining the armed attack threshold. This is used as a jumping off point for a discussion on the importance of State responsibility within the context of neutrality and distinction in cyber operations. These findings are then applied to several cyber operations including the Estonian Cyber Defence League and more recent attacks emanating from unsecured African networks. On account of the extreme difficulties involved in tracing cyber attacks and proving attackers' identity and intent, we conclude by arguing for the adoption of flexible standards of State responsibility for cyber attacks, but offer the cautionary note that this may enforce the prevailing status quo strategic ambiguity.

II. THE NEW CYBERWARFARE: DEFINITIONS & LITERATURE REVIEW

On January 12, 2010, corporate America was compromised again as cyber attacks being reportedly directed by the Chinese Politburo stole intellectual property from Google along with that of 40 other corporations,[17] mostly located within the United States.[18] In this case, the attackers employed a tactic known as "phishing," in which e-mail is sent from someone the user supposedly knows and trusts.[19] Once opened, infected attachments download "malware" onto the host's computer, allowing the hackers access to confidential information stored within the user's network. Although Google has stated that little if any of its property was lost, similar cyber attacks have led to the theft of gigabytes

[17] Tom Gjelten, *Secret Cable: China Said To Coordinate Google Attack*, NAT'L PUB. RADIO (Dec. 7, 2010), http://www.npr.org/2010/12/07/131863666/secret-cable-china-said-to-coordinate-google-attack.

[18] *See* Scott Shackelford, *Google Needs Help Against Online Attackers*, S.F. CHRONICLE, Jan. 24, 2010, at E4.

[19] *See* Tim Greene, *Chinese attacks like the one against Google are on pace to double this year*, ITWorld.com, Mar. 4, 2010, http://www.itworld.com/security/98982/chinese-attacks-one-against-google-are-pace-double-year.

of sensitive information in recent years.[20]

Many cybersecurity experts have called the attack on Google routine. Indeed it was. Nearly half of more than 22 million computers scanned for malware as part of a recent survey were found to be infected.[21] Some sources estimate that between one-quarter and one-third of all home computers worldwide are infected, to say nothing of phones, printers, and other devices with Internet connections. These ubiquitous, unsecured systems have allowed for myriad system breaches across companies and countries alike. For instance, Symantec reported in February 2010 that during the previous 12 months, 75% of businesses had experienced cyber attacks causing average losses of $2 million per year.[22] According to U.S. Senator Susan Collins, more than 1.8 billion cyber attacks are being launched against U.S. government websites each month.[23] This means that the United States is "under cyber attack virtually all the time," according to Defense Secretary Robert Gates.[24] This state of affairs prompted Lewis to state: "We have a faith-based approach, in that we pray every night nothing bad will happen."[25]

What can the U.S. government do in response? Not enough. It has been reported that while the U.S. State Department made a formal protest to Chinese authorities over the Google incident,[26] China, not surprisingly, denied any State involvement.[27] Why are we unable to be

[20] *See, e.g.*, *Intellectual Property Theft Fuels Underground Cyber Economy*, VENTUREBEAT (Mar. 27, 2011), http://venturebeat.com/2011/03/27/intellectual-property-theft-fuels-the-underground-cyber-economy.

[21] *See* Dancho Danchev, *Report: 48% of 22 million scanned computers infected with malware*, ZDNET, Jan. 27, 2010, *available at* http://www.zdnet.com/blog/security/report-48-of-22-million-scanned-computers-infected-with-malware/5365.

[22] *Symantec 2010 State of Enterprise Security Study Shows Frequent, Effective Attacks on Worldwide Business*, SYMANTEC (February 22, 2010), http://www.symantec.com/about/news/release/article.jsp?prid=20100221_01.

[23] *See* Steve Mistler, *Legislation Wouldn't Give President Internet Kill Switch, Collins Says*, SUN J., (Feb. 3, 2011, 12:00 AM), http://www.sunjournal.com/state/story/980334. Note the disparity between the figures offered by Senator Collins and the number of cyber attacks reported by CERT. This underscores the extent to which information sharing is problematic in the cybersecurity arena.

[24] *Gates: Cyber Attacks A Constant Threat*, CBS NEWS (Apr. 21, 2009), http://www.cbsnews.com/stories/2009/04/21/tech/main4959079.shtml.

[25] *See* Ken Dilanian, *Privacy Group Sues to Get Records About NSA-Google Relationship*, L.A. TIMES (Sep. 14, 2010), http://www.latimes.com/business/la-fi-nsa-google-20100914,0,5669294.story.

[26] Cecilia Kang, *Hillary Clinton Calls for Web Freedom, Demands China Investigate Google Attack*, WASH. POST (Jan. 22, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/01/21/AR2010012101699.html.

[27] *China Rejects Claims of Cyber Attacks on Google*, BBC News (Jan. 24, 2010), http://news.bbc.co.uk/2/hi/8478005.stm.

more assertive about these problems? The problems are two-fold. First, it is very difficult to prove who actually orchestrates cyber attacks. The science of tracing such attacks is advancing, as is discussed in section III, but remains largely circumstantial. But more importantly for present purposes, the legal regime governing cyber attacks is poorly defined, especially regarding State responsibility. With an increasing number of cyber attacks originating from sophisticated cyber criminals, "hackivists," and State-sponsored patriotic hackers, a new era of cyberwarfare is emerging.

What are the characteristics of the new cyberwarfare? To answer that, it is first necessary to reexamine classic cyberwarfare. Definitions vary, but "cyberwarfare" generally refers to an attack by one hostile nation against the computers or networks of another to cause disruption or damage (as compared to a criminal or terrorist attack involving private parties). From a U.S. military perspective, cyberwar is termed "computer network operations" (CNO) and includes computer network defense and exploitation involving the offensive and defensive use of IT to protect critical national infrastructure and eliminate cyber threats to U.S. Department of Defense computers or networks.[28] The specific doctrine of cyberwar is a classified and still evolving topic in U.S. defense circles, but prevailing military doctrine calls for U.S. dominance across all domains of warfare, including cyberspace. Consequently, the U.S. Department of Defense doctrine calls for using cyber attacks to "attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure."[29] Simply put, no options are off the table when it comes to securing "U.S. military strategic superiority in cyberspace."[30] The United States has achieved a great deal of success in remaining dominant in offensive cyber attack capabilities as seen during a number of campaigns ranging from the Balkans to

[28] Computer network defense is a military term referring to "actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity against or within DOD information systems and computer networks," while computer network exploitation refers to operations conducted through "the use of computer networks to gather data from target or adversary automated information systems or networks." *See Computer Network Operations and Network Warfare Operations*, CYBERSPACE & INFORMATION OPERATIONS STUDY CENTER, *available at* http://www.au.af.mil/info-ops/netops.htm.

[29] *Id.*

[30] *See* CHAIRMAN OF THE JOINT CHIEFS OF STAFF, U.S. DEP'T OF DEF., NATIONAL MILITARY STRATEGY FOR CYBERSPACE OPERATIONS (2006) *available at* http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf (defining cyberspace as "A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures") (emphasis removed).

the invasion of Iraq and arguably remains the world's foremost cyber power. But, due in part to U.S. successes, other actors are entering the fray, creating a new era in cyber operations.

Today, though lists vary, the cyber powers include the United States, the United Kingdom, China, Russia, Germany, France, and Israel. Some of these powers use the strategic ambiguity in cyberspace to undertake espionage on a hitherto unfathomable scale. As Stephen Chabinsky, a senior FBI official responsible for cybersecurity explains: "A spy might once have been able to take out a few books' worth of material, now they take the whole library. And if you restock the shelves, they will steal it again."[31] Between August 2007 and August 2009, at least 71 U.S. government agencies, contractors, universities, and think tanks with connections to the U.S. military have suffered penetration through cyber espionage, some multiple times. According to a congressional commission, these include many of the 10 most prominent U.S. defense contractors, among them Raytheon, Northrop Grumman, Boeing, and Lockheed Martin, the latter of which may have lost plans for the F-35 Joint Strike Fighter.[32] Estimates place losses to cybercrime at more than one trillion dollars.[33] Despite the prevalence of cybercrime, only 17% of companies have reported electronic crime losses to law enforcement agencies.[34] Part of the reason for this apathy may stem from the fact that the global dimension of cybercrime makes jurisdiction and prosecution difficult at best, in large part due to the attribution problem.

Thus, in this new era of cyberwarfare, the leading actors remain nations even as the list of cyber powers continues to lengthen. But non-State actors, including commercial entities, terrorist groups, and especially organized crime complicate the picture, such as when States hire cyber criminals as mercenaries to launch cyber attacks against other States.[35] It is these activities, cybercrime, and State-sponsored espionage, that are the activities "currently dominat[ing] cyber conflict"[36] rather than governments attacking one another in cyberspace,

[31] *See Cyberwar, supra* note 1, at 25.

[32] *See* Keith Epstein, *China Stealing U.S. Computer Data, Says Commission*, BUS. WK. (Nov. 21, 2008, 4:01 PM), http://www.businessweek.com/bwdaily/dnflash/content/nov2008/db20081121_440892.htm; Siobhan Gorma, August Cole & Yochi Dreazen, *Computer Spies Breach Fighter-Jet Program*, WALL ST. J., Apr. 21, 2009, http://online.wsj.com/article/SB124027491029837401.html.

[33] *Cyberwar, supra* note 1, at 25.

[34] *See* JOSEPH F. GUSTIN, CYBER TERRORISM: A GUIDE FOR FACILITY MANAGERS 139 (2004).

[35] *Id.* at 2.

[36] LEWIS, *supra* note 10, at 2.

or indeed cyber terrorism, which remains rare.[37] Indeed, there has not yet been a genuine cyber war.[38] Neither cybercrime nor espionage can rise to the level of an act of war, even with State complicity. As Lewis argues, "[t]he individuals and nations that engage in these activities do not think of themselves as engaging in warfare, at least as our current rules define it, and the lack of international norms for cyberspace only reinforces this sense of impunity."[39] For a cyber attack to be an act of war, it would have to be the equivalent of an armed attack, which is discussed below. In this new era of cyberwarfare in which an increasing number of State and non-State actors are vying for intelligence, military advantage, and economic competitiveness, State responsibility remains a key component of cybersecurity—a fact that has garnered insufficient attention in the literature to date.[40]

Much of the existing scholarship has only obliquely dealt with burdens of proof and the issue of State responsibility for cyber attacks in international law. The more popular works, such as Richard Clarke's *Cyber War*, are focused on national security but largely neglect the importance of State responsibility as a means of increasing accountability.[41] Some legal works note that armed coercion is generally chargeable to States more so than other forms of coercion, but do not address the burden of proof needed to constitute attribution.[42] Other articles adopt *Nicaragua's* framework as applied to non-State actors, but fail to discuss the benefits and drawbacks of this approach.[43] While much of the existing scholarship focuses on cyber terrorism by non-State actors,

[37] Part of the reason for this relative inactivity may be due to the tacit cooperation between cyber criminals and host nations, which has the benefit of constraining support for cyber terrorism. While financial crimes, the theft of IP, and extortion may be tolerated, cyber attacks against the host State or other nations that threaten to escalate hostilities are not. As Lewis states, "[t]he political environment in which the most advanced cyber criminals exist militates against them becoming mercenaries for many terrorist groups without the consent of their host." *Id.* at 8.

[38] *Id.* at 2.

[39] *Id.*

[40] In a worst case scenario cyber attack, factories and chemical plants explode, satellites spin out of control, the power grid fails, financial systems fall into turmoil, and societies begin to self-destruct. *See generally* RICHARD CLARKE & ROBERT KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT (2010).

