UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 12
Issue 3 *Online Issue*

Article 1

10-1-2010

The United States Cyber Command: International Restrictions vs. Manifest Destiny

Tod Leaven

Christopher Dodge

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
12 N.C. J.L. & TECH. ON. 1 (2010)

THE UNITED STATES CYBER COMMAND: INTERNATIONAL RESTRICTIONS VS. MANIFEST DESTINY

Tod Leaven* & ***Christopher Dodge*****

At this time, it is not in the best interest of the United States to adopt, join, or participate in any international treaty resembling a cyberspace extension of the existing "conventional" international laws of warfare. With the activation of the United States Cyber Command, the United States has begun to take the necessary steps to ensure better international cyberspace compliance. The high technology and resource thresholds present in conventional warfare provide warning signs which allow nations to monitor each other for treaty compliance and provide time for measures, such as sanctions, to halt any non-compliant behavior. Cyber-warfare, on the other hand, exposes nations to virtually limitless sudden and immediate attacks, without providing these similar warnings. The advent of cyber-attacks in warfare illustrates how technology can suddenly advance so far and so quickly that the framework of prior treaties is completely inadequate in handling these technological advances. However, lessons learned from prior treaties, notably the series of chemical warfare treaties, can guide the United States' pursuit of peace through this next technological hurdle. Finally, because of the need to secure its leadership in cyberspace, the United States must currently operate efficiently and effectively without the hindrances of an international treaty.

I. INTRODUCTION

United States Secretary of Defense Robert Gates commissioned the United States Cyber Command ("USCYBERCOM") on June 23, 2009, in order "to coordinate Pentagon efforts in the emerging battlefield of cyberspace and

computer-network security."[1] Although the mission statement of USCYBERCOM includes the goals to "prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries,"[2] Lt. Gen. Keith Alexander, director of USCYBERCOM, maintains that "[t]his is not about efforts to militarize cyberspace, . . . [r]ather it's about safeguarding the integrity of our military system."[3] While USCYBERCOM may not have utilized cyberspace in this capacity yet, offensive strikes through cyberspace have previously been conducted by nation-states,[4] and possibly civilians.[5] But,

---

* Tod M. Leaven is a civil litigation attorney at North Carolina Prisoner Legal Services and a former Counterintelligence Agent for the United States Army.

** Christopher Dodge is a J.D. Candidate at the University of North Carolina School of Law, class of 2012.

[1] Thom Shanker, *New Military Command for Cyberspace*, N.Y. TIMES (June 23, 2009), http://www.nytimes.com/2009/06/24/technology/24cyber.html.

[2] Fact Sheets, UNITED STATES STRATEGIC COMMAND http://www.stratcom.mil/factsheets/cc (last visited Sept. 11, 2010, 1:32 PM).

[3] Mike Mount, *U.S. Won't Militarize Cyberspace, Nominee Says*, CNN (April 16, 2010, 12:04 PM) http://www.cnn.com/2010/POLITICS/04/16/military.cyberspace/. This relates to external threats only, since currently "[t]he U.S. military is not allowed to operate within the boundaries of the United States unless authorized by the president. DHS [Department of Homeland Security] is on [sic] charge of cybersecurity inside the border of the United States." *Id. But see* Siobhan Gorman, *U.S. Backs Talks on Cyber Warfare*, WALL ST. J. (June 4, 2010), http://online.wsj.com/article/NA_WSJ_PUB:SB10001424052748703340904575284964215965730.html ("Cyber Command, if asked, would provide 'support' to the Department of Homeland Security to protect networks running the government or key infrastructure, [General Alexander] said. The military also has a strong interest in ensuring the security of some private networks, such as power, because 90% of the military's power is provided by the private sector, [General Alexander] said.").

[4] John Markoff, *Georgia Takes a Beating in the Cyberwar with Russia*, N.Y. TIMES (Aug. 11, 2008), http://bits.blogs.nytimes.com/2008/08/11/georgia-takes-a-beating-in-the-cyberwar-with-russia. The U.S. has engaged in cyber-warfare as early as June 1982 when the U.S. Central Intelligence Agency used a "logic bomb" to explode a portion of a gas pipeline in the Soviet Union. Matt Murphy, *War in the Fifth Domain*, ECONOMIST (June 1, 2010), http://www.economist.com/node/16478792?story_id=16478792.

[5] Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1025 (2007). The exact identity

capabilities such as those presented by cyber-warfare present an argument for a complete overhaul of how current international law should be applied to the new challenges presented by cyber-warfare.[6]

Largely because the weapons of cyber-warfare differ substantially from those of conventional warfare,[7] this Recent Development argues that entering into an international treaty at this time would not be in the best interests of the United States. This Recent Development instead provides that, with the commission of USCYBERCOM, the United States has begun to take the necessary steps to further assert and maintain dominance in cyber-warfare, enabling the United States to wait until more information is available to better analyze its position before entering into an international cyber-warfare treaty. Part II of this Recent Development briefly discusses the current social climate behind the movement for an international treaty on cyber-warfare, as well as similar movements for international treaties in the past. Part III illustrates the dangerous particularities present in cyber-warfare. Part IV discusses how cyber-warfare is currently being addressed, the recent proposals for an international treaty on cyber-warfare, and why the United States should not take part in such a treaty at this time. This Recent Development concludes by arguing

---

of the Russian attackers against Estonia in 2007 remains uncertain, although "[a] group of Russian civilians claim to have operated under the authority of the Russian government." Noah Shachtman, *Kremlin Kids: We Launched the Estonian Cyber War*, WIRED MAGAZINE (Mar. 11, 2009), http://www.wired.com/dangerroom/2009/03/pro-kremlin-gro. There are also reports of the attacks originating from multiple Russian civilian hackers organized through chat boards. *See* Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED MAGAZINE (Aug. 21, 2007), http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

[6] *See generally* Wolfgang McGavran, *Intended Consequences: Regulating Cyber Attacks*, 12 TUL. J. TECH. & INTELL. PROP. 259 (2009) (arguing for an intent-based approach to govern cyber-warfare); RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT TREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT (2010) (Arguing for a "Cyber War Limitation Treaty" ("CWLT") akin to the Strategic Arms Limitation Treaty of the Cold War).

[7] *See id.* at 261–63.

that it is not in the best interest of the United States to enter into an international cyber-warfare treaty at this time.

II. LESSONS LEARNED

A. *The Social Climate Behind the Current Treaty*

Over the past thirty years, the world has rapidly moved from being run by telephones, typewriters, and file cabinets to being run by computers.[8] This transformation has affected nearly every facet of civilization—commerce, energy, education, agriculture, manufacturing, medicine, leisure, and the military.[9] Globalization and efficiency have exploded exponentially.[10] This tumultuous period of technological leaps coincided with the fall of Soviet Russia, a fall that left a power vacuum over half of the world.[11] Current and emerging powers are still racing to fill this power

---

[8] *See generally* Yannis Veneris, *Modeling the Transition from the Industrial to the Informational Revolution*, 22 ENV'T AND PLAN. A 399 (1990).

