PEACETIME CYBER-ESPIONAGE: A DANGEROUS BUT NECESSARY GAME

Luke Pelican[‡]

I. INTRODUCTION

A. Background

In March of 2006, journalist David Perera reported on the potential for Chinese hackers to break into the Department of Defense's Non-classified Internet Protocol Router Net (NIPRNet),[1] the network that provides communications services among various commands and branches within the military.[2] This could be done, Perera wrote, to stifle the American response to a potential invasion of Taiwan.[3]

At an Air Force Information Technology Conference just a few months later, then Major General William Lord told his audience "China has downloaded 10 to 20 terabytes of data from the NIPRNet."[4] He suggested these attempts were aimed at acquiring data to allow hackers clandestine access to the network in the future, and called the issue "a nation-state threat by the Chinese."[5]

Cyber-espionage threats are growing.[6] According to Army General Keith

---

‡ J.D., LL.M., August 2011. The author would like to thank his thesis advisor, Marvin Ammori, and Maj. Erik Mudrinich, USAF, for insight and feedback in the completion of this article.

[1] DSIN Data Services, http://commcns.org/L31uPR.

[2] David Perera, *The Great Wall*, GOV'T EXEC. MAGAZINE (Mar. 1, 2006), http://commcns.org/JNRzPt.

[3] *Id.*

[4] Patience Wait, *Chinese Seek Military ID Info*, GOVERNMENT COMPUTER NEWS (Aug. 15, 2006), http://commcns.org/L31sHE. *See also* Richard A. Clark, Introductory Remarks to Directors' Seminar at the Belfer Center for Science and International Affairs (Sept. 14, 2010) (comparing the amount of data stolen to the equivalent of a digitized Library of Congress), http://commcns.org/JiD3Cd.

[5] Wait, *supra* note 4.

[6] *See generally* JAMES LEWIS, CTR. FOR STRATEGIC AND INT'L STUDIES, SIGNIFICANT CYBER ATTACKS SINCE 2006 (last modified Jan. 19, 2012), http://commcns.org/KTnDmc.

Alexander, Commander of U.S. Cyber Command, "DOD systems are probed by unauthorized users approximately 250,000 times an hour, over 6 million times a day."[7] However, another estimate from Chief Information Assurance Officer for the Department of Defense Robert Lentz suggests the number is actually closer to 360 million probes per day.[8] With regard to federal government systems more generally, attacks on those systems in 2010 increased thirty-nine percent from the previous year.[9] The United States is by no means the sole target of these efforts—the United Kingdom,[10] France,[11] and South Korea[12] are among the more recent targets of cyber-espionage. Moreover, certain countries have been publicly identified as perpetrators of this conduct.[13]

The threat posed by cyber-espionage will continue to develop, but debate exists as to how the United States can adequately address it. Following this introduction, the article briefly examines the cyber-espionage phenomenon with particular attention paid to major events over the last five years. The following section surveys international and U.S. law on espionage and draws on the work of scholars to suggest a less alarmist view of espionage generally. In particular, this article concludes that cyber-espionage, like any other form of espionage, is permissible under international law. The next section focuses on the consequences of espionage in the cyber domain and how, despite its notoriety, it should be recognized as a valuable tool for countries in promoting international stability. Lastly, the article reviews the tools that are at the government's disposal in dealing with cyber-espionage, and examines proposals made by scholars to address this method of intelligence gathering.

---

[7] General. Keith Alexander, Dir., Nat'l Sec. Agency, Cybersecurity Policy and the Role of U.S. CyberCom, Address Before the Center for Strategic and International Studies (June 3, 2010), *available at* http://commcns.org/Lfyavb.

[8] Declan McCullagh, *NSA Chief Downplays Cybersecurity Power Grab Reports*, CNET (Apr. 21, 2009), http://commcns.org/MobuYP.

[9] Elizabeth Montalbano, *Federal Cyber Attacks Rose 39% in 2010*, INFORMATIONWEEK (Mar. 23, 2011), http://commcns.org/J0EqAw.

[10] Richard Norton-Taylor & Julian Borger, *Chinese Cyber-spies Penetrate Foreign Office Computers*, GUARDIAN (UK), Feb. 4, 2011, http://commcns.org/Kw5aOv.

[11] Max Colchester & Gabriele Parussini, *France Investigates Attack on Computers*, MARKET WATCH (Mar. 7, 2011), http://commcns.org/LWN3iu.

[12] Song Sang-ho, *China Stole South Korean Secrets on Drone: Lawmaker*, KOREA HERALD (Mar. 7, 2011), http://commcns.org/Jj7r0p.

[13] *Chinese Hackers Target Government Computers*, THE LOCAL (Dec. 27, 2010), http://commcns.org/J2BggP (discussing Germany accusing China of hacking its government systems); *Agency Admits Spying on Afghan Politician and SPIEGEL Journalist*, SPIEGEL ONLINE—INTERNATIONAL (Apr. 24, 2008) http://commcns.org/KjfPrC (reporting on Germany admitting its espionage aimed at an Afghan minister).