[41] *Id.*

[42] *See* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 7 COLUM. J. TRANSNAT'L L. 885, 885 (1998).

[43] *See* Arie J. Schapp, *Cyberlaw Edition: Cyber Warfare Operations, Development and Use Under International Law*, 64 AIR FORCE L. REV. 121, 143–146 (2009).

such as Dan Verton's *Black Ice: The Invisible Threat of Cyberterrorism,*[44] the topics of corporate liability, State responsibility, attribution, and sovereignty have been almost entirely ignored in recent works on cyberwarfare.[45] There is thus a relative paucity of literature dealing with cyber attacks through the lens of international law and relations, to say nothing of the ethical and human rights implications of cyber attacks.[46]

Nor has the growing literature on Internet governance applied its findings to the question of State responsibility for cyber attacks.[47] Even those recent works that do address cyber attacks and critical infrastructure protection do so primarily from a U.S.-centric vantage point, such as Cordesman's *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection,*[48] or Lulasik's *Protecting Critical Infrastructures Against Cyber-Attack.*[49] Consequently, there is an important gap in international law literature that this Article addresses by explicitly laying out the cases for and against each potential regime of State responsibility for cyber attacks along with their strengths and weaknesses. However, before the respective legal options for state responsibility are examined, a brief introduction of the technical challenges of tracing cyber attacks is warranted.

III. THE SCIENCE OF TRACING CYBER ATTACKS

The science of tracing cyber attacks is primitive at best. Sophisticated attacks by knowledgeable hackers, whether private or state-sponsored, are nearly impossible to trace to their source using modern practices.[50]

[44] *See* DAN VERTON, BLACK ICE: THE INVISIBLE THREAT OF CYBERTERRORISM (2003); *see also* JOHNNY RYAN, COUNTERING MILITANT ISLAMIST RADICALISATION ON THE INTERNET: A USER DRIVEN STRATEGY TO RECOVER THE WEB (2007).

[45] *See* LECH JANCZEWSKI & ANDREW M. COLARIK, CYBER WARFARE AND CYBER TERRORISM (2008).

[46] *See, e.g.,* Jonathan B. Wolf, *War Games Meets the Internet: Chasing 21st Century Cybercriminals With Old Laws and Little Money,* 28 AM. J. CRIM. L. 95 (2000); Debra Wong Yang et al., *Countering the Cyber-Crime Threat,* 43 AM. CRIM. L. REV. 201 (2006).

[47] *See* Lawrence Lessig, *The Law of the Horse: What Cyberspace Might Teach,* 113 HARVARD L. REV. 500 (1999) (proposing that the law, markets, social norms, and architecture each be viewed as distinct models for regulating human action); D. Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons,* 91 CALIF. L. REV. (2003); D. Johnson & D. Post, *Law and Borders—The Rise of Law in Cyberspace,* 48 STAN. L. REV. 1367 (1996).

[48] *See* JUSTIN CORDESMAN, CYBER-THREATS, INFORMATION WARFARE, AND CRITICAL INFRASTRUCTURE PROTECTION (2002).

[49] *See* STEPHEN LULASIK, PROTECTING CRITICAL INFRASTRUCTURES AGAINST CYBER-ATTACK (2003).

[50] *See generally* HOWARD F. LIPSON, CERT COORDINATION CTR., TRACKING AND TRACING CYBER-ATTACKS: TECHNICAL CHALLENGES AND GLOBAL POLICY ISSUES 5 (2002), *available at* http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA408853&Location=U2&doc=GetTRDoc.pdf.

The current foundation of network communications in cyberspace, the Transmission Control Protocol (TCP) and the Internet Protocol (IP), dates back to 1982.[51] It is this antiquated system of communication designed for a small number of academic and governmental researchers sharing information with low risks of system breaches that represents the crux of the problem in tracing cyber attacks.[52] An IP packet can be intercepted or spoofed mid-route, making it impossible to trace. Thus, while in theory it is possible to trace the IP addresses of cyber attackers and use that information to locate them, "sophisticated hackers are able to re-route or otherwise confuse programs designed to locate them."[53] Similarly, if a hacker uses a botnet to carry out attacks, the process of tracing IP packets becomes much more time and resource intensive.

Of course, TCP/IP is not the only problem—system vulnerabilities are multiplied when considering the myriad problems with often rushed to market commercial off-the-shelf software, which is often rife with "technical debt."[54] Other issues include the facts that the Internet was never designed to track, or trace users, or to resist untrustworthy users; a packet's source address itself is untrustworthy and is easily masked; and there are myriad strategies that hackers employ, such as tunneling and data log destruction, which makes tracking difficult. Ultimately, the current threat environment in cyberspace exceeds the Internet's design parameters. But the primary overarching issue is that the current system was designed for a small number of trustworthy and tech savvy researchers, which is simply no longer the case with more than two billion Internet users worldwide.

Can the cyber infrastructure be modernized to enhance security and stop cyber attacks once and for all? The short answer is yes, but not easily. Some, like Mike McConnell, former director of National Intelligence, remain adamant that the Internet needs to be re-engineered to enable tracing cyber attacks: "We need to re-engineer the Internet for attribution, geolocation, intelligence analysis, and impact assess-

[51] *Id.* at 5.

[52] *Id.* at 14.

[53] *See generally* Scott Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192 (2009).

[54] "Technical debt" is an engineering term used here to refer to software that is rushed to market with multiple system vulnerabilities. *See* Ward Cunningham, Experience Report: The WyCash Portfolio Management System, Address at the Seventh Annual Conference on Object-Oriented Programming Systems, Languages, and Applications, 18–22 October 1992, Vancouver, British Columbia (Mar. 16, 1992), *available at* http://c2.com/doc/oopsla92.html.

ment."[55] But this is not going to happen, at least in the short term, according to Ian Brown of the Oxford Internet Institute among others—even if the United States put its full weight behind the proposal. Changes of this magnitude are slow, costly, and difficult to implement. As a case in point, consider how slowly the move to Internet Protocol Version 6 (IPv6) has been.[56] And many people are not convinced that the architecture should be overhauled, as it would likely mean forgoing even the semblance of anonymity and privacy on the Internet.

While full-fledged reengineering is a dim possibility, alternative strategies for dealing with attribution are promising. Technologies pioneered by the U.S. Cyber Emergency Response Team (USCERT) such as the use of probabilistic traceback techniques to audit a small percentage of packets have great potential and would ease the process of locating distributed denial of service (DDoS) attack sources.[57] It is also possible to trace individual IP packets back to their addresses, though this is much more difficult.[58] In the aftermath of the DDoS attacks against Estonia in 2007, cybersecurity experts followed attacks back to the zombie computers that formed botnets and then watched as these computers phoned home, eventually finding the highest-level controlling devices.[59] Microsoft's Scott Charney has written that it is possible to increase attribution "through wider application of existing strong authentication technology (along with appropriate auditing), through more effective technical trace-back mechanisms (when legally permitted), or through more streamlined international assistance (in cases where foreign assistance is practical)."[60] However, there is always going to be some level of anonymity online, especially for tech-savvy users familiar with products designed to enhance privacy and help mask identification.[61] Attribution will thus remain a "huge technical

[55] Mike McConnell, *McConnell on how to win the cyber-war we're losing*, WASH. POST, Feb. 28, 2010.

[56] *See Ipv6 Factsheet*, ICANN (Oct. 26, 2007), http://www.icann.org/en/announcements/announcement-26oct07.htm (noting that IPv6 was first proposed in 1996 and has yet to see fruition).

[57] *See* Rex Hughes, *A Treaty for Cyberspace*, 86(2) INT'L AFF. 523; 541 (2010).

[58] Lipson, *supra* note 50, at 27.

[59] CLARKE & KNAKE, *supra* note 40, at 15.

[60] SCOTT CHARNEY, MICROSOFT CORP., RETHINKING THE CYBER THREAT: A FRAMEWORK AND PATH FORWARD 8 (2009), *available at* http://www.microsoft.com/downloads/en/details.aspx?displaylang=en&FamilyID=062754cc-be0e-4bab-a181-077447f66877.

[61] *See* Jonathan Mayer, *There's Anonymity on the Internet. Get over It.*, FREEDOM TO TINKER (Oct. 27, 2009), http://www.freedom-to-tinker.com/blog/jrmayer/there%E2%80%99s-anonymity-internet-get-over-it; *see also* Mike Perry, *Meet the Torbutton Developer*, MOZILLA FIREFOX, https://

problem" for the foreseeable future according to Jonathan Mayer of the Stanford Computer Science Department Security Laboratory, the least of which is because some nations are weary of developing advanced transparent tracing techniques since this would hamper the activities of militias and intelligence agencies.[62]

A full review of the myriad technical issues and their potential solutions is beyond the scope of this Article. Simply put, though improvements in attribution capabilities are possible through wider application of existing authentication technologies and traceback mechanisms, these countermeasures are unlikely to ever offer a complete solution to the problem. Cyber attacks will likely continue to proliferate both in numbers and severity; the question then is how they should best be dealt with under international law and through international collaboration.

Technological capabilities aside though, attribution is more than mere tracing.[63] Even though the capability of tracing many cyber attacks, even distributed botnets, may at this point be within the technical capabilities of the most sophisticated cyber powers—including the United States—that alone is not enough to establish attribution. It is also necessary to know something about who launched a given cyber attack and why. This requires defining the applicable burden of proof. That is why Judge Advocate Charles Williamson of the U.S.A.F. has said, "Out of all the areas of international law that need to be changed to provide defenders protection against cyber attacks, this is the most important."[64] It is to this thorny issue of international cyber law that we turn next.

IV. THE FUNDAMENTAL ISSUE OF ATTRIBUTION AND THE CASE FOR THE OVERALL CONTROL STANDARD

Determining an appropriate standard for attribution is a critical element in building a functioning regime of international cyber law. This is, in large part, because concrete attribution is difficult to attain, even with many companies and governments working together to determine the true source of an attack. There are many elements to

addons.mozilla.org/en-us/firefox/addon/torbutton/developers (last visited June 11, 2011) (noting that onion routing is a way to use multiple networks to mask user identification).

[62] Interview with Jonathan Mayer, Ph.D. student, Stanford Computer Sci. Dep't, in Stanford, Cal. (Feb. 21, 2011).

[63] *See generally* CLARKE & KNAKE, *supra* note 40.

[64] Electronic interview with Charles Williamson, Deputy Staff Judge Advocate, U.S. Air Force (Apr. 22, 2010).

attribution ranging from the identification of the machines that launched the attack to the individual who pressed the button, to identification of the nation under whose jurisdiction the individual falls. And even when governments believe they have identified an attacker they may choose not to share this information with the public or courts. For instance, it was not widely known that the Chinese Politburo directed the cyber attacks on Google outside of U.S. defense circles until classified U.S. diplomatic cables were leaked to the press.[65] The National Academies of Science summarized the problem succinctly:

> It may be difficult even to know when a cyberattack has begun, who the attacker is, and what the purpose and effects of the cyberattack are/were. Indeed, it may be difficult to identify even the nature of the involved party (e.g., a government, a terrorist group, an individual), let alone the name of the country or the terrorist group or the individual. Knowing the nature of the party is an important element in determining the appropriate response. And, of course, knowing which country, terrorist group, or individual is in fact responsible is essential if any specific response involving attack is deemed appropriate.[66]

A critical part of this analysis lies in defining the degree of certainty needed about the identity of an attacker before a counterattack may be launched to neutralize it. The laws of war require that a State must identify itself when it attacks another State under *jus in bello*, though this convention is honored more in the breach than in compliance.[67]

When there is a question about State sponsorship of aggression

[65] Gjelten, *supra* note 17.