[9] *See, e.g.*, JOHN C. LEATHERMAN, INTERNET-BASED COMMERCE: IMPLICATIONS FOR RURAL COMMUNITIES (2000), *available at* http://www.eda.gov/PDF/ leatherman.pdf; SMART GRID, OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY, UNITED STATES DEPARTMENT OF ENERGY, http://www.oe.energy.gov/smartgrid.htm; Maya Simon et al., *The Internet and Education*, PEW INTERNET (Sept. 1, 2001) http://www.pewinternet.org/Reports/2001/The-Internet-and-Education.aspx; *See* 2009 World Congress on Computers in Agriculture Convention program guide, http://www.wcca2009.org/documents/OnsiteProgramv007_000.pdf (last visited Nov. 14, 2010) (illustrating current issues in agriculture and computers); JAMES CORTADA, THE DIGITAL HAND: HOW COMPUTERS CHANGED THE WORK OF AMERICAN MANUFACTURING, TRANSPORTATION, AND RETAIL INDUSTRIES *passim* (2004); Lindsey T. Goehring, Recent Development, *H.R. 2068: Expansion of Quality or Quantity in Telemedicine in the Rural Trenches of America?*, 11 N.C. J.L. & TECH. ON. 99 (2009); Paul N. Edwards, *Why Build Computers? The Military Role in Computer Research*, *in* THE CLOSED WORLD: COMPUTERS AND THE POLITICS OF DISCOURSE IN COLD WAR AMERICA 43 (1996).

[10] *See generally* INTERNATIONAL FORUM ON GLOBALIZATION, http://www.ifg.org/about.htm (last visited Nov. 14, 2010) (illustrating general issues and concerns with the rapid pace of globalization).

[11] WOODFORD MCCLELLAN, RUSSIA, A HISTORY OF THE SOVIET PERIOD 323–40 (1986) (detailing the aims of Soviet foreign policy and the extent of global dominance and influence).

vacuum.[12] It is natural that life-changing and potentially dangerous technological leaps amidst global insecurity would heighten sensitivities about the horrors of technology run amuck.[13] An international treaty banning the ill use of this technology is a natural impulse. This current global insecurity is most similar to the global insecurity during the late industrial revolution.

The best lessons on dealing with proposed cyber-warfare treaties come from the history of a series of chemical warfare treaties coinciding with this same late industrial revolution timeframe.[14] Unlike nuclear weapons, for which overwhelming resource demands serve as a gatekeeper,[15] chemical weapons are by and large cheap and readily accessible.[16] Fortunately, state-

---

[12] *See generally* INTERNATIONAL MONETARY FUND, CHINA'S GROWTH AND INTEGRATION INTO THE WORLD ECONOMY, PROSPECTS AND CHALLENGES (2004) (Occasional Paper 232), *available at* http://www.imf.org/external/pubs/ft/op/232/op232.pdf.

[13] Jason Manning, *The Computer Revolution*, THE EIGHTIES CLUB, THE POLITICS AND POP CULTURE OF THE 1980S (2000), http://eightiesclub.tripod.com/id325.htm (summarizing the polarizing fears and cheers of the computer revolution).

[14] Actually, the first chemical warfare treaties were much earlier, but they were punctuated and highly focused. The Strasbourg agreement was signed August 27, 1675, between the French and the Germans, banning the use of "perfidious and odious" toxic devices. This agreement was formed in the wake of the "siege of the city of Groningen, where Christoph Bernhard van Galen, the Bishop of Münster, employed several different explosive and incendiary devices containing belladonna alkaloids intended to produce toxic fumes." Corey J. Hilmas et al., *History of Chemical and Biological Warfare, in* MEDICAL ASPECTS OF CHEMICAL WARFARE 11 (Shirley D. Tuorinsky et al. eds., 2008).

[15] *See* ARJUN MAKHIJANI ET AL., INST. FOR ENERGY AND ENVTL. RESEARCH, URANIUM ENRICHMENT, JUST PLAIN FACTS TO FUEL AN INFORMED DEBATE ON NUCLEAR PROLIFERATION AND NUCLEAR POWER (Institute for Energy and Environmental Research, 2004), *available at* http://www.ieer.org/reports/uranium/enrichment.pdf.

[16] For example, Zyklon-B, a common and readily accessible pesticide, was the gassing agent utilized by Nazi Germany in its extermination camps. CHRISTOPHER R. BROWNING, THE ORIGINS OF THE FINAL SOLUTION: THE EVOLUTION OF NAZI JEWISH POLICY, SEPTEMBER 1939–MARCH 1942, at 356 (2004).

sponsored chemical warfare has largely disappeared.[17] The success achieved by the chemical warfare treaties makes them an even more attractive lesson for effectively negotiating proposed cyber-warfare treaties.

B. *Past Chemical Warfare Treaties*

The late nineteenth century saw the birth of the automobile, airplane, machine-gun, telephone, gasoline engine, radio, and motion picture.[18] Interestingly, this tumultuous period of technological leaps also witnessed fourteen major wars.[19] With the exception of England, all the major world powers fell and Germany and the United States expanded quickly to fill the vacuum.[20] Fearful of the combination of the world's first large scale production of chemicals, the exponential advancement of metallurgy and weaponry, and Russia's diminishing stature as compared with its more aggressive neighbors, Tsar Nicholas II proposed the Hague Convention of 1899.[21] The second declaration

---

[17] The only modern state sponsored chemical warfare was during the Vietnam War and the Iran-Iraq war. *See, e.g.*, Tom Fawthrop, *Vietnam's War Against Agent Orange*, BBC NEWS (June 14, 2004), http://news.bbc.co.uk/2/hi/health/3798581.stm; Elaine Sciolino, *Iraq Chemical Arms Condemned, but West Once Looked the Other Way*, N.Y. TIMES (Feb. 13, 2003), http://www.nytimes.com/2003/02/13/world/threats-responses-iranians-iraq-chemical-arms-condemned-but-west-once-looked.html.

[18] PETER N. STEARNS, THE INDUSTRIAL REVOLUTION IN WORLD HISTORY 43–57 (2nd ed. 1998).

[19] The Second Opium War (1856–1860), the American Civil War (1861–1865), the Franco-Prussian War (1870–1871), the Anglo-Zulu War (1879), the Third Carlist War (1872–1876), the Russo-Turkish War (1877–1878), the Aceh War (1873–1904), the War of the Pacific (1879–1884), the Anglo-Egyptian War (1882), the First Franco-Dahomean War (1890), the Second Franco-Dahomean War (1892–1894), the First Sino-Japanese War (1894–1895), the Spanish-American War (1898), and the Second Boer War (1899–1902). *See* DALE E. FLOYD, THE WORLD BIBLIOGRAPHY OF ARMED LAND CONFLICT FROM WATERLOO TO WORLD WAR I: WARS, CAMPAIGNS, BATTLES, REVOLUTIONS, REVOLTS, COUPS D'ETAT, INSURRECTIONS, RIOTS, ARMED CONFRONTATIONS *passim* (1979).

[20] JOHN HAYWOOD, HISTORICAL ATLAS OF THE 19TH CENTURY WORLD 1783–1914, at 5.03–5.04 (2002).