[66] COMM. ON OFFENSIVE INFO. WARFARE, NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 275 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2010) [hereinafter NATIONAL ACADEMIES].

[67] *See* Hague Convention No. III Relative to the Opening of Hostilities art. I, Oct. 18, 1907, 36 Stat. 2259, 2271 T.S. 598 (entered into force Jan. 26 1910) [hereinafter Hague Convention]. Consider the following example:

> During conflict between the United States and Zendia, a U.S. cyberattack is launched on a computer controlling a Zendian air defense network. A normally reliable human informant passes on a message to the United States, but the message is unfortunately incomplete, and the only information passed along is the computer's electronic identifier, such as an IP address or a MAC (Media Access Control) address; its physical location is unknown. The open question is whether this computer is a valid military target for a U.S. cyberattack. NATIONAL ACADEMIES, *supra* note 69, at 253.

opening the door to countermeasures, Article VIII of the International Law Commission's Draft Articles on the Responsibility of States for International Wrongful Acts comes into play. Article VIII implicates State control when State actors or official organs are "acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."[68] An exact definition of "control," however, has been left up to the courts to interpret, which has resulted in two primary competing standards for State responsibility being developed under Article VIII: the effective and overall control standards. As was stated above, the effective control standard, originating in the ICJ *Nicaragua* case, recognizes a country's control over paramilitaries or other non-State actors only if the actors in question act in "complete dependence" on the State.[69] In contrast, the overall control doctrine, from the International Criminal Tribunal for the Former Yugoslavia (ICTY) *Tadic* case, holds that where a State has a role in organizing, coordinating, and providing support for a group, the group's acts are attributable to the State.[70] In so finding, the majority interpreted the decision of the ICJ in *Nicaragua* as requiring the government of a State to exercise "effective" control over the operations of a military force in order for the acts of that force to be imputed to the State.

One of the most recent cases in which the ICJ reviewed the competing standards of State responsibility was the Application of the Genocide Convention ("Bosnian Genocide Case").[71] There, the Court adopted the effective control rather than the overall control standard in deciding that Bosnia lacked the specific intent to commit genocide. In essence, the Court required "smoking-gun" evidence or its equivalent.[72] The standard laid down by the Court was beyond any doubt, not beyond a reasonable doubt.[73] The ICJ reasoned that this high-level of certainty is commiserate with the seriousness of the allegation.[74] Such a high burden of proof would be difficult to satisfy in the kinetic attacks

[68] Int'l Law Comm'n, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, Vol. II, Part 2, art. 8, U.N. Doc. A/56/10, chp.IV.E.1 (Nov. 2001).

[69] Nicaragua, *supra* note 14.

[70] *See* Tadic, *supra* note 15; *see generally* Shackelford, *supra* note 53.

[71] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Mont.), 2007 I.C.J. 91, ¶ 391 (Feb. 26) [hereinafter Bosnian Genocide].

[72] David Luban, *Timid Justice: The ICJ Should Have Been Harder on Serbia*, SLATE (Feb. 28, 2007, 4:56 PM), http://www.slate.com/id/2160835/index.html.

[73] Bosnian Genocide, *supra* note 74, ¶ 422.

[74] *See* Scott Shackelford, *Holding States Accountable for the Ultimate Human Rights Absue: A Review of the International Court of Justice's Bosnian Genocide Case*, 14 HUM. RTS. BR. 21, 24 (2007).

at issue in this case. Proving the intent behind State-sponsored cyber attackers would be harder still. The distinction between the reasonable doubt and beyond any doubt standards was significant enough to potentially have been dispositive of the Bosnian Genocide Case's outcome. Future cases will also likely turn on this distinction, necessitating an in depth analysis of the benefits and drawbacks of each standard for State responsibility as applied to State sponsors of cyber attacks.

A. *The Drawbacks of the Effective Control Standard*

As a result of the divergence in international law on the issue of State responsibility, the two competing standards emerging for cyber attacks have thus far only been applied by the courts in other contexts. For non-State actors, the ICJ held in *Nicaragua* that effective control was the appropriate standard to apply, at least in the paramilitary context of that case.[75] If this decision were extended to cyber militias, it would mean that State sponsors of cyber attacks would only be held accountable if their effective control could be proven beyond any doubt—such as potentially the Estonian Cyber Defence League discussed in part D of this section. Given what has been demonstrated about the technical challenges of proving the identity of cyber attackers, however, such a standard could give a free pass to State sponsorship of cyber attacks. In a sophisticated global cyber attack, missing or corrupted data commands may be sufficient to disprove State control and defeat accountability. Without either new techniques such as the probabilistic tracing project mentioned in section III, or unsophisticated attackers, effective control may well make State responsibility for cyber attacks virtually a non-starter.

There are also other important drawbacks to adopting the ICJ's *Nicaragua* formulation with regards to proving State responsibility for cyber attacks, among them the fact that the Court divided the use of force into "most grave" and "less grave" categories.[76] This distinction has split commentators. Some see this view as formalistic and restrictive, thus encouraging aggression of a low-key kind.[77] According to Gray, others see a low threshold of armed attack mixed with collective

[75] Nicaragua, *supra* note 14, at 392; *see* Giuliana Capaldo, *Providing a Right of Self-Defense Against Large Scale Attacks by Irregular Forces: The Israeli-Hezbollah Conflict*, 48 HARV. INT'L. L. J. ONLINE 101, 105 (2007).

[76] *Id.* ¶ 101.

[77] CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 141 (2000).

self-defense as a recipe for the internationalization of civil conflicts.[78] As applied to cyber attacks, this doctrine would arguably give a pass to low-level cyber attacks, potentially up to and including the cyber attacks on Estonia, a pass at least as applied to the Law of Armed Conflict. In turn, this could encourage further attacks by cyber criminals and other non-State actors. Instead, while the laws of cyberwarfare remain malleable, a flexible approach like the overall control standard should be adopted—though this carries certain drawbacks, which we discuss below.

B. *Evaluating the Overall Control Standard*

The ICJ has consistently used the more restrictive effective control standard in its jurisprudence, most recently in *Bosnian Genocide*, but other tribunals, including the ICTY, have not applied the standard as uniformly. Judge Antonio Cassese, the first President of the Hague Tribunal, attacked the *Bosnian Genocide* judgment as demanding an "unrealistically high standard of proof."[79] Likewise, this burden is nearly impossible to satisfy in cyberspace without major improvements in the tracing of cyber attacks. As a result, if international law is to have sufficient applicability to the cyber realm, it is essential that a flexible approach such as the overall control standard be adopted as part of a future international regime for cybersecurity. Negotiations have begun between representatives of the United States and Russia over the framework of such a treaty, though the two sides are far apart, which is to be expected given the significant national security implications of the subject matter.[80] If these talks do bear fruit, their scope should be expanded to include the formulation of a standard for State responsibility for cyber attacks.

C. *The 'Government Awareness' Approach*

There is also precedent within the ICJ context itself to support a third more flexible standard of State responsibility. Specifically, the ICJ

[78] *See* Kenneth Watkin, *Controlling the Use of Force: A Role for Human Rights Norms in Contemporary Armed Conflict*, 98 AM. J. INT'L L. 1, 5 (2004).

[79] Caroline Tosh, *Genocide Acquittal Provokes Legal Debate*, INST. FOR WAR & PEACE REPORTING (Mar. 2, 2007), http://iwpr.net/?p=tri&s=f&o=333772&apc_state=henh.

[80] John Markoff & Andrew E. Kramer, *In Shift, U.S. Talks to Russia on Internet Security*, N.Y. TIMES, Dec. 12, 2009, http://www.nytimes.com/2009/12/13/science/13cyber.html?_r=1&partner=rss&emc=rss; *see also* Hughes, *supra* note 57; *see also* Ella Karapetyan, *Security Conference Convenes in Munich*, BALTIC TIMES (Feb. 9, 2011), http://www.baltictimes.com/news/articles/27935.

held in the *Iran Hostages* case that the actions of a State's citizens could be attributed to the government if the citizens "acted on behalf on [sic] the State, having been charged by some competent organ of the Iranian State to carry out a specific operation."[81] There, while the Court did not find sufficient evidence to attribute the actions of the citizens to the government, the Court did find that the Iranian government was nonetheless responsible because it was aware of its obligations under the 1961 Vienna Convention on Diplomatic Relations and the 1963 Convention on Consular Relations to protect the U.S. embassy and its staff, and failed to comply with its obligations.[82]

The Court's reasoning in *Iran Hostages* could be extended to cyber operations in two ways. First, State governments could be vicariously liable for resulting damage from cyber attacks if the citizens of the State acted on behalf of a competent government organ. Second, if there is insufficient evidence to find attribution outright, as there was in *Iran Hostages*, then a governmental awareness standard could apply. If the government were aware of its obligations under international law to prevent its citizens and information infrastructure from launching cyber attacks and failed to comply with these responsibilities, that State could then be held in breach of international law, raising important issues regarding neutral States discussed below in section V.[83] That State could then be held in breach of international law. However, given the fact that many nations around the world would be in breach of this approach without major improvements in their own cybersecurity, including the United States, there may be a strong preference in the international community for the overall control standard. This preference might be reinforced by the need to clarify the applicable international law for the government awareness standard to adequately func-

[81] United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), 1980 I.C.J. 3, ¶ 58 (May 24).

[82] Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. INT'L L. & POL. 57, 98 (2001).

[83] The *Corfu Channel* case should also be considered in this context. In that case, Albania mined the Corfu Strait, and the British Royal Navy sued for damages and loss of life that it sustained as a result of ships colliding with the mines. There, the ICJ stated: "... it cannot be concluded from the mere fact of the control exercised by a State over its territory and waters that that State necessarily knew, or ought to have known, of any unlawful act perpetrated therein." The Corfu Channel Case (United Kingdom-Albania), 1949 I.C.J. 4, 18 (Apr. 9). Yet, even in *Corfu Channel* the Court noted that the standard of State responsibility should be somewhat flexible when it stated, "... the other State, the victim of a breach of international law, is often unable to furnish direct proof of facts giving rise to responsibility. Such a State should be allowed a more liberal recourse to inferences of fact and circumstantial evidence." *Id.*

tion, which is no small feat. But either the overall control or the government awareness standard has the benefit of moving beyond the rigid effective control framework and holding State sponsors of cyber attacks accountable when significant evidence exists of their involvement or acquiescence.

Yet there are other difficulties posed by adopting a standard of State responsibility with a lower burden of proof than effective control that need to be addressed. Principal among these is the danger of prosecuting accused State sponsors of attacks that are innocent. Politically, this worry may cause some countries to push for the higher burden of proof enshrined in the effective control standard so as not to be wrongly accused of sponsorship. Such critiques may in part be addressed by a clarification that a requirement of "beyond a reasonable doubt" under the overall controls standard is still a very high burden of proof (BOP) that the prosecuting entity must meet, making frivolous or unwarranted cases unlikely.[84] What is more, there is the possibility that some States would in fact prefer a lower burden of proof, at least when they are attacked, so as to justify retaliatory cyber attacks in response.