[21] Michael L. Nash, *A Century of Arbitration: The International Court of Justice*, 274 CONTEMP. REV. 1 (1999).

of this convention was a ban on the use of projectiles that "diffus[ed] . . . asphyxiating or deleterious gases."[22] The second Hague convention in 1907 added a ban on "poison or poisoned weapons."[23] Though well-attended, the two Hague Conventions fell victim to the expansive foreign policies of the great powers: the German Empire, the Russian Empire, the British Empire, France, and the United States. The French were the first to use chemical weapons during World War I in the early Twentieth Century, but the German Empire soon followed suit.[24] Thus despite the treaties in place, by the War's end, chlorine, phosgene, and mustard gases were manufactured and utilized by every major combatant.[25]

Though touted today as the first successful treaties in the nascent body of the international law of war, the Hague Conventions were an abysmal failure regarding chemical weapons. This was because countries still considered chemical weaponry necessary for obtaining a tactical advantage during warfare. The state that could deploy the deadliest gas with the greatest precision could maximize casualties amongst opponents while minimizing its own losses. During the Crimean War in 1854, British chemist and noted politician Lyon Playfair[26] rationalized chemical warfare to the British Ordinance Department by stating:

---

[22] Hague Convention of 1899, Declaration Concerning Asphyxiating Gases, Jul. 29, 1899, 32 Stat. 1839–40.

[23] Hague Convention of 1907, Respecting the Laws and Customs of War on Land, Pt. IV, § II, Ch. I, art. 23, Oct. 18, 1907, 36 Stat. 2301–02.

[24] Michael Duffy, *Weapons of War—Poison Gas*, FIRST WORLD WAR http://www.firstworldwar.com/weaponry/gas.htm (last visited Nov. 9, 2010). At the time of the armistice in 1918, a single plant in Ohio was producing daily more than ten tons of lewisite, a blistering gas more lethal than mustard gas, in preparation for a planned offensive in 1919. *See, e.g.*, Joel A. Vilensky & Pandy R. Sinish, *Weaponry: Lewisite—America's World War I Chemical Weapon*, http://www.historynet.com/weaponry-lewisite-americas-world-war-i-chemical-weapon.htm/2 (last visited Nov. 9, 2010).

[25] L.F. HABER, THE POISONOUS CLOUD: CHEMICAL WARFARE IN THE FIRST WORLD WAR 170 (1986); A.M. PRENTISS, CHEMICALS IN WAR: A TREATISE ON CHEMICAL WARFARE 661–666 (1937).

[26] Playfair lived from 1818 to 1898. His very successful political career in England included Postmaster General (1873–1874), Chairman of Ways and

> It is considered a legitimate mode of warfare to fill shells with molten metal which scatters among the enemy, and produced the most frightful modes of death. Why a poisonous vapor which would kill men without suffering is to be considered illegitimate warfare is incomprehensible. War is destruction, and the more destructive it can be made with the least suffering the sooner will be ended that barbarous method of protecting national rights. No doubt in time chemistry will be used to lessen the suffering of combatants, and even of criminals condemned to death.[27]

This sentiment was echoed throughout the Hague conventions and World War I. It was not until 1925, after the world sobered up to the suffering brought about by chemical weapons, that the global powers were able to formulate a more thoughtful, respected, and enduring ban on chemical warfare.[28]

The Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or other Gases, and of Bacteriological Methods of Warfare, commonly referred to as the Geneva Protocol, was signed in 1925.[29] This treaty only prohibited the initial use of chemical weapons and left open the possibility of unlimited production, storage, and retaliation against a chemical

---

Means (1880–1883), and Vice-President of the Committee on Education (1886). He was ennobled as a Baron, was made a Knight Grand Cross of the Order of the Bath, and the Royal Institute of Public Health awarded him the Harben Gold Medal in 1897. WEMYSS REID, MEMOIRS AND CORRESPONDENCE OF LYON PLAYFAIR *passim* (1899), *available at* http://books.google.com/books?id=YpbKDTpVOAcC&pg=PR7&source=gbs_selected_pages&cad=3#v=onepage&q&f=false.

[27] Hilmas, *supra* note 14, at 11 (quoting C.A. Browne, *Early References Pertaining to Chemical Warfare*, 8 CHEMICAL WARFARE 22, 22–23 (1922)).

[28] It is estimated that chemical warfare during the First World War produced 1,296,853 casualties. A.M. PRENTISS, CHEMICALS IN WAR, A TREATISE ON CHEMICAL WARFARE 661–666 (1937). It is estimated that British casualties alone were 185,000 injured and 8,700 dead. STOCKHOLM INT'L PEACE RESEARCH INST., THE PROBLEM OF CHEMICAL AND BIOLOGICAL WARFARE: VOL. 1 THE RISE OF CB WEAPONS 130 (1971).

[29] The Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, June 17, 1925, 26 U.S.T. 571, 94 L.N.T.S 65.

warfare initiator.[30] This strategy was overwhelmingly successful. World War II, a war notorious for genocide and despicable barbarism, witnessed only a few isolated instances of chemical weapon field use by the Japanese in the Pacific, and even then it was never against Westerners.[31] The major powers of the middle Twentieth Century continued chemical weapons production at an unprecedented level,[32] but the fear of retaliation kept the use of such gasses at bay.[33] With a few notable exceptions, mainly the Vietnam War and the Iran-Iraq War, the Geneva Protocol effectively ended state-sponsored chemical warfare.[34]

---

[30] *See* Text of the Biological and Toxin Weapons Convention, http://www.brad.ac.uk/acad/sbtwc/keytext/genprot.htm (last visited Nov. 9, 2010).

[31] Yuki Tanaka, *Poison Gas—The Story Japan Would Like to Forget*, 1 BULLETIN OF THE ATOMIC SCI. 10, 16–17 (Oct. 1988), *available at* http://books.google.com/books?id=tAYAAAAAMBAJ&q=yuki#v=snippet&q=yuki&f=false. Seven years after they signed the Geneva Protocol, the Italians used mustard gas during the invasion of Ethiopia in the Second Italo-Abyssinian War. David Nicholle, ANTHONY MOCKLER, HAILE SELASSIE'S WAR: THE ITALIAN-ETHIOPIAN CAMPAIGN, 1935–1941, at 81 (1984). However, this was not officially part of World War II. *Id.*

[32] *See, e.g.*, Burton Wright III, *The Chemical Warfare Service Prepares for World War II*, ARMY LOGISTICS UNIVERSITY, http://www.almc.army.mil/alog/issues/NovDec98/MS274.htm (last visited Nov. 9, 2010); *A Short History of the Development of Nerve Gases*, NOBLIS, INC., http://www.noblis.org/MissionAreas/nsi/BackgroundonChemicalWarfare/HistoryofChemicalWarfare/Pages/HistoryNerveGas.aspx (last visited Nov. 9, 2010) (discussing Nazi Germany's discovery and manufacture of Tabun, Sarin, and Soman).

[33] Adolph Hitler, a casualty of World War I gassing, refused to use chemical weapons out of fear of Allied retaliation. Barton J. Bernstein, *Why We Didn't Use Poison Gas in World War II*, AM. HERITAGE, http://www.americanheritage.com/articles/magazine/ah/1985/5/1985_5_40.shtml (last visited Nov. 9, 2010). Of course, there was no similar fear of retaliation from European Jews, whom the Nazis massacred at extermination camps by utilizing Zyklon-B, a cyanide-based pesticide. CHRISTOPHER R. BROWNING, THE ORIGINS OF THE FINAL SOLUTION: THE EVOLUTION OF NAZI JEWISH POLICY, SEPTEMBER 1939–MARCH 1942 *passim* (2004).