D. *Supplementing State Responsibility with the 'Sliding Scale' Approach*

The worry of unwarranted lawsuits may also be tempered by supplementing either the *Tadic* or *Iran Hostages* standards with the sliding scale approach introduced by Judge Higgins of the ICJ in 2003. This approach simply requires that "the graver the charge the more confidence there must be in the evidence relied on."[85] In the context of cyber attacks, this would mean that the graver the cyber attack, the more evidence would be required before a State could be held accountable. One potential problem with this approach is that some States could have a perverse incentive to sponsor more devastating attacks so as to raise the necessary burden of proof and potentially defeat accountability. This would also have the effect of ratcheting up the burden of proof requirement to something approaching the effective control standard. Many of the cyber powers may well be supportive of such an approach, since it would give them the benefit of making use of the status quo strategic ambiguities endemic in cyberspace to launch an

[84] Stephen Erikkson, *Humiliating and Degrading Treatment Under International Humanitarian Law: Criminal Accountability, State Responsibility, and Cultural Considerations*, 55 AIR FORCE L. REV 269, 294 (2004).

[85] *See* Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶ 33 (Nov. 6) (separate opinion of Judge Higgins).

array of attacks without worrying about attribution. But how would these standards of proof play out in practice?

E. *Analyzing Recent Cyber Attacks Under the Competing State Responsibility Standards*

A string of recent cyber attacks offer the opportunity to analyze the utility of the various approaches to State responsibility mentioned above. "Stuxnet" and "Night Dragon" represent two illustrative examples.

The factual background of Stuxnet has already been reviewed, but for attribution purposes, prior to the leak, why was Israel commonly thought to have been behind the attacks? First, there were technical reasons. For example, one of the path names used in Stuxnet included a sub-folder with a modified Hebrew name.[86] Second, there was a motive analysis conducted—who with the necessary technical prowess stood to gain from a multi-year delay in Iran's nuclear program? The technical evidence was highly circumstantial and could easily have been faked. But would this quite limited technical evidence combined with a motive suffice for a burden of proof analysis? Certainly this evidence would not fulfill the requirements under the effective control standard, and perhaps not for the overall control standard either. This highlights the difficulty in applying the State responsibility doctrine, be it flexible or not, to cyber attacks.

"Night Dragon" refers to a series of cyber attacks launched by servers located within China and using hosted services from the United States to wage attacks against multinational oil and gas firms in the United States, Kazakhstan, Taiwan, and Greece using compromised servers in the Netherlands.[87] The sheer number of States involved in this attack is far from atypical, again highlighting the difficulties involved with defining State responsibility for these types of attacks. What was the technical evidence in this case signifying that China was indeed behind the attacks? The cybersecurity firm McAfee found the following: the attackers used Beijing-based IP addresses from 9:00 a.m. to 5:00 p.m. Beijing-time meaning that they may have been "company men"; the password used to unlock the operation was "zw.china"; and many of the tools necessary to undertake the attacks may be found in postings from

[86] *See* Mary Landesman, ***Debunking the Bunk of Stuxnet***, ABOUT.COM (Oct. 2, 2010), http://antivirus.about.com/b/2010/10/02/debunking-the-bunk-of-stuxnet.htm.

[87] *See* MCAFEE, GLOBAL ENERGY CYBERATTACKS: "NIGHT DRAGON" 4 (2011), *available at* http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf.

a Chinese-language chat room.[88] To its credit, McAfee states that it has "no direct evidence" of attribution in this case. But does this increased array of technical details, as well as the motive of Chinese resource-exploitation firms obviously benefiting from underbidding Western competitors, satisfy one of the standards of State responsibility? The effective control standard would once again likely be a bridge too far. The overall control standard may be applicable if it could be proven that the Chinese government organized or coordinated the group's acts. The government awareness approach would require a clarification of the applicable international law. Interestingly in this case, McAfee identified an individual who runs a company in Heze City, Shandong Province in China who appears to be responsible for at least some of these intrusions. The need to rely on the Chinese authorities to investigate the matter, to say nothing of extraditing and determining an appropriate forum to try the accused, highlights the extreme difficulties with holding cyber attackers accountable.

Given the circumstantial evidence that is often all investigators have to go on in investigating cyber attacks, the natural question is: what would hard evidence look like? According to Mayer, hard evidence requires direct examination of the system in question by well-trained forensic specialists.[89] Such luxuries are rare—and if the only way to obtain the system is through a kinetic attack, then the cure could be worse than the disease. As technology improves it may be possible to attain a higher degree of confidence in technical evidence of attribution. Until then, however, analysis of motives and intent to attain some probability of accurate attribution is often the only way to assess and respond to cyber attacks at present.

F. *State Responsibility Summary*

In summary, it is easy for governments to hide their information warfare operations under the effective control standard. It should thus be sufficient as matter of international law to prove overall control by a government in a cyber attack, rather than complete control. For example, if the overall control standard were used instead of effective control, if it were possible to prove Russian or Chinese incitement behind the cyber attacks on Estonia, Georgia, or the United States, this

[88] *Id.* at 18; Mayer, *supra* note 62.

[89] Mayer, *supra* note 62.

would be sufficient to satisfy State responsibility.[90] A comprehensive future legal regime could grant Estonia, and other victim nations, adequate reparations for such attacks. But if effective control becomes the dominant paradigm for determining State responsibility for cyber attacks, even a victim State of a worst-case scenario cyber attack may not receive justice. Alternatively, the ICJ precedent of *Iran Hostages* could be used as another vehicle to hold accountable State sponsors of cyber attacks. But, given the propensity of cyber attacks to cross neutral networks besides those of the belligerent States, it is critical when discussing the *jus ad belllum* issue of State responsibility to also give due attention to applying the Law of Armed Conflict in cyberspace including the *jus in bello* problems of neutrality and distinction in international law.

V. Applying the Law of Armed Conflict to Cyberspace

A great debate is currently raging in academic and policy circles about the applicability of international law generally, and the Law of Armed Conflict (LOAC) in particular, to cyberspace. The field may be broken down into four camps. In the first, some assert there is no difficulty at all in applying laws—which were developed for other purposes—to the new frontier of cyberspace. We will call this group the "extenders," since they prefer the extension of existing legal regimes into cyberspace. Elements within the U.S. Department of Defense have come out in favor of this approach.[91] Adherents to a second camp—who can be called the "treaty makers"—maintain that cyberspace is a unique environment necessitating an entirely novel regulatory structure. One proponent of this approach is Rex Hughes of Chatham House, who believes that a comprehensive treaty for cyberspace regulation is essential for moving towards cyber peace.[92] Despite the support for this approach, both the details for how such a treaty would function and whether there is sufficient political will to make it a reality remain uncertain.

[90] It is also helpful to analyze U.S. case law in this regard, particularly the string of cases interpreting the applicability of the Alien Tort Claims Act to accomplice liability. *See, e.g.*, Cabello v. Fernández-Larios, 402 F.3d 1148, 1157 (9th Cir. 2005) (noting that "that plaintiffs were required to show that guardsmen were under the effective control of defendant officials"). However, because of the differences in the actors and applicable law, such comparisons only have limited utility in discussing State-sponsored cyber attacks.

[91] *See, e.g.*, Office of Gen. Counsel, Dep't of Def., An Assessment of International Legal Issues in Information Operations (2d ed. 1999) [hereinafter "DOD Assessment"].

[92] Hughes, *supra* note 57, at 541.

A third camp holds little hope for the usefulness of international law in bringing about cyber peace. For example, Rein Lang, Estonia's Justice Minister, has complained that "international law is of little help" in dealing with cyber attacks.[93] Stewart Baker, former Assistant Secretary for Policy at the U.S. Department of Homeland Security, and Lewis of CSIS, have echoed this sentiment.[94] We call this group the "critics." A fourth group includes commentators like Richard Clarke who hold out hope for the ability of international law to promote some degree of cyber peace, but believe this peace should be based on State responsibility:

> There ought to be a well-articulated national obligation to police any activities coming out of your country. . . . So if you find yourself suddenly under attack from a server in Uganda then you can—in real time, in an hour so, and not a day later or a week later—tell Uganda exactly what's going on . . . and then they have the ability to immediately step up and do something about it.[95]

This fourth group puts the burden of international cyber law on individual States but, given their vastly different cybersecurity capacities, harmonization of such a system would be difficult.

Despite the fragmentation of this debate, there is widespread agreement that greater clarity is needed in the international legal framework to dealing with cyber attacks, particularly with regards to State-sponsored attacks.[96] For example, according to Daniel Ryan of

[93] *Id.*

[94] *See* Interview with Stewart Baker, Former Assistant Sec'y for Policy, Dep't of Homeland Sec., in Wash., D.C. (Jan. 4, 2011); Interview with James Lewis, Dir. and Senior Fellow, Tech. and Pub. Policy Program, Ctr. for Strategic and Int'l Studies, in Wash., D.C. (Jan. 5, 2011).

[95] Interview with Richard Clarke, Founder, Good Harbor Consulting in Alexandria, VA (Jan. 4, 2011).

[96] *See e.g.*, Susan W. Brenner, *Toward a Criminal Law of Cyberspace: Distributed Security*, 10 B.U. J. SCI. & TECH. L. 1, 76 (2004) (noting that the traditional model of law enforcement, with its reactive approach and hierarchical, military-style organization, cannot deal effectively with cybercrime); *see generally* Daniel M. Creekman, *A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China*, 17 AM. U. INT'L L. REV. 641 (2002) (covering the various ways in which the U.S. may respond to cyber terrorism emanating from China); Joginder S. Dhillon & Robert I. Smith, *Defensive Information Operations and Domestic Law: Limitations on Government Investigative Techniques*, 50 A.F. L. REV. 135 (2001) (discussing procedures in law enforcement of domestic information); Reuven Young, *Defining Terrorism: The Evolution of Terrorism as a Legal Concept in International Law and Its Influence on*

National Defense University, "[w]e don't know when or if a cyberattack rises to the level of an 'armed attack.'"[97] Defining that boundary is critical since it defines when the LOAC is activated. The lack of agreement in this area engenders confusion. "If nations don't know what the rules are, all sorts of accidental problems might arise," Harvard law professor Jack Goldsmith states. "One nation might do something that another nation takes to be an act of war, even when the first nation did not intend it to be an act of war."[98] Assuming that the LOAC may in fact be applied to cyberspace, the obvious question is how? This is particularly relevant with regard to *jus ad bellum,* since most cyber attacks will not breach the armed attack threshold, as discussed below.

Jus ad bellum has its roots in just war theory dating back to Cicero, coming back into fashion in the Middle Ages beginning with the writings of Augustine of Hippo and Thomas Aquinas. The central notion behind the doctrine is that conflict can and ought to meet certain philosophical, religious, and/or political criteria. Today, *jus ad bellum* is governed by customary international law and the U.N. Charter, particularly Articles 2(4), 39, 42, and 51.[99] There is currently a great deal of confusion as to how these thresholds, enacted to deal with traditional armed attacks, should be applied in cyberspace. We briefly catalog the different approaches to defining this armed attack threshold below and discuss what the implications are in terms of attribution and cybersecurity.

The U.N. Charter generally divides conflict into three zones. The first zone is framed by the Article 2(4) threshold, which makes the threat or use of force illegal without a U.N. Security Council (UNSC) authorization. There are many examples of such threats that States have not treated as breaching Article 2(4), including troop movements, verbal threats, trade disputes, and economic sanctions. The second zone is defined by the Articles 39 and 42 threshold, at which point the UNSC may designate a breach to international peace and security. Examples of times in which the UNSC has used this authority include cases of ethnic cleansing, apartheid, or genocide. The final barrier is

Definitions in Domestic Legislation, 29 B.C. INT'L & COMP. L. REV. 23, 91, 100 (2006) (defining international terrorism by using cyber attacks as an example).