[34] Iraq's use of chemical weapons during the Iran-Iraq war was a violation of the Geneva Protocol. Iraq had reserved the right to use chemical weapons against non-treaty participants, but Iran ratified the treaty prior to the conflict. *Geneva Protocol reservations*, STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE http://archives.sipri.org/contents/expcon/cbwarfare/cbw_research_

Nearly seventy years after the Geneva Protocol, and almost one hundred years after the first Hague Convention, the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, commonly known as the Chemical Weapons Convention, was signed.[35] As its full title details, it was a comprehensive ban which included the destruction of current stockpiles.[36] As of July 8, 2010, more than sixty percent of the world's chemical stockpiles had been destroyed.[37] Why were the Geneva Protocol and the Chemical Weapons Convention so successful? Not only was the dream of chemical weapons as a mystical panacea thoroughly crushed by harsh reality, but the specter of runaway science had diminished when the world realized that the industrial revolution was not Armageddon.

III. THE DIFFICULTIES OF CYBER-WARFARE

A. *Estonia, 2007: Anonymity in Cyber-Warfare*

---

doc/cbw_historical/cbw-hist-geneva-res.html (last visited Nov. 9, 2010). The United States utilized chemical weaponry on mass-scale during the Vietnam War. However, the U.S. did not ratify the 1925 Geneva Protocol until 1975, after its involvement in Vietnam. *See* Fawthorpe, *supra* note 17.

[35] Convention on the Prohibition of the Development, Production, Stockpiling, and Use of Chemical Weapons and on their Destruction, Nov. 23, 1993, S. Treaty Doc. No. 103-21, 1974 U.N.T.S. 45, *available at* http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XXVI-3&chapter=26&lang=en.

[36] ARTICLES OF THE CHEMICAL WEAPONS CONVENTION, http://www.opcw.org/chemical-weapons-convention/articles/ (last visited Nov. 9, 2010).

[37] *Global Campaign to Destroy Chemical Weapons Passes 60 Percent Mark*, ORGANISATION FOR THE PROHIBITION OF CHEMICAL WEAPONS, http://www.opcw.org/nc/news/article/global-campaign-to-destroy-chemical-weapons-passes-60-percent-mark/ (last visited Nov. 9, 2010). *See* Karen Drewen, *U.S. Army Bids Farewell to Modern Chemical Weapons Capability, NSCMP Completes Final Step in Destroying Binary Chemical Weapons*, ARMY.MIL NEWS (Nov. 29, 2007), http://www.army.mil/-news/2007/11/29/6348-us-army-bids-farewell-to-modern-chemical-weapons-capability-nscmp-completes-final-step-in-destroying-binary-chemical-weapons.

In April 2007, several Estonian Web sites, including some important to their government infrastructure, were attacked and effectively shut down as a result of a cyber-attack.[38] Although many in Estonia suspected involvement from the Russian government during these cyber-attacks,[39] an Estonian newspaper instead discovered that the three nations generating the most traffic to the newspaper's Web site were Egypt, Vietnam, and Peru.[40] Such traffic would obviously be highly unusual for the Web site of an Estonian newspaper.[41] Attacks like this are possible because of the potential difficulty in ascertaining the identity or location of the attacker.[42] In fact, the attacker can make the cyber-attack seem as if it came from a completely different location.[43] Because of this anonymity, despite the widespread belief that the Russian government was involved at least to some extent, there still exists uncertainty as to whether the Russian government did in fact participate in the attacks.[44]

This unsolved attack against Estonia was made possible because the characteristics of the Internet create a scenario where any online computer in the world can be the source of the attack.[45] Easy access to such effective offensive machinery provides a

---

[38] Scott J. Shackelford, *Estonia Three Years Later: A Progress Report on Combating Cyber Attacks*, 13 No. 8 J. INTERNET L. 22, 22 (Feb. 2010).

[39] *See* Hollis, *supra* note 5, at 1025.

[40] Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED MAGAZINE, Issue 15.09 (Aug. 21, 2007), *available at* http://www.wired.com/politics/security/magazine/15-09/ff_estonia.

[41] *See id.*

[42] Hollis, *supra* note 5, at 1031–32.

[43] *Id.*; Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 892 (1999).

[44] Jonathan A. Ophardt, *Cyber Warfare And The Crime Of Aggression: The Need For Individual Accountability On Tomorrow's Battlefield*, 2010 DUKE L. & TECH. REV. 3, ¶ 22 (2010), *available at* http://www.law.duke.edu/journals/dltr/articles/2010dltr003.html.

[45] *Id.* ¶ 21. One of the methods used in such a scenario is the use of botnets. *Id.* ¶ 20. Defining botnets, Ophardt says that "[s]ome malware allows targeted computers to be 'slaved' to the commands of a single operator who can remotely control aspects of their behavior. These 'slave' computers are commonly known as 'botnets.'" *Id.*

cheap means for an attacker to deal devastating blows to an enemy while maintaining a high level of anonymity.[46] Such potential could make cyber-warfare a top weapon of choice for a terrorist organization.[47] Because of the uncertainty of being able to both detect a cyber-attack and properly identify the source of a cyber-attack, it is likely that it will take several cyber-attacks before action is taken in response.[48]

B. *Difficulty Identifying the Origin of the Attack*

United States Web sites have also been subject to several cyber-attacks.[49] These cyber-attacks can be traced back as far as 2001.[50] Even the British, attacked by Chinese hackers in 2007, had difficulty discerning whether the attacks were instigated by the People's Liberation Army or by individuals acting independent of the Chinese government.[51] Accurately discovering the source of the attacks is important because effective deterrence against cyber-attacks requires proper identification of the attacker.[52] This difficulty was exemplified when cyber-attacks occurred against the United States and South Korea in July 2009, and, rather than originating from North Korea or China as expected,[53] the attacks were based from a server in Miami, Florida.[54] Furthermore, there

---

[46] *Id.* ¶ 21.

[47] McGavran, *supra* note 6, at 265. McGavran exemplifies the capabilities of attackers using these services, saying "[b]ecause proficient cyber warriors are capable of masking their locations, it is a nigh-impossible task to trace the perpetrators. The trail becomes cold after these attacks in hours or even minutes." *Id.*

[48] MARTIN C. LIBICKI, CYBERDETERRENCE AND CYBERWAR 43 (2009), *available at* http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf.

[49] John Markoff & Andrew E. Kramer, *U.S. and Russia Differ on a Treaty for Cyberspace*, N.Y. TIMES (June 27, 2009), http://www.nytimes.com/2009/06/28/world/28cyber.html.

[50] *Id.*

[51] Richard Norton-Taylor, *Titan Rain—how Chinese hackers targeted Whitehall*, THE GUARDIAN (Sept. 5, 2007 03.06 BST), http://www.guardian.co.uk/technology/2007/sep/04/news.internet.

[52] LIBICKI, *supra* note 48, at 41.

[53] JEFFREY CARR, INSIDE CYBER WARFARE 193 (2010).

[54] *U.S. Government Sites Among Those Hit by Cyberattack*, CNN (July 8, 2009), http://www.cnn.com/2009/TECH/07/08/government.hacking/index.html.

may not be anyone to blame at all, as a suspected cyber-attack could even be a complete accident.[55] Even if a cyber-attacker may have been conducting cyber-warfare for an extended period of time but had not yet been identified by the nation they were allegedly attacking,[56] the attacker may be unsure why the cyber-attack is only now being responded to.[57] In sum, the inability to pinpoint the cyber-attacker creates serious questions and uncertainty about how the United States should respond to an attack.[58]

C. *Difficulty Identifying the Parties who Performed the Attack*

Such anonymous capabilities could even make it seem as if an innocent nation instigated an attack, as was exemplified when an anonymous distributed denial of service attack, originating from the United States, attacked the Web site of the Georgian president in July 2008.[59] However, a few weeks later, President Obama, then still campaigning for office, indicated that it was Russia who had issued these cyber-attacks.[60] Such a statement has considerable merit when taking into consideration the fact that these (allegedly Russian) cyber-attacks took place at the same time as the conventional Russian attacks against Georgia in 2008.[61] There are reports, however, that these attacks were not organized by the Russian government as President Obama had believed, or from the United States, but were actually instigated by a vast number of

---

[55] LIBICKI, *supra* note 48, at 45. Examples of accidents like these "could be bad software (which has explained many widespread outages), human error, or natural accidents (the Northeast power outage in 2003 can be traced back to untended trees in Ohio)." *Id.*

[56] *See id.* at 42.

[57] *Id.*

[58] CARR, *supra* note 53, at 176–77.

[59] 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, 57 (2009).

[60] Gregory Hafkin, *The Russo-Georgian War of 2008: Developing the Law of Unauthorized Humanitarian Intervention After Kosovo*, 28 B.U. INT'L L.J. 219, 228 (2010). Hafkin also states that President Obama "accused Russia of 'clear and continued violation of Georgia's sovereignty and territorial integrity,' [and] demanded that Russia withdraw ground troops from Georgia." *Id.*

[61] *See* McGavran, *supra* note 6, at 265.

unknown individuals who were capable of such a large-scale cyber-attack.[62]

In addition to nation-states and individual hackers, cyber-attacks may even be performed by an apparent non-combatant.[63] This proved especially true when a Russian journalist was able to partake in the Georgian cyber-attacks by simply acquiring the means to do so from the Internet.[64] This journalist, Evgeny Morozov, stated that "in less than an hour, I had become an Internet soldier. I didn't receive any calls from Kremlin operatives; nor did I have to buy a Web server or modify my computer in any significant way."[65] Morozov even began his transformation without any knowledge of cyber-attacks.[66] It appears evident that cyber-warfare presents a new challenge to international security, where seemingly anyone can become an enemy of the state.[67] With possible or alleged cyber-combatants ranging from civilians, to journalists, to nation-states themselves, these events show that individuals, not just nation-states, are ready and willing to affirmatively use cyber-warfare against another nation.[68]

---

[62] Kastenberg, *supra* note 59, at 63. *Contra* Charles J. Dunlap, Jr., *Towards a Cyberspace Legal Regime in the Twenty-First Century: Considerations for American Cyber-Warriors*, 87 NEB. L. REV. 712, 720 (2009) ("However, only a nation-state, in my judgment, could cause the kind of debilitating damage that would equate to defeat in war.")

[63] *See* Ophardt, *supra* note 44, ¶¶ 12–23. Ophardt points out that the Russian cyber-attacks against Georgia in 2008 were, at least in part, carried out by individuals instead of a state. Ophardt, *supra* note 44, ¶ 2, ¶ 12.

[64] *See* Kastenberg, *supra* note 59, at 59.

[65] Evgeny Morozov, *An Army of Ones and Zeroes—How I became a soldier in the Georgia-Russia cyberwar*, SLATE, (Aug. 14, 2008, 5:31 PM), http://www.slate.com/id/2197514.

[66] *Id.* In his account, Morozov states that he was "acting entirely on [his] own and using only a laptop and an Internet connection." *Id.*

[67] Ophardt, *supra* note 44, ¶ 21.

[68] Christopher V. Greene, *Cyberwarfare and Our Allies: The Importance of Theater Security Cooperation*, NAVAL WAR COLLEGE 14 (Oct 23, 2009), http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA513954&Location=U2&doc=GetTRDoc.pdf. At one point, "in 2001 … a Navy P-3 surveillance plane colli[sion] with a Chinese fighter plane … [was followed by] 'a huge increase in attacks on United States government computer targets from sources that could not be identified.'" Markoff & Kramer, *supra* note 49.

Unlike conventional warfare, cyber-warfare does not require military training for participants to actively engage in the act.[69] This relatively simple method of becoming a cyber-combatant[70] can become even more powerful when a nation such as Russia actively encourages its citizens to participate in cyber-attacks.[71] Therefore, the relative simplicity and frequency of cyber-attacks, combined with possible state encouragement of such actions, shows that preventing cyber-attacks can present extraordinary difficulties to United States national security forces.[72] With the new dangers of cyber-warfare, some argue that both the United States and international organizations such as NATO need to develop strategies to counter the potential effectiveness and lethality of cyber-warfare.[73]

IV. PROPER DECISIONS FOR THE FUTURE

A. *How Cyber-Warfare is Being Addressed Now*

The capabilities and implications of cyber-warfare have led to a widespread call for an international treaty expanding the current application of the law of war to cyber-warfare.[74] Currently, the law of war under the Geneva Conventions could apply to a large-scale

---

[69] CARR, *supra* note 53, at 27.

[70] *See* Morozov, *supra* note 65.

[71] CARR, *supra* note 53, at 119. Carr states that the Russian government may operate "through Nashi and other groups whose membership includes hackers, resulting in an organized yet open call for unaffiliated hackers to join in." *Id.* Nashi, a Russian youth movement, may also have been involved in the government-sponsored attack on Estonia in 2007. Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192, 206 (2009). For a detailed news report on involvement between the Russian government and Nashi, *see* Tim Whewell, *The Kremlin's New Commissars*, BBC (July 12, 2006, 11:34 AM), http://news.bbc.co.uk/2/hi/programmes/newsnight/5169610.stm.

[72] Shackelford, *supra* note 38, at 23.

[73] *Id.*

[74] *See* John Naughton, *The War of the Cyberworlds is Coming, and We'd Better Be Ready*, THE OBSERVER (June 28, 2009), http://www.guardian.co.uk/technology/2009/jun/28/cyber-warfare-internet-attacks.

cyber-warfare.[75] This body of law has been wholly criticized as being completely inapplicable to the unique challenges that cyber-warfare presents.[76] Currently, the main obstacle to adopting an international cyber-warfare treaty is that the United States does not believe that now is the time for such a treaty.[77] This stance, in our present opinion, is proper for the United States. As far as the law governing cyber-warfare is concerned, at the very least, nations are under an obligation "to prevent and respond to cyberterrorist acts."[78] The commission of USCYBERCOM may be the beginning of such greater domestic protection against the threat of cyber-attacks, and it currently has better capabilities in dealing

---

[75] Sean Watts, *Combatant Status and Computer Network Attack*, 50 VA. J. INT'L L. 391, 411–12 (2010).

[76] *See* Hollis, *supra* note 5, at 1029 (arguing for an "international law for information operations"). Specifically, Hollis argues that "the existing system suffers from several, near-fatal conditions: uncertainty (i.e., states lack a clear picture of how to translate existing rules into the IO [information operations] environment); complexity (i.e., overlapping legal regimes threaten to overwhelm state decision makers seeking to apply IO); and insufficiency (i.e., the existing rules fail to address the basic challenges of modern conflicts with non-state actors and to facilitate IO in appropriate circumstances)." *Id.*

[77] Shackelford, *supra* note 71, at 221. *But see* Siobhan Gorman, *U.S. Backs Talk on Cyber Warfare*, WALL ST. J. (June 4, 2010), http://online.wsj.com/article/SB10001424052748703340904575284964215965730.html (stating that the United States has begun to consider negotiations with Russia over an international cyberwar treaty after Russia had begun negotiations); Ellen Nakashima, *15 nations agree to start working together to reduce cyberwarfare threa*t, WASH. POST (July 17, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/07/16/AR2010071605882.html (reporting that several different nations have agreed to take steps to reduce the dangers of cyber-warfare). We believe, however, that these new developments do not mark an alteration in United States policy to immediately enter into a cyber-warfare treaty, but rather, a proper stance by the United States to remain open to the possibility of a treaty in the future.