[97] Tom Gjelten, *Extending the Law of War to Cyberspace,* NAT'L PUB. RADIO (Sept. 22, 2010), http://www.npr.org/templates/story/story.php?storyid=130023318.

[98] *Id.*

[99] *Jus in bello* on the other hand is governed by the Hague Conferences of 1899 and 1907, as well as the Geneva Conventions. *See* Hague Convention, *supra* note 67.

Article 51, which allows for the individual or collective use of self-defense in response to an armed attack. An armed attack is more serious than a mere use of force, constituting an invasion by military forces like the 9/11 attacks.[100] An important question arises as to when the preemptive use of force may be used to counter an imminent armed attack. This issue is discussed below, but an important part of this consideration is determining when an armed attack has occurred. When can a cyber attack, for example, be the same as an invasion by military forces activating the laws of war?

FIGURE 1.1:
ZONES OF CONFLICT UNDER THE U.N. CHARTER

	Art. 2(4) Threshold	**Art. 39/42 Threshold**	**Art. 51 Threshold**
Definition	Threats or uses of force not deemed as breaches of international peace and security by the UNSC	Threats or uses of force that the UNSC has deemed to breach international peace and security	Self defense in response to armed attacks
Examples	Verbal threats, trade disputes, economic sanctions	Genocide, apartheid, ethnic cleansing	One country invading another

International law permits self-defense only in the case of an attack so egregious that the victim would be justified in responding in kind.[101] This definition rules out preemptive or aggressive self-defense in most instances. The question then is whether and to what extent cyber attacks constitute an armed attack activating the Article 51 right of self-defense.[102]

There are three basic tests to determine whether a cyber attack may be considered an armed attack. The first is the "equivalent effects

[100] Thomas Wingfield, Professor of Int'l Law, George C. Marshall Eur, Ctr. for Sec. Studies, Presentation at the CCDCOE NATO Conference on Cyber Conflict, in Tallinn, Estonia (June 16, 2009).

[101] *Compare* U.N. Charter, art. 2, para. 4 (general prohibition on use of force), *with id.* art. 51 (inherent right of self defense).

[102] In 1974, the General Assembly defined the term aggression as "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any manner inconsistent with the Charter of the United Nations." G.A. Res. 3314, art. 1, U.N. GAOR, 29th Sess., Supp. No. 31, U.N. Doc. A/9631 (Dec. 14, 1974).

test," which requires that for a cyber attack to be considered an armed attack it must result in the same consequences as would a kinetic attack and physical invasion by traditional military forces. This approach has been supported by the U.S. Department of Defense General Counsel's office in the past.[103] The second test is Picket's, which is based on the scope, intensity, and duration of the cyber attack. This test questions whether the harm is of such breath and depth that it should be treated as an armed attack under international humanitarian law (IHL). The third and final test is the Schmitt analysis. The Schmitt analysis analyzes a number of factors on a case-by-case basis to determine whether or not an attack constitutes a use of force that moves beyond the Article 2(4) threshold. These factors, detailed below, include but are not limited to severity, immediacy, and directness.

FIGURE 1.2:
REPRESENTATIVE FACTORS FOR SCHMITT ARMED ATTACK ANALYSIS[104]

- Severity—how many people were killed, and how much damage was sustained?
- Immediacy—how fast and unexpected was the military action?
- Directness—is there a clear cause and effect relationship?
- Invasiveness—are there militaries crossing borders, causing substantial effects?
- Measurability—how accurately do we know the effects?
- Presumptive legitimacy—is this an action that presumably takes a country to accomplish, indicating a high level of coordination?
- Responsibility—which nation's military forces were responsible?

On one end of the spectrum, Schmitt argues that a cyber attack on an air traffic control system causing airplane crashes and numerous casualties would be considered a use of force, whereas an attack on a

[103] DOD ASSESSMENT, *supra* note 91, at 18–19.

[104] *See* James B. Michael, et al., Presentation at the 27th Annual IEEE Int'l Computer Software and Applications Conference, Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System (Nov. 5, 2003).

university computer system designed to delay a government research program would not.[105] But Schmitt's analysis, though quite helpful academically, is not easily applicable in an operational setting. In an environment where seconds count, neither soldiers nor politicians may have the time to undertake such detailed analyses.

All of the above approaches to analyzing armed attacks have the drawback of being cumbersome to a greater or lesser degree. Waiting to see the result of an attack may be the only certain way of determining intent, for example, but it has the rather significant drawback of potentially allowing a great deal of damage. Above the armed attack threshold, the LOAC may indeed be applicable. Below it, an array of international legal provisions may be employed, among them Mutual Legal Assistance Treaties, extradition treaties, the Cybercrime Convention, the Vienna Convention on Diplomatic Immunity, status of forces agreements, and perhaps even the U.N. Convention on the Law of the Sea (dealing in part with submarine cables).[106] Indeed, scholars have sought to establish a definitive cyber framework by positing analogies to other relevant comparative law regimes—the Law of the Sea, Air Traffic Control, the Law of Outer Space, and the Antarctic Treaty System—which presently govern other parts of the global commons.[107] Regimes addressing outer space may provide the best analogies as cyberspace, distinctively, is not topographically defined in space.[108] The nature of cyberspace makes comprehensive tracking difficult since although the physical components of Internet—that is, its host servers—are routed in particular jurisdictions, controlling the packets of information that comprise cyberspace is beyond the purview of the average Internet user. Similarly, spacecraft and satellites may be owned by a certain sovereign State or company, but while in orbit pass above many different jurisdictions.[109]

During his confirmation hearing, U.S. Senators sent General Keith B. Alexander, now head of U.S. Cyber Command (CYBERCOM), a list of questions: Would he develop 'significant' offensive cyber-weapons? Might these encourage others to follow suit? How sure would he need to be about the identity of an attacker to 'fire back'? Answers to these

[105] NATIONAL ACADEMIES, *supra* note 66, at 254.

[106] *See* Shackelford, *supra* note 53 (using analogies to explore the array of international law that may be applicable to cyber attacks).

[107] *Id.*

[108] Julie J.C.H. Ryan, et al., *Cybersecurity Regulation: Using Analogies to Develop Frameworks for Regulation,* in INTERNATIONAL CYBERSECURITY LEGAL & POLICY PROCEEDINGS 76, 85 (2010).

[109] *Id.* at 89.

inquiries were restricted to a classified supplement. In public, General Alexander said that the president would be the judge of what constituted cyberwar.[110] The political threshold for a serious cyber attack (as opposed to espionage) by a nation-state is very high, likely as high as the threshold for conventional military action. At a minimum, this suggests that a serious cyber attack is a precursor, a warning which may signify that a more serious conflict is about to begin.[111]

The open question is what happens when a high standard for State responsibility, such as the effective control standard, is married to the substantial effects doctrine for armed attacks. This, in essence, would allow the cyber powers to benefit from the high burden of proof such standards establish and not risk being held accountable for any sponsored attacks. A high armed attack threshold would mean that attacks up to and likely including Stuxnet would not activate the LOAC, meaning that cyber espionage could continue unabated. Such a system will continue to enforce the status quo strategic ambiguity. If little progress can therefore be expected under *jus ad bellum*, what of the related problem of defining the rights and responsibilities of neutral nations under *jus in bello*?

A. *Neutrality, Distinction, and State Responsibility in Cyber Operations*

As has been shown in the case of State responsibility, international law has thus far been proven to be ill equipped to deal with the emergence of the new cyberwarfare being sponsored by an increasing number of cyber powers. State practice currently upholds the view that some level of cyber attack is lawful under international law, particularly in the case of cyber espionage.[112] The question is how far cyber attackers will be allowed to go—particularly with regards to neutral nations and civilian targets. O'Donnell and Kraska discuss these interrelated problems of defining neutrality and distinction succinctly when they state: "[H]ow attacks on computer network affects third countries or neutral forces beyond the scope of the conflict may well be dispositive in determining its use."[113]

This section focuses on defining the rights and responsibilities of neutral nations, which is an increasingly important task at a time when

[110] *Cyberwar*, *supra* note 1, at 25.

[111] LEWIS, *supra* note 10, at 7.

[112] Brian T. O'Donnell & James C. Kraska, *Humanitarian Law: Developing International Rules for the Digital Battlefield*, 8 J. CONFLICT & SECURITY L. 133, 140 (2003).

[113] *Id.* at 146.

cyber attacks are emanating from unsecured networks around the world. In particular, this section addresses the issue by illustrating the current legal framework including the *jus in bello* principles of distinction and neutrality. Using this framework of international law and protocol, we will then outline exactly how and why the principles of neutrality and distinction are so difficult to apply to cyberwarfare, and how clarifying State responsibility might help in this regard.

B. *Neutrality and Distinction in Cyberspace*

A cogent analysis of cyber conflict and its underpinnings in international cyber law starts with the *jus in bello* principles of military necessity, proportionality, unnecessary suffering, and perfidy—the so-called "Caroline criteria." Military necessity, for example, limits targets to "those that make a direct contribution to the enemy's war effort."[114] Proportionality requires weighing the amount of collateral damage against the military advantage of an attack.[115] Immediacy means that the threat of an attack must be imminent. Therefore, preemptive Israeli airstrikes on the Osirak Reactor in Iraq were largely held to be in line with international law,[116] whereas the Bush Administration's reliance on this doctrine before the invasion of Iraq was questionable to say the least.[117] But the two most important doctrines for the immediate purposes are neutrality and distinction. Each will be addressed below.

Distinction requires parties to an armed conflict to distinguish between the civilian population and infrastructure and combatants.[118] Additional Protocol II to the Geneva Convention applies in non-internationalized internal armed conflicts and also incorporates the principle of distinction. It requires that "the civilian population and individual civilians shall enjoy general protection against the dangers arising from military operations,"[119] and also that "the civilian popula-

[114] NATIONAL ACADEMIES, *supra* note 66, at 246; *see also* T. D. Gill, *The Temporal Dimension of Self-Defence: Anticipation, Pre-emption, Prevention and Immediacy*, 11 J. CONFLICT SEC. L. 361, 361–62 (2006).

[115] *Id.* at 246.

[116] *See* Anthony D'Amato, *Israel's Air Strike Against the Osiraq Reactor: A Retrospective*, 10 TEMP. INT'L & COMP. L.J. 259, 264 (1996).

[117] *See* Ivo H. Daalder, *Policy Implications of the Bush Doctrine on Preemption*, COUNCIL ON FOREIGN RELATIONS (Nov. 16, 2001), http://www.cfr.org/international-law/policy-implications-bush-doctrine-preemption/p5251.

[118] Schapp, *supra* note 43, at 150.

[119] *Id.* (citing Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II),

tion . . . as well as individual civilians, shall not be the object of attack"[120] unless they take part in the hostilities.[121] That is to say, the mere "presence of civilians within or near a legitimate military target does not make an attack against that target unlawful."[122] In addition to these major tenets, the LOAC bars belligerents from rendering objects indispensable to the survival of the civilian population useless, including the destruction of foodstuffs, agricultural crops, livestock, drinking water installations and supplies, and irrigation works.[123] It also imposes on belligerents the duty to exercise care in conducting attacks in order to protect the natural environment as well as those installations with highly destructive potential including dams and nuclear power plants.[124] But the general premise that attacks be limited to military targets is not as easy as it may seem since:

> Military objectives . . . embrace more than troops, weapons systems, and military equipment. Rather, they include all objects which, by their nature, purpose, use, or location, effectively contribute to the military initiative being pursued and whose destruction would constitute a 'military advantage' to the force attacking the objective.[125]

In a major cyber conflict, this might or might not include elements of the civilian digital infrastructure, thereby necessitating an analysis of dual-use targets, as is discussed below.[126]

The principle of neutrality is an essential principle in maintaining international peace and security. Neutrality allows a State to remain neutral in a conflict and as such retain immunity from attack, so long as

art. 13(1), June 8, 1977, 1125 U.N.T.S. 609, [hereinafter Additional Protocol II]); Summary of the Co-Chairs. Informal High-Level Expert Meeting on Reaff. & Dev. Of Int'l Humanitarian Law (Jan. 27–29, 2003), http://ihl.ihlresearch.org/_data/n_0002/ resources/live/AlabamaSummary.pdf.

[120] Schapp, *supra* note 43, at 150 (citing Additional Protocol II, art. 13(2)).

[121] *Id.* (citing Additional Protocol II, art. 13(3)).

[122] O'Donnell & Kraska, *supra* note 112, at 155.

[123] Jeffrey T.G. Kelsey, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, 106 MICH. L. REV. 1427, 1436 (2008).

[124] *Id.* at 1437.

[125] James P. Terry, *The Lawfulness of Attacking Computer Networks in Armed Conflict and in Self-Defense in Periods Short of Armed Conflict: What Are the Targeting Constraints?*, 169 MIL. L. REV. 70, 84 (citing DEP'T OF NAVY, ANNOTATED SUPPLEMENT TO THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS, 8.1.1 (1997)).

[126] *See* discussion *infra* section V.B.

the neutral State does not assist either side or allow its territory to be used by a belligerent. In general, neutrality affords States the right to "maintain relations with all belligerents,"[127] and requires that a neutral State's territory be secure from assault or trespass.[128] Consequently, States that declare themselves neutral and behave accordingly are entitled to immunity, which includes a prohibition on belligerents moving troops, munitions, or other war supplies across neutral territory.[129] But if the neutral State fails to enforce its own neutrality by preventing violations of its territory by belligerents—such as allowing troops to pass through its territory—the other party may be justified in attacking those troops within the neutral State's territory.[130]

In a cyber context, the question is, how aggressive must neutral States be in securing their networks from cyber attackers? Ryan explains the problem:

> We have a notion enshrined in international law that says that you don't lose your neutrality if belligerents use your telephone lines or telegraph lines to communicate even if they are crossing your territory . . . The problem with cyberwar is that they are potentially not just transferring orders but also potentially weapons—cyber weapons.[131]

Other commentators have suggested that the only behavior that is required in order to remain neutral in a cyber conflict is that the neutral State not originate the attack, and that the State take some action to prevent the attack from transiting through its nodes and routers.[132] Placing this onus on States assumes relatively equal capacity while, as previously mentioned, States possess a wide range of cybersecurity capabilities. The cybersecurity capabilities of many nations are simply not on par with those of the cyber powers even as overall

[127] Schapp, *supra* note 43, at 152; *see also* Stephen W. Koms & Joshua E. Kastenberg, *Georgia's Cyber Left Hook*, PARAMETERES, Winter 2008/2009, at 60, 62.

[128] *Id.* at 153 (citing Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, art. 1, Oct. 18, 1907, 36 Stat, 2277, 1 Bevans 631 [hereinafter Hague Convention V] ("the territory of neutral Powers is inviolable.")).

[129] *Id.* (citing Hague Convention V, *supra* note 131, art. 2).

[130] U.S. DEP'T. OF ARMY, FIELD MANUAL 27-10, THE LAW ON LAND WARFARE ¶ 520 (July 18, 1956) (hereinafter FM 27-10).

[131] Julie J. C. H. Ryan & Daniel J. Ryan, Neutrality in the Context of Cyberwar, (Mar. 2011) (unpublished conference paper presented at the 6th International Conference on Information Warfare and Security) (on file with author).

[132] *See* Koms & Kastenberg, *supra* note 127, at 62.

spending on cybersecurity continues to increase rapidly.[133] The U.S. Department of Defense estimates that nearly 120 nations and many millions of individuals already hold the necessary hardware and software to launch cyber attacks.[134] There are now also more than 250 Cyber Emergency Response Teams currently operating worldwide. Unfortunately, cooperation between these teams remains limited.[135]

Consider, for example, some of the implications of the spread of broadband access. The U.N. is working to spread Internet technology to Africa and the Secretary General of the ITU has argued that governments must regard the Internet as "basic infrastructure" akin to roads. Similarly, former British Prime Minister Gordon Brown has argued that broadband access is the "electricity of the digital age."[136] But what are the consequences of having fast Internet connections in nations with weak governance? Some scenarios addressing this concern are included in this section.[137]

In addition to the laws of war, telecommunications law would be expected to frame the issue of cyber neutrality well, but that regime, beginning with the Hague Convention V, was created in 1907.[138] How could a framework of international law developed over a century ago have any bearing on the current debate over cyber neutrality? The Convention defined a narrow exception for neutrality law, positing that a "neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus, so long as the neutral state impartially permits the use of those structures by all belligerents."[139] Applying the spirit of this convention to the Internet age, this exception would provide unfettered discretion for neutral States to allow cyber attacks to pass across their Internet networks so long as it did so in an even-

[133] LEWIS, *supra* note 10, at 2; *see* Aaron Ricadela, *Symantec, McAfee, Checkpoint Await Spending Surge*, BLOOMBERG BUS. WK. (Jan. 18, 2010, 10:19 PM), http://www.businessweek.com/technology/content/jan2010/tc20100115_453540.htm.

[134] See Christopher C. Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 EUR. J. INT'L L. 825, 850 (2001) (arguing that assessing self-defense responses to cyber attacks and the role international institutions play to attain these objectives need clear rules).

[135] Hughes, *supra* note 57, at 534.

[136] Gordon Brown's Super-Fast Broadband for All Plan, BBC NEWS (Mar. 22, 2010), http://news.bbc.co.uk/2/hi/8579333.stm.

[137] *See infra* section V.

[138] *See* Joshua E. Kastenberg, *Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law*, 64 A.F. L. REV. 43 (2009).

[139] Hague Convention V, *supra* note 128, art. 1.

handed manner. So, on one hand, neutrality and distinction have been interpreted to include a right for a threatened State "to use force to neutralize a continuing threat located in the territory of a neutral state, but not acting on its behalf, when the neutral state is unable or unwilling to fulfill its responsibility to prevent the use of its territory as a base or sanctuary for attacks on another nation."[140] That is to say, even neutral States have an affirmative obligation to "refrain from harboring perpetrators of terrorist acts."[141] On the other hand, the Hague Convention V suggests a far more limited set of responsibilities for neutral States in a cyber conflict. These competing justifications necessitate clarification, as is attempted below.

Taken together, distinction and neutrality are important tenets of the LOAC and provide a framework from which to understand the context of the new cyberwarfare. But these principles have also been shown to be problematic. To understand why, consider the context of dual-use network infrastructure. When one belligerent State attacks another belligerent State's military network infrastructure, it can create ill effects on civilians who use that same military network infrastructure. This paradigm is not very common simply because civilians do not often utilize military networks. A far more common paradigm is applied when the network infrastructure itself has intermixed civilian and military components. An attack on this type of network infrastructure will have ill effects on civilians regardless of whether the belligerent intended these effects. This reflects a problem common to network infrastructure and dual-use targets, which comprise the majority of critical national infrastructure, especially in the United States. These targets are typically defined as those "used for both military and civilian purposes," such as power plants that provide electricity to both the civilian and military grids.[142] In the cyber context, dual-use targets include the computer networks of certain research facilities, air traffic control networks, as well as communications nodes and systems.[143]

The circumstances under which an attack on a dual use target is legal under the LOAC are nebulous, to say the least. The electrical grid is a common example. In this case, the goal of an attack would be to degrade an adversary's military capabilities, rather than terrorize a

[140] DOD ASSESSMENT, *supra* note 91, at 16.

[141] NATIONAL ACADEMIES, *supra* note 66, at 249.

[142] *See, e.g.*, Kenneth R. Rizer, Bombing Dual-Use Targets: Legal, Ethical, and Doctrinal Perspectives, AIR & SPACE POWER J. (May 1, 2001), http://www.airpower.maxwell.af.mil/airchronicles/cc/Rizer.html.

[143] Schapp, *supra* note 43, at 156.

civilian population. Despite this intention, such an attack may still run afoul of Protocol I's provisions if it is indiscriminate; it might not be limited to solely military objectives or the impact might be disproportionately felt by the civilian population. There is a divergence of opinion among commentators, particularly regarding proportionality—some maintain that only direct civilian casualties resulting from an attack should be considered, while others would include all indirect effects and collateral damage, which can be substantial even in targeted attacks like Stuxnet.[144]

Another example to consider is the potential of a cyber attack on air defense networks that results in the unintended consequence of crashing a commercial aircraft. This network is technically a dual use target as it was targeted for a military purpose, but had unintended civilian casualties. The open question is how this event can be properly incorporated into the distinction framework. Are the civilian casualties a direct or indirect effect? What interactive role would proportionality play? And should a coordinated cyber attack against another target, such as a power plant, be classified differently? A power plant could also be considered a dual use target and the consequences of an attack, regardless of the attackers' intentions, would cause significant hardship for the civilian population. Militaries around the world are increasingly interested in attacks on the Supervisory Control and Data Acquisition (SCADA) systems that control these smart systems, even as such targeting complicates the application of international humanitarian law, specifically Additional Protocol II.[145] Confusion only increases when civilian networks are used or commandeered by an aggressor to facilitate a cyber attack. Under these circumstances, the civilian network could become a valid and lawful target.[146] But, for how long? And for what purposes? These are questions that the current framework of international cyber law has yet to answer. Consequently, while attacking dual-use targets is often a strategic imperative in a military attack, be it kinetic or cyber, these are also the targets upon which civilians have the greatest reliance. Balancing the need for military victory with The Hague Conventions is a weighty task. Accounts differ as to whether such dual-use targets may be properly targeted, but suffice to say that it is an area where opinions differ, no less so than with regards to the issue of neutrality.

[144] MATTHEW C. WAXMAN, INTERNATIONAL LAW AND THE POLITICS OF AIR OPERATIONS 22 (2000).

[145] O'Donnell & Kraska, *supra* note 112, at 157.

[146] Terry, *supra* note 125, at 84–85.

Neutrality, like distinction, is also exceedingly difficult to classify within cyber context, for three primary reasons. First of all, there is considerable confusion about whether cyber attacks definitively cross into a neutral State's territory, either by land, sea, or air. There is no doubt that these cyber attacks cross nodes, but does this constitute a real incursion onto a neutral State's territory? Some commentators argue that cyber attacks are indeed violations of neutrality, noting that "[c]yber attacks routed through the networks of neutral States violate neutrality law, despite the lack of physical intrusion,"[147] and arguing that this is analogous to "moving a weapon across the territory of a neutral state."[148] These commentators point to the U.S. Air Force's broad definition of "weapons," which include all "devices designed to kill, injure, or disable people or to damage or destroy property," in justifying their position.[149] However, this argument may oversimplify the situation by ignoring the telecommunications exception, and treating all types of cyber attacks equally. As discussed in section III, that is not technically accurate.[150]

A second reason for the considerable confusion regarding the application of law of neutrality to cyber attacks is that it is exceedingly difficult to determine whether a cyber attack alone can draw a neutral State into a conflict. When a cyber attack is launched through the networks of a neutral State, the subsequent attack is broader and more effective. The cyber attacks on Georgia are a keen example of this, as is discussed below. A belligerent State that has been attacked may not be satisfied with a lack of action on the part of a neutral State to prevent such attacks from traveling through its nodes. This paradigm reflects an important inequity in the law of neutrality. Where a neutral State does not take action against the aggressive belligerent nation encroaching on its territory, the aggrieved belligerent State may take action against that neutral State. The law of neutrality gives that aggrieved belligerent nation the prerogative to attack regardless of whether the neutral State permitted the attack to occur or was simply unable to

[147] Kelsey, *supra* note 123, at 1443.