[78] Christopher E. Lentz, *A State's Duty to Prevent and Respond to Cyberterrorist Acts*, 10 CHI. J. INT'L L. 799, 823 (2010). This obligation arises under "Security Council Resolution 1373, which creates binding duties upon all states to prevent and respond to 'terrorist acts.'" *Id.* at 801. Lentz argues that "[i]nternational law should recognize that states have a duty to prevent and respond to cyberterrorist acts. Security Council Resolution 1373 created a similar duty regarding terrorist acts, and this should be expanded into the frontier of cyberspace." *Id.* at 816.

with the unique problems of cyber-warfare than other possible countermeasures.[79]

Cyber-warfare is not left completely untouched by the laws currently on the books in the United States, however, as some laws "dealing with international radio or wire communications, and malicious interference with satellites, similar to wire fraud" could apply to cyber-attacks.[80] These laws could be applied when a cyber-attack is not serious or on a large enough scale to merit international attention.[81] Laws like these that are already in place may keep open the possibility of domestic action against cyber-attacks.[82] Therefore, although current international laws may not be sufficient to effectively counter cyber-attacks,[83] it is certainly possible to use current domestic military procedures to combat cyber-terrorism in the United States.[84] Furthermore, these laws could be implemented in a much quicker, more efficient, and more self-serving fashion than by entering into an international agreement.[85]

As one might expect, current international agreements that might be translated to cyber-warfare are presumed to concern relations among different nations, instead of individual actors.[86] Uncertainty still remains, therefore, in how the same law can be translated to individuals, acting independently from any government, who may engage in cyber-warfare.[87] The difference is significant because the ability of a nation to both properly

---

[79] *See* Mount, *supra* note 3.
[80] Shackelford, *supra* note 71, at 225.
[81] *Id.*
[82] *Id.* at 225–26.
[83] *See* Hollis, *supra* note 5.
[84] *See* CARR, *supra* note 53, at 188–89.
[85] *See id.* at 74. Carr states that "[g]lobal cooperation may be a reality one day, but unless something changes to pressure sanctuary states into changing their behavior, there is no impetus for them to do so." *Id.* Carr also says that states may become "sanctuary states," *Id.*, if there is "repeated failure by a state to take criminal action against its attackers." *Id.* at 48.
[86] Hollis, *supra* note 5, at 1047.
[87] *Id.* at 1048.

prevent and retaliate against a cyber-attack depends on this determination.[88]

One example of how important this determination could be is that, at least according to the International Court of Justice, use of military force may not be applicable against an individual who engages in cyber-warfare, leaving the responsibilities instead to the laws of the state that has been, or believes itself to have been, attacked.[89] The problem with this approach to non-state actors is that the attacked state may not be able to use proper defense means against the attack.[90] This restriction exists because the ability of a state to respond is restricted by international agreement, often described as *jus in bello*.[91] Therefore, a response must be meticulously studied and prepared so as to not be too severe against the attacker, assuming that the attack is somehow properly traced to the correct source at all, in order for a response to be both effective and legal.[92]

As we have seen, the two initial requirements to defend against cyber-attacks are proper attribution, followed by the development of a proportional response.[93] These factors may be interconnected, and mishandling either could lead to inadequate and even disastrous results.[94] To satisfy the legal requirements in responding to cyber-attacks, but still be effective, the state that has been attacked must therefore do all that it can to ensure that these two

---

[88] *Id.* at 1049.

[89] *Id.*

[90] *Id.*

[91] CARR, *supra* note 53, at 71. According to Carr, "[j]us in bello stands for the proposition that states do not have a right to use unlimited force against other states during war." *Id.* Carr says that "jus in bello uses four basic principles to regulate the conduct of states during warfare. These are: distinction, necessity, humanity, and proportionality." *Id.* For greater detail regarding *jus in bello* in the modern era, *see* Steven R. Ratner, *Jus ad Bellum and Jus in Bello After September 11*, 96 AM. J. INT'L L. 905 (2002).

[92] CARR, *supra* note 53, at 73. Carr describes these measures, saying, "the victim-state's system administrator must map out the attacking computer system to distinguish its functions and the likely consequences that will result from shutting it down." *Id.*

[93] Shackelford, *supra* note 71, at 201.

[94] CARR, *supra* note 53, at 73.

factors are met.[95] When these requirements are met, the state could be shielded from liability for mistakes taken in response to a cyber-attack.[96] To ensure that a state does not act disproportionally to the threat or the attack, a balancing test is required which weighs the strength of the response in relation to the potential danger such a response will present the state allegedly responsible for the original cyber-attack.[97]

This cyber-invasion will almost certainly be highly unwelcomed by the state allegedly responsible for the original attack.[98] Therefore, an alternative response would be to first ask the state where the attack allegedly began to end the attack, and only to exert a response by the attacked nation if the first step proves ineffective.[99] Once these countermeasures are taken, normal criminal and constitutional law would be applied to judge the response.[100] This countermeasure system could make effective response difficult, as there may still be difficulty in determining which United States department should handle the matter.[101] However, the previous issues that the United States faced in applying the current law of war to cyber-warfare might be alleviated with the commission of USCYBERCOM.[102]

B. *Current Proposals for an International Cyber-Warfare Treaty*

Even if a state decides not to try to meet these difficulties through domestic action, these new difficulties in cyber-warfare still need to be addressed in a manner that allows for effective state responses.[103] Currently, the two nations in strongest disagreement

---

[95] *Id.*
[96] *Id.*
[97] *Id.*
[98] Hollis, *supra* note 5, at 1050.
[99] *Id.* According to Hollis, "The requested state is expected to comply with such requests." *Id.*
[100] LIBICKI, *supra* note 48, at 96.
[101] *Id.*
[102] Lance Whitney, *U.S. Cyber Command prepped to launch*, CNET (March 23, 2010, 11:47 AM), http://news.cnet.com/8301-1009_3-10470186-83.html.
[103] David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SEC. L. & POL'Y 87, 102 (2010). Although he does not give examples of what these "workable procedures" would be, Graham notes that "there is now a growing

over an international treaty are the United States and Russia.[104] The Russian government currently holds that an international treaty updating the law of war with a cyber-warfare section is imperative.[105] The United States opposes this view, instead arguing for cooperative domestic handling among foreign states in cyber-warfare.[106] Specifically, the U.S. plan, as identified by Deputy Defence Secretary William Lynn, advocates for increased focus and improvement in domestic countermeasures to cyber-warfare, while discouraging any international treaty on the matter.[107]

One of the largest proponents for an international treaty is the United Nations.[108] Specifically, United Nations Secretary-General Hamadoun Touré[109] stated that "a cyberwar will be worse than a tsunami—we have to avoid it."[110] Unsurprisingly, Touré has pushed for an international treaty regarding cyber-warfare.[111] Elsewhere in Europe, NATO has become active in cyber-warfare countermeasures with the establishment of "the Cooperative Cyber Defense Center of Excellence."[112] One reason that NATO may be

---

effort to formulate acceptable alternatives to the notion of 'conclusive attribution.'" *Id.* at 93. This means that a state may respond to a cyberattack "only by directly and conclusively attributing the attack to another state actor." *Id.* at 101.