[148] *Id.* (citing Davis Brown, A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict, 47 Harv. Int'l L.J. 179, 184 (2006) (noting "In the information age, armed forces need not always deploy bombers and artillery to accomplish these objectives. In other words, the use of computer technology to wage war necessitates a reevaluation of the definition of the term 'weapon'")).

[149] DEPT. OF THE AIR FORCE, POLICY DIRECTIVE 51-4, COMPLIANCE WITH THE LAW OF ARMED CONFLICT para. 6.5 (1993); Kelsey, *supra* note 123, at 1443.

[150] *See supra* section III.

prevent the attack. The real problem lies in determining the precise intent of neutral States.

Third, and most importantly for cybersecurity purposes, is the issue of attribution. Short of compromising network access on a macro scale, it is exceedingly difficult for a neutral State to pinpoint the origins of or detect attacks by belligerent nations through its networks. Also consider that communications across the Internet are controlled by algorithms that relay the packets along different paths that are neither known nor controllable by network users.[151] Furthermore, some packets within an individual communication "may take different paths from other packets that are part of the same transmission, all transparent to and beyond the control of those engaged in the communication."[152] In this sense, neither the belligerent nation nor the neutral party have any idea what path a cyber attack will take, thereby reducing the relative culpability and increasing the deniability of a neutral State accused of having implicitly acquiesced to an attack transmitted across its networks. Defining the rights and responsibilities of neutral States is made even more difficult by the fact that presently "belligerents have many incentives to engage in cyber warfare across the Internet nodes of neutral states,"[153] including the lower costs associated with cyberwarfare as opposed to conventional kinetic warfare.[154]

C. *Solutions*

What can be done about these problems? Three options are commonly discussed. First, for the purpose of clarifying distinction, some have argued for the principle's expansion, allowing greater flexibility for States to launch and respond to cyber attacks that have a low potential for the loss of human life.[155] Unfortunately, this would do nothing to stem the overall flow of cyber attacks. In order to improve neutrality concerns, some have argued for a definition based on intent similar to that of State responsibility, which has the same benefits and drawbacks discussed earlier in this section.[156] A second and potentially

[151] Ryan & Ryan, *supra* note 131, at 3 (2011) (citing Jeff Tyson, How Internet Infrastructure Works, HOWSTUFFWORKS.COM (April 3, 2001), http://computer.howstuffworks.com/internet/basics/internet-infrastructure.htm).

[152] Ryan & Ryan, *supra* note 131, at 6.

[153] Kelsey, *supra* note 123, at 1445.

[154] *See* George K. Walker, *Information Warfare and Neutrality*, 33 VAND. J. TRANSNAT'L L. 1079, 1108 (2000).

[155] *See* Kelsey, *supra* note 123, at 1445.

[156] *Id.* at 1448.

more politically possible clarification lies in applying the telecommunications exception, which would alleviate many of the concerns that neutral states have about policing their networks. But having such a legal regime may encourage non-neutral powers to feign neutrality and still collaborate with belligerent powers. It could also provide incentives for a continuing race to the bottom, allowing States the benefits of launching cyber attacks while relieving them of the responsibility to police their networks and increasing network security. Third, there is also the potential for using the framework from U.N. Security Council Resolution (UNSCR) 1373, which requires States to reign in terrorist financing. UNSCR 1373, passed in the wake of the polarizing events of September 11, gave the U.N. Security Council both greater influence on the domestic law of individual States and the legislative influence that allowed it to deal with member States generally.[157] Such a radical departure from the original intent of UNSCR 1373 would likely require an additional Security Council Resolution, with little likelihood that such an approach would be supported by all of the permanent members at present. Consequently, it seems likely, at least for the present, that given their vested interests States will continue to make use of the status quo strategic ambiguity online, with some—like Estonia—raising cyber militias, and others—like weak governance States in Africa where widespread broadband is beginning to emerge—becoming havens for cyber criminals. Without a defined regime of State responsibility in place, such activities will likely proliferate. The following section explores the potential effects of these scenarios on the development of international cyber law.

D. *Checking Cyber Militias and the Growth of Cybercrime*

So-called 'hackivism,' breaking into computer networks for politically-motivated purposes, by non-State actors is an increasingly common feature of cyber attacks.[158] Israelis and Palestinians launched cyber attacks on one another after the second intifada in late September 2000.[159] Chinese and U.S. hackivists attacked one another's web presences after the 2001 incident between a U.S. reconnaissance aircraft

[157] Toby L. Friesen, *Resolving Tomorrow's Conflicts Today: How New Developments Within the U.N. Security Council Can Be Used to Combat Cyberwarfare*, 58 NAVAL L. REV. 89, 108 (2009).

[158] *See* NATIONAL ACADEMIES, *supra* note 66, at 278–79.

[159] Associated Press, Cyberwar Also Rages in Mideast, WIRED (Oct. 26, 2000), http://www.wired.com/politics/law/news/2000/10/39766.

and a Chinese jet fighter.[160] Russian hackivists were widely reported to have been responsible for the cyber attacks on Estonia in 2007 and Georgia in 2008.[161] The Estonian government is currently developing a State-sponsored cyber militia to defend its digital assets from future attacks.[162] This section briefly reviews several cyber operations associated with the various levels of State-sponsorship for cyber attacks discussed in section IV, with specific focus on the Estonian Cyber Militia and the use of emerging African networks for cybercrime.

Since being attacked in 2007, Estonia has been at the forefront of developing novel offensive and defensive solutions to standing cybersecurity problems. Among these is the Estonian "Cyber Defence League" (CDL), an organization "aimed at protecting Estonian cyberspace" and more broadly the national defense as part of the National Defence League.[163] Rain Ottis of the Cooperative Defence Centre of Excellence defines a cyber militia as "a group of volunteers who are willing and able to use cyber attacks in order to achieve a political goal."[164] Ottis notes that Estonia's proposed cyber militia consists of volunteers only insomuch as they act of their own free volition, without contractual obligations or payments from governments or otherwise.[165] Members of cyber militias may be personally acquainted, but are only loosely connected in the real world.[166] The objectives of the League are quite broad, and include: protecting Estonians' e-lifestyle, enhancing public-private cooperation in protecting critical national infrastructure, and sharing cybersecurity related knowledge.[167] In an emergency, the League would work with Estonia's Cyber Emergency Response Team to respond to attacks as provided for under the 2009 Emergency Preparedness Act. Any Estonian with an information security background may

[160] Michelle Delio, A Chinese Call to Hack U.S., WIRED (April 11, 2001), http://www.wired.com/news/politics/0,1283,42982,00.html.

[161] Joseph Menn, Expert: Cyber-Attacks on Georgia Websites Tied to Mob, Russian Government, L.A. TIMES BLOGS (Aug. 13, 2008, 6:39 PM), http://latimesblogs.latimes.com/technology/2008/08/experts-debate.html.

[162] Rain Ottis, Scientist at Coop. Cyber Def. Ctr. of Excellence, Proactive Defense Tactics Against On-Line Cyber Militia (July 1, 2010) (unpublished conference paper presented at the 9th Eur. Conference on Info. Warfare and Sec.) *available at* http://www.ccdcoe.org/articles/2010/Ottis_ProactiveDefense.pdf.

[163] FAQ, What is the Cyber Defence League?, (copy on file with authors).

[164] Ottis, *supra* note 162.

[165] *Id.* at 2.

[166] *Id.*

[167] *Id.*

apply to join.[168] Currently, the Estonian National Defence League writ large has 3,500 "young male" members from all over Estonia, but it is unknown how many of these are members of the cyber branch. There are even reports of Estonia considering a draft to further beef up the CDL.

How would the doctrines of State responsibility apply to the Estonian Cyber Defence League? Even the most stringent effective control standard would seem to be fulfilled given the extensive government direction of the proposed activities of the League. This makes it a relatively straightforward and fairly transparent case of State-sponsorship. Accountability, though, will remain a problem until mechanisms for reparations or sanctions are in place to deal with State sponsorship that falls below the level of an armed attack. However, what of cyber criminals, especially those making use of expanding networks in nations with weak governance?

Africa has recently seen an explosion in the growth of information technology. Between 2000 and 2009 the number of Internet users grew by 1,809.8%.[169] Broadband access in Africa was hugely expanded by the decision of France's Telecom-Orange to install a submarine fiber optic cable capable of providing Internet access to over 20 countries in West Africa.[170] Yet this increased bandwidth and broadband speed is directly proportional to spikes in cybercrimes.[171] As broadband technology proliferates due to falling costs and faster speeds, it will likely continue to spur a surge in cybercrime.[172] The divide between the number of new broadband users and the number of educated broadband users will increase serious risks of cybercrime as users not cognizant of security protection will be increasingly vulnerable to attacks.[173]

The spread of broadband access to developing countries in Africa

[168] See Defence League (Kaitseliit), KAITSELIIT.EE, http://www.kaitseliit.ee/index.php?op=body&cat_id=288 (last visited Feb. 28, 2011).

[169] DR. MARTHIE GROBLER & JOEY JANSEN VAN VUUREN, BROADBRAND BROADENS SCOPE FOR CYBER CRIME IN AFRICA (2010), *available at* http://researchspace.csir.co.za/dspace/bitstream/10204/4338/1/Groblerl_2010.pdf (citing 2009 Internet Usage Statistics for Africa (Africa Internet Usage and Population Stats), INTERNETWORLDSTATS.COM, http://www.internetworldstats.com/stats1.htm (last visited 1 Apr. 2010)).

[170] 2009 Internet Usage Statistics for Africa (Africa Internet Usage and Population Stats), INTERNETWORLDSTATS.COM, http://www.internetworldstats.com/stats1.htm (last visited Apr. 1, 2010)).

[171] K. Doyle, *Could South Africa Lead Cyber Crime Rankings?*, ITWEB, http://www.itweb.co/za/index.php?option=com_content&view=article&id=27948:could-sa-lead-cyber-crime-rankings (last visited Nov. 17, 2009).

[172] Grobler, *supra* note169, at 5.

[173] *Id. See also* Gary Boas, *Fiber Optics off the Coast of Africa*, PHOTONICS SPECTRA, Apr. 6, 2010, *available at* http://www.photonics.com/Article.aspx?AID=42577.

has increased the ease with which hackers can launch cyber attacks. Each day approximately 6,500 new spam-related websites are discovered, along with fifteen new bogus antivirus vendor websites, more than double the 2008 rate.[174] A 2006 cybercrime survey found that Nigeria was the African country most rife with cybercrime, and in that year Africa already ranked as the continent with the third most cybercrime activity.[175] African countries themselves are also frequent victims, with at least 27 documented cases of syndicates stealing millions from various governmental departments across Africa.[176] Newly connected computers in Africa are continuously being compromised and used to launch attacks on other computer systems.