[104] Markoff & Kramer, *supra* note 49.

[105] *Id.*

[106] *Id.*

[107] *US wants NATO 'cyber shield'* (Sept. 16, 2010), http://www.theaustralian.com.au/australian-it/government/us-wants-nato-cyber-shield/story-fn4htb9o-1225924785541. Lynn's plan involves "five pillars", which include "recognising cyberspace as the next domain of warfare; the need for active defences; the protection of critical infrastructure; enhancing collective defence; and the need to 'marshall our technological prowess.'" *Id.*

[108] *See* David Meyer, *ITU Head: Cyberwar Could Be 'Worse Than Tsunami'*, ZDNET UK, (Sept. 3, 2010, 12:35 PM), http://www.zdnet.co.uk/news/security-threats/2010/09/03/itu-head-cyberwar-could-be-worse-than-tsunami-40089995/.

[109] *Id.*

[110] *Id.*

[111] *Id.*

[112] Barry Rosenberg, *NATO unites to thwart cyber threats*, DEFENSE SYSTEMS (Apr. 8, 2010), http://www.defensesystems.com/articles/2010/04/06/cyber-defense-nato.aspx.

at the forefront of the development of new international law is the heavy involvement of Russia in cyber-warfare.[113] However, NATO may not yet be effectively equipped to deal with cyber-warfare.[114] One of the problems, as has previously been stated, is the difficulty of understanding how the law of conventional war applies to cyber-war.[115] Such possible difficulties were exemplified when even the Russian cyber-attacks against Estonia could not warrant NATO protection.[116]

One way for a treaty to be effective would be to first define what constitutes a cyber-attack, then to proceed to specify what law applies to the cyber-attack, as well as explain proper remedies.[117] Alternatively, one could look at the cyber-attack itself and determine the intent of the cyber-attack.[118] This method may offer a solution without too much disruption of current international law, as a cyber-attack would be better defined in the context of "use of force terms" currently in existence.[119]

For a state to confidently respond to a cyber-attack, some argue that properly identifying the source of the attack should not be necessary, provided that the attacked state acts in "good-faith."[120]

---

[113] McGavran, *supra* note 6, at 274. For further discussion of Lynn's five pillar defense argument in respect to NATO policy, *see* Kevin Coleman, *A NATO Cyber Alliance*, DEFENSE TECH (Sept. 20, 2010), http://defensetech.org/2010/09/20/a-nato-cyber-alliance.

[114] Shackelford, *supra* note 38, at 25.

[115] *Id.*

[116] LIBICKI, *supra* note 48, at 179.

[117] Shackelford, *supra* note 38, at 27.

[118] McGavran, *supra* note 6, at 272. McGavran argues that "by focusing on the primary intent, which could be deduced under a totality of circumstances test, annoyance attacks can be distinguished from attacks that intend to cause disruption." *Id.*

[119] *Id.* McGavran describes the "consequentiality approach" as where "a cyber attack would count as the use of force if its *effects* are the same as those that would have resulted from conventional military attacks." *Id.* For more detail on the history and application of this approach, *see generally* Papanastasiou Afroditi, *Application of International Law in Cyber Warfare Operations*, SSRN (Sept. 8, 2010), http://ssrn.com/abstract=1673785.

[120] Matthew Hoisington, Comment, *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, 32 B.C. INT'L & COMP. L. REV. 439, 453 (Spring, 2009).

However, states may find difficulty with this standard because there is currently much confusion as to what constitutes "force" under the United Nations charter.[121] Still, the power of the United Nations has expanded recently following acts by the United Nations Security Council attempting to place a greater emphasis on international security.[122] Furthermore, since cyber-warfare may be properly categorized as subject to "legislative action" under the United Nations,[123] the United Nations Security Council may be able to act affirmatively in situations involving cyber-warfare.[124] However, such measures are not *always* applicable to cyber-warfare, as certain cyber-attacks which cannot be identified may not allow for the same response.[125]

By contrast, USCYBERCOM may be able to avoid lengthy processes such as these, as actions taken by USCYBERCOM may not have to be fully disclosed to the government.[126] Even if disclosure were to be mandated, they would not be subject to typical review by government as in other agencies, being reviewed "instead by the House and Senate Armed Services Committees."[127] Despite the possible difficulties this hierarchy may create,[128] such a scenario may allow USCYBERCOM to become very effective,

---

[121] *Id.* at 440–41. The U.N. Charter states simply that "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." U.N. Charter art. 2, para. 4.

[122] Toby L. Friesen, Article, *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, 109 (2009).

[123] *Id.* at 117–18. Friesen argues that cyber-warfare fits as "[l]egislative action" because "cyberwarfare is a threat to peace and security," is "immediate … as demonstrated by the recent attacks against Georgia and Estonia", and "pose[s] some inherent obstacle to the creation of a consensual international agreement." *Id.*

[124] *Id.* at 118.

[125] Major Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law,* 64 A.F. L. REV. 121, 146 (2009).

[126] Stephen Dycus, *National Leadership, Individual Responsibility: Congress's Role in Cyber Warfare*, 4 J. NAT'L SEC. L. & POL'Y 155, 161 (2010).

[127] *Id.*

[128] *Id.*

because if cyber-defenses "are regarded as 'traditional military activities,' [USCYBERCOM] might escape both the presidential findings requirement for covert actions and any reporting to the intelligence committees."[129] Opening up this freedom for USCYBERCOM to operate may be the answer to Secretary Lynn's proposal to keep the United States at the forefront of cyber-warfare activities.[130]

C. *Why Now is Not the Time for a Cyber-Warfare Treaty*

The United States should not enter an international cyber-warfare treaty at this present time because the world does not have a great enough appreciation for the technology and its consequences yet to be able to formulate a thoughtful regulatory treaty; any such treaty, if entered into, would be intrinsically unenforceable; and tying the hands of the United States, with its premier position in cyber-space, would only cause global harm.

As with the chemical weapons treaties at the end of the Industrial Revolution, the world is not able to formulate a thoughtful, respected, and enduring cyber-warfare treaty.[131] Chemical warfare was rationalized as a vehicle for Germany to secure its rapid expansion as a world power, for the Ottoman and Austria-Hungarian Empires to regain their lost stature, and for the United Kingdom to maintain global dominance.[132] Similarly,

---

[129] *Id.* at 161–62.

[130] *See* Camille Tuutti, *Lynn Details Pentagon's Cyber-Defense Measures*, EXECUTIVEGOV (Aug. 26, 2010), http://www.executivegov.com/2010/08/lynn-details-pentagons-cyber-defense-measures.

[131] *See supra* Part II.B, particularly text accompanying notes 19–24.