Although some initiatives have been launched to deal with this explosion in cybercrime, they have so far not abated the rapid increase in criminal use of new African broadband networks. Slow download rates increase the time it takes to patch at-risk or already compromised systems. For example, McAfee's daily virus definition patches can require more than 100MB—with a 56Kb dialup link that could take a full day to download. While higher transfer speeds create a catch-22 situation, faster processing means that there is a greater volume of data that is easier to steal—in other words "the faster the link, the higher the amount of threats that might come."[177] A lack of IT education, absence of African-language capabilities online, an often antiquated African criminal law system, and a lack of coordination and harmonization further contribute to the African cybercrime epidemic. Efforts by the African Information Security Association and the ITU's High Level Expert Group to develop strategies and guidance to countries dealing with cybercrime are helpful, but so far have done little to stem the tide. Only Tunisia, Egypt, and Kenya maintain Cyber Security Incident Response Teams. The natural question is to ask what utility state responsibility has under such difficult conditions?

Few States are currently on par with Estonia when it comes to cybersecurity. African nations experiencing an unprecedented explosion of broadband access cannot be singled out for ineffectively dealing with the explosion in cybercrime occurring within their borders. As worldwide broadband access continues to expand, some of the cyber criminals using these new networks are likely to be State-sponsored. Already, there have been reports of Russian cyber criminals targeting

[174] Grobler, *supra* note 169, at 3.

[175] *Id.* at 2.

[176] *Id.*

[177] *Id.*

South African government websites.[178] The rights and responsibilities of African States and other developing nations to secure their networks and enhance cybersecurity have so far proven to be elusive given their widely varying technical capabilities. Thus, even if State responsibility could be defined precisely in order to deal with these situations, it could have little practical effect in creating incentives for a race to the top by itself. Instead, State responsibility must be supplemented with deep multilateral collaboration that ideally includes the cyber powers and NATO working together to assist beleaguered nations as they attempt to enhance cybersecurity. As the next subsection demonstrates, however, cooperation is currently lacking even within the NATO Alliance.

E. *Cyber Conflicts and NATO*

During the 2007 cyber attack on Estonia, several Estonian officials raised the issue of whether Article 5 of the North Atlantic Treaty Organization (NATO) could be invoked, which maintains that an assault on one allied country obligates the alliance to attack the aggressor.[179] This was the first time in NATO history that a member State had formally requested emergency assistance in the defense of its digital assets.[180] Estonia did receive the limited help that it requested from NATO. Further assistance was unavailable since NATO and the international community alike viewed the 2007 cyber attacks on Estonia as an instance of cybercrime or cyber terrorism as opposed to cyberwar.[181] This was also the case in the cyber attacks against Georgia, in which there was also no conclusive evidence that the Russian government was indeed behind the attacks.[182] There are two reasons for this lack of assistance. First, the attacks were not serious enough to constitute an armed attack necessary for activating NATO Article 5. Second, State responsibility for the attacks could not be conclusively proven. NATO has taken steps to address the gaps in its cybersecurity strategy that the cyber attacks on Estonia underscored, creating the Cooperative Cyber Defense Centre of Excellence in Tallinn, Estonia, and the new Cyber Defense Management Authority (CMDA) in Brus-

[178] See Cybercriminals Move Focus to SA and 2010, IOL SPORT (July 26, 2007, 07:26 AM), http://www.iol.co.za/sport/cybercriminals-move-focus-to-sa-and-2010-1.363522.

[179] North Atlantic Treaty, art. 5, Apr. 4, 1949, 63 Stat. 2241, 2244, 34 U.N.T.S. 243, 246.

[180] Rex B. Hughes, NATO and Cyber Defence: Mission Accomplished?, 2009 ATLANTISCH PERSPECTIEF 4 (2009).

[181] Koms & Kastenberg, *supra* note 127, at 64.

[182] Schapp, *supra* note 43, at 146.

sels, which is a NATO effort to centralize cyber defense capabilities.[183] But without a legal regime for State responsibility in place going forward, such efforts are insufficient by themselves.

It is critical for NATO's future efforts in cybersecurity for its member States to have a comprehensive and settled standard on which to gauge State responsibility for cyber attacks. Specialists at the CDMA, or at the various CERTs of the member States, will not be able to gather the necessary intelligence to prove which nation or group launched a given cyber attack if the standard of proof itself is left undefined. If the effective control standard is indeed accepted as the required standard for State responsibility, then information gathering would have to be total, necessitating new technologies capable of tracking individual packets conclusively back to their true source. Alternatively, if the overall control standard is adopted by the international community, then significant evidence beyond a reasonable doubt of State sponsorship or support for cyber attacks would be sufficient to hold accountable those States, or groups within those States, that launch cyber attacks against NATO member nations or businesses operating within member States. Thus, it is in NATO's own best interest to have a standard of State responsibility for cyber attacks defined and to push for the adoption of the overall control standard over the effective control standard. However, as has been stated, this will likely run against the interests of the cyber powers, making such a deal politically unlikely for the time being. Similarly, many nations will also be unwilling to contribute financially to secure unprotected systems in Africa or elsewhere, unless cyber criminals begin to sufficiently impact the bottom line of enough companies and annoy enough governments for the political calculus to change.

VI. CONCLUSION

This Article has made the case that attribution is a fundamental problem in cybersecurity given the technical challenges of tracing, as seen in the Stuxnet and Night Dragon examples, among others. As a result, we have argued that a burden of proof analysis is essential to satisfy State responsibility for cyber attacks. To this end, we have weighed the benefits and drawbacks of the primary vying regimes for State responsibility under international law: the effective and overall control standards. Due to the technical difficulties of proving attribu-

[183] NATO Opens New Centre of Excellence on Cyber Defence, NATO NEWS (May 20, 2008), http://www.nato.int/docu/update/2008/05-may/e0514a.html.

tion for cyber attacks, along with the unreasonably high standards of proof imposed by the courts that have interpreted the effective control standard, we have argued for the adoption of the overall control standard. This has the benefit of holding State sponsors of cyber attacks accountable where there exists sufficient proof beyond a *reasonable* doubt, as opposed to beyond *any* doubt. Adopting the overall control standard for cyber attacks is thus within the best interests of individuals, companies, and the international community. Given the preference for the effective control standard by the ICJ, ostensibly by the cyber powers, and also in the recent definition of "aggression" adopted by the International Criminal Court, however, the case for a lower burden of proof seems politically unlikely, at least for the foreseeable future.[184] Also, determining a standard for State responsibility is only one element of promoting cybersecurity. There are myriad other related issues that deserve further research and attention by scholars and policymakers alike, such as determining the appropriate forum in which to prosecute State sponsors of cyber attacks, with candidates ranging from the ICJ to national courts and specialized tribunals.

Given this politically difficult situation, it is important to consider whether there may be technical solutions that could help mitigate the challenges to establishing attribution for cyber attacks. Cisco Systems' Donald Proctor has stated, "as we get smarter in our sensor networks and in the way we think about network events and correlation, we'll be able to define attribution with an increasing level of accuracy."[185] Other more practical technical responses may also go a long way towards addressing attribution. These include the issuance of identification cards, similar to a driver's license, or even federated identity schemes.[186] Restricting proxy servers is also a logical step, as that would make it much more difficult for attackers to gain control of another

[184] See Special Working Group's Proposal on the Crime of Aggression, COAL. FOR THE INT'L CRIMINAL COURT, http://www.iccnow.org/?mod=swgca-proposal (last visited Feb. 28, 2011) (defining "aggression" as "planning, preparation, initiation or execution, by a person in a position effectively to exercise over the political or military action of a state, of an act of aggression which, by its character, gravity and scale, constitutes a manifest violation of the charter of the United Nations"). U.N. General Assembly Resolution 2625 declares a war of aggression "a crime against the peace" and exhorts states to refrain from "acts of reprisal involving the use of force . . . [and] from organizing, instigating, assisting, participating in acts of civil strife or terrorist attacks in another State." G.A. Res. 2625 (XXV), GAOR, 25th Sess., Supp. No. 18, U.N. Doc. A/8018, at 122–23 (Oct. 24, 1970).

[185] *Id.*

[186] See David F. Carr, What's Federated Identity Management?, EWEEK.COM (Nov. 11, 2003), http://www.eweek.com/c/a/Channel/Whats-Federated-Identity-Management/.

computer. The benefits of this approach are obvious. Countries like China or North Korea would feel less inclined to launch cyber attacks if hackers' identities could not be so easily masked.

We must also consider that the costs of giving up anonymity online may be equally grave. In countries like Iran, civil rights activists depend on anonymity to launch criticism of the government and further their cause. Also consider the case of the January 2011 coup in Tunisia, which was orchestrated in large part by Tunisian 'hackivists' successfully using DDoS attacks to make an end run around Tunisian censorship.[187] Robert Knake at the Council on Foreign Relations likens this divide on attribution to "crime fighters versus . . . freedom fighters."[188] But there is also the argument that tech savvy cyber criminals will be the best equipped to find ways of getting around traceability issues, while human rights dissidents will face the biggest burden. Compromise may take the form of cyber transactions involving energy and transportation networks or utilities to be made more traceable without necessarily ending anonymous Internet postings more universally.[189]

At the global level, this Article has thus summarized two important trends in the security policies of the cyber powers. First, some States are attempting to shift the test for State responsibility to a lower burden of proof in order to provide justification for moving towards more active defense models, reflecting the difficulty of attribution in cyberspace. This may in part be due to the recognition that any burden of proof is extremely difficult in cyberspace without direct forensic evidence of an attack. Other States more worried about motive and intent being used to justify attribution may push for a higher burden of proof in order to defeat accountability. Second, State practice demonstrates that many states are pushing the thresholds between intervention, use of force, and armed attacks higher so as to tolerate an increasing degree of cyber espionage and other aggressive cyber activities. Even Stuxnet would likely not be categorized as an armed attack, but rather as a covert action. This same scenario has played out in other analogies, according to David Fidler of the Mauer School of Law: "We see here the pattern we usually see with the great powers trying to create more room for their muscle flexing by increasing space for their cyber operations, and then a justification for going after those that threaten them with the

[187] Aidan Lewis, Tunisia Protests: Cyber War Mirrors Unrest on Streets, BBC NEWS (Jan. 14, 2011, 11:24 AM), http://www.bbc.co.uk/news/world-africa-12180954.

[188] *Id.*

[189] *Id.*

lower state responsibility standard."[190] Thus, even a lower standard of proof such as the overall control standard may well help hold State sponsors accountable, but since such an attack would not cross the armed attack threshold, as yet undefined regimes for reparations or other countermeasures would also be needed.

The domestic and global implications of human society's increasingly critical dependence on the Internet makes our ability to deter, detect, and minimize the effects of cyber attacks increasingly necessary.[191] Today, NATO and the United States are at the point of determining how the governance of cyberspace should develop, including attempting to influence the vector of *jus ad bellum* from the very inception of the legal framework for cyberwarfare. The strategies and practices assumed in the short-term will therefore greatly impact how this fast evolving body of law is shaped. Policymakers should consider not only what serves short-term military and commercial interests, but also the shared long-term interest of building a secure and robust cyberspace buttressed by State responsibility and utilizing accountability through multilateral collaboration for the world's existing two-billion Internet users and the billions more to come.

[190] Electronic interview with David Fidler, James Louis Calamaras Professor of Law, Mauer School of Law, Ind. Univ. (Feb. 28, 2011).

[191] Lipson, *supra* note 50, at 3.