[132] From 1848 to 1871, the unification of Germany with Prussia brought about a Navy to Rival England, an army to rival any power in Europe, and growing influence to rival the former Hapsburgs. HAYWOOD, *supra* note 20, at 5.11. The Ottoman Empire had been in existence since 1299 and spanned three continents in the Sixteenth and Seventeenth Centuries. ENCYCLOPEDIA OF THE OTTOMAN EMPIRE, at xxvii (Gábor Ágoston et al. ed. 2009). During the late Nineteenth Centuries, the Ottoman Empire had lost much of its territories, had undergone painful modernization, and had experienced governmental upheavals and boiling internal ethnic tensions. *Id.*; *see also* HAYWOOD, *supra* note 20, at 5.14. The Hapsburgs, the ancestry of the Austria-Hungarian Empire, was the most important royal house in Europe and ruled the Holy Roman Empire from 1438

cyber-warfare is viewed as a vehicle for China to secure its rapid expansion as a world power, for Russia and continental Europe to regain their lost stature, and for the United States (and to some extent the United Kingdom) to maintain global dominance.[133] Though the horrors of World War I need not be repeated for the world to learn the potential for human suffering brought about by unfettered cyber-warfare, there does, at a minimum, need to be a greater appreciation for this potential suffering, if only in theory.[134]

---

to 1740. PETER HAMISH WILSON, THE HOLY ROMAN EMPIRE, 1495–1806, at 72–74 (St. Martin's, NY, 1999). By the late Nineteenth Century, it had lost much of its territory and European influence. HAYWOOD, *supra* note 20, at 5.11–5.13. After Napoleon's defeat, the United Kindom was the sole global power. RONALD HYAM, BRITAIN'S IMPERIAL CENTURY, 1815-1914: A STUDY OF EMPIRE AND EXPANSION 15 (1976). However, the sun was setting on *Pax Britannica* as American and German industrial and military might were beginning to prove rivals. THE OXFORD HISTORY OF THE BRITISH EMPIRE: THE TWENTIETH CENTURY 1–47 (Judith M. Brown et al. ed.) (1999). Though its territorial expansion was at its zenith shortly after the First World War, the financial strain of its vast empire, along with negative public sentiment, was already showing in the late Nineteenth Century. *Id.*

[133] *See, e.g.*, Charles W. Williamson, *Carpet Bombing in Cyberspace*, ARMED FORCES J., http://www.armedforcesjournal.com/2008/05/3375884 (last visited Nov. 9, 2010).

[134] *Compare* REID, *supra* note 26 (describing Lyon Playfair's rationalization) *with* Hollis, *supra* note 5:

> [Cyber-warfare] has the potential to do through the transmittal of data streams what militaries have previously done with bombs and missiles (i.e., depriving the adversary of infrastructure that supports military operations such as electrical or communication systems). But IO [information operations] also offers the promise of accomplishing such goals without as much collateral damage—e.g., disabling an electrical grid temporarily through CNA [computer network attacks] in lieu of destroying the power plant that produces the electricity, or using electronic warfare to disable broadcasting communications in lieu of bombing the facilities and causing some collateral loss of life.

Hollis, *supra* note 5, at 1032. Instead of focusing on terrible but highly plausible outcomes such as the widespread physical collapse of civil infrastructure, including air traffic control, emergency response systems, and banking systems, much journalism seems to liken the effects of cyber-warfare to "being teleported back to the 1970s." Naughton, *supra* note 74. The advent of governmental cloud computing makes governmental function even more sensitive to cyber warfare. *See* Shahid Kahn, Recent Development,

Right now, more focus should be on greater global recognition of this need, rather than on an immediate treaty.

Another reason that now is not the time to enter into a cyber-warfare treaty is because a treaty lacking any means of enforcement does more harm than good. A treaty cannot be enforced if the aggressor is unknown.[135] Even if a cyber-warfare treaty were modeled after the Geneva Protocol in that it allowed for unbridled retaliation, the aggressor's complete anonymity would shield it from the feared retaliation.[136] Even worse, the use of subterfuge could lead to retaliation upon innocent actors.[137] Until a tracing mechanism is realized, this anonymity aspect negates any fruits of a treaty.

Even if the U.S. joining an international treaty on cyber-space is ultimately inevitable, it can be likened to the U.K.'s inevitability in joining the Eurodollar. Though the United Kingdom joined the European Union in 1973, it has yet to join the Eurodollar.[138] Professor Minford of the Cardiff Business School summarizes British skepticism behind continental Europe's political motivations best when he states that "they want us to join the club they have in mind, in order to enjoy our assistance (our strengths) and to limit our ability to compete with it and even undermine it by doing things differently."[139] The U.K.'s abstention from monetary unity served as a great stabilizer for European trade and commerce during twenty years of great fluctuations in the Eurodollar value.[140] It is wise for the U.K. to sit out while the imperfections of monetary unity get ironed out. Likewise, there is similar

---

"Apps.Gov": Assessing Privacy in the Cloud Computing Era, 11 N.C. J.L. & TECH. ON. 259 (2010).

[135] *See, e.g.*, LIBICKI, *supra* note 48, at 41; Ophardt, *supra* note 44, at ¶¶ 21–22. *But see* Hoisington, *supra* note 120, at 453 (stating that identity is not needed if acting in good faith self-defense).

[136] *See* Hollis, *supra* note 5, at 1031–32.

[137] *See* Schmitt, *supra* note 43, at 892; Kastenberg, *supra* note 59, at 57.

[138] ALAN S. MILWARD, POLITICS AND ECONOMICS IN THE HISTORY OF THE EUROPEAN UNION 4 (Routlage, N.Y., 2005).

[139] PATRICK MINFORD, SHOULD BRITAIN JOIN THE EURO—THE CHANCELLOR'S FIVE TESTS EXAMINED, 126 IEA Occasional Paper 2 (Sept. 2002).

[140] *See id.* at 4–6.

skepticism in the United States of continental Europe's and Russia's calls for a cyber-warfare treaty.[141] Given its premier position in cyberspace, it is better if the U.S. abstains from a treaty on cyber-warfare. With roughly eighty percent of the Internet's traffic coming through the United States, it would be hard for any cyber-warfare not to have incursions into the U.S. Internet infrastructure.[142] This necessitates U.S. freedom and flexibility in handling its responses to cyber-conflicts because tying the hands of the U.S. with an ill-thought-out treaty could be deleterious to global cyber-infrastructure. Examples of plausible scenarios which could impede U.S. efficiency and effectiveness are treaty overbreadth, where too many events mandate action, and underbreadth, where too few events are actually actionable. This can be especially problematic in that the U.S. might be joined into a conflict wholly outside of its interests or concern solely because a cyber-ally was targeted. It is wise for the U.S. to allow any crippling effects of a cyber-warfare treaty to be addressed and remedied before it joins.

V. CONCLUSION

Cyber-attacks present difficulties to the United States that are unique and original that any currently proposed international treaty the United States enters will eventually become adverse to the interests of the United States at one point or another. To be sure, this may have been true for several past treaties, but nearly every aspect of cyber-warfare is more complex, versatile, and easily accessible to enemies of the United States than any other past or present threat to national security. Entering into a treaty at this point could tie the hands of United States security forces security, as opposed to preventing or stopping any threat. In fact, "the apparent ease with which a cyber attack may be carried out without

---

[141] Kastenberg, *supra* note 59, at 48 (citing various Presidential Decision Directives which basically state two major reasons why other nations would want to hinder U.S. cyber strength: (1) that the United States is the most powerful nation on earth and this power is dependent upon critical infrastructures and cyber-based information systems, and (2) that the U.S. should review offensive capabilities against enemy computer networks).

[142] *Id.* at 44–47.

attribution could make it impossible to fight back at all."[143] The mere activation of USCYBERCOM shows that the United States will not stay idle in cyber-warfare. Domestic improvements are simply more appealing to the United States in combating cyber-warfare than entering into an international treaty at this time. Going forward, USCYBERCOM should only be the beginning in creating U.S. cyber-security forces.

[143] Dycus, *supra* note 126, at 163.

12 N.C. J.L. & TECH. ON. 1, 28
Cyber-Warfare