B. Definitions

This paper addresses cyber-espionage, also known as "cyber-exploitation," defined by Herbert Lin as "the use of actions and operations—perhaps over an extended period of time—to obtain information that would otherwise be kept confidential and is resident on or transiting through an adversary's computer systems or networks."[14]

Action through cyber-exploitation is generally covert and is conducted though the least intrusive means in order to extract the sought-after information.[15] Individuals who engage in cyber-exploitation attempt to leave undisturbed the normal operations of a computer system or network, and an ideal method is one that goes undetected by the user.[16]

Cyber-espionage can be contrasted with other forms of cyber activities. Such activities include "cyberterrorism" or full-on "cyberwar", both of which could have devastating effects, as compared to others that are less severe in nature, such as low-level "cybercrime" or "cybervandalism."[17] The technical aspects of these activities complicate the determination of whether cyber-espionage is merely espionage or whether it is something more a daunting task for federal regulators and those tasked with defending our networks.

One technique that can be utilized is system probing, which consists of gathering valuable intelligence while causing no damage to the network. Dr. Herbert Lin of the National Research Council analogizes such activity to approaching a country's airspace without violating it to engage in observations from the air and to test the countries air defense response.[18] This type of behavior alone, although typically regarded as unfriendly, would not normally raise any use of force concerns.[19] If a method of cyber-espionage is the use of such a payload, even if it is designed not to result in any harm to the host system, the host country will not necessarily have that knowledge and could perceive the payload as a harmful threat.[20]

Indeed, probing can be a precursor to something far more destructive,

---

[14] Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SECURITY L. & POL'Y 63, 63 (2010).

[15] *Id.* ("Cyberexploitations are usually clandestine and conducted with the smallest possible intervention that still allows extraction of the information sought.").

[16] *Id.* at 63-64.

[17] Myriam Dunn Cavelty, *Cyberwar: Concept, Status Quo, and Limitations*, CTR. FOR SECURITY STUDIES, 1-2 (2010), http://commcns.org/J2Bi8r (discussing the different categories of cyber-exploitation and the limitations involved in controlling them).

[18] *See* Lin, *supra* note 14, at 79. *See also* Section IV, *infra.*

[19] *Id.*

[20] Lin addresses these and other difficult questions relating to cyber-espionage. Lin, *supra* note 14, at 82-84.

illustrated by the Russian-Georgian crisis of 2008.[21] While there have been many more examples of pure cyber-espionage activities that have not served as staging for a subsequent attack, government and military officials must nonetheless consider the possibility that a systematic probing and incursion onto sensitive systems could be such a preparatory measure.[22]

Dr. Lin also provides an example in which an "offensive cyber operation" deploys a dual purpose payload into the computer network of an adversary.[23] The payload's first role is merely data observation and collection, activity that falls under the espionage category. The second role is to neutralize the system upon command.[24] Whether the deployment of such a payload amounts to espionage or rises to the level of the threat or use of force is a difficult question to resolve.

The Stuxnet worm presents an example of the potential for this type of dual-payload system, though the worm was not employed for espionage purposes. Stuxnet first gained public attention in June of 2010 by researchers in Belarus, who observed its presence on computers belonging to their Iranian clients.[25] Stuxnet's purpose was to disable centrifuges at the Natanz Fuel Enrichment Plan in Iran by manipulating industrial control equipment developed by Siemens.[26] Stuxnet raises significant questions for policymakers and may represent the future of cyber operations.

C. Recent Incidents of Cyber-Espionage

In addition to the NIPRNet example above, other incidents help to illustrate exactly the range of cyber-espionage threats countries face.

---

[21] David Hollis, *Cyberwar Case Study: Georgia 2008*, SMALL WARS JOURNAL 4 (2011), http://commcns.org/Jm6cXB. *See also* discussion on Russia, *infra* Section III.C.

[22] Christopher Bronk, *Blown to Bits: China's War in Cyberspace, August-September 2020*, STRATEGIC STUDIES QUARTERLY 18 (2011), http://commcns.org/LauaG1 (discussing comprehensive cyberespionage campaign conducted prior to broader cyberattack).

[23] An offensive cyber operation serves to introduce "an upgradeable software agent into an adversary system." This agent engages in cyberexploitation and operates destructive action, such as destroying read-only memories that control the boot sequence of machines. Lin, *supra* note 14, at 78-79.

[24] *See* Lin, *supra* note 14, at 79.

[25] Kim Zetter, *Surveillance Footage and Code Clues Indicate Stuxnet Hit Iran*, WIRED (Feb. 16, 2011), http://commcns.org/KoyQsM; David Albright, Paul Brannan & Christina Walrond, *Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report*, INSTITUTE FOR SCIENCE AND INTERNATIONAL SECURITY 1-2 (2011), http://commcns.org/JiD3Ce.

[26] Paul K. Kerr, John Rollins & Catherine A. Theohary, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*, CONG. RES. SERV. 1 (2010), http://commcns.org/JNRATu; David Albright, Paul Brannan & Christina Walrond, *Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report*, INSTITUTE FOR SCIENCE AND INTERNATIONAL SECURITY 1-2 (2011), http://commcns.org/JiD3Ce.

In the fall of 2007 British authorities announced that various government systems had been penetrated by hackers. The London Telegraph reported that the hackers were associated with the People's Liberation Army of China and that the hackers had targeted up to ten departments, including the Foreign Office and Home Office.[27] One expert characterized the conduct as occurring over a period of years, and that it fit within "a new doctrine of the PLA described as 'pressure point warfare'—the attacking of specific nodes to leave the adversary paralyzed."[28] Attempts to gain access to British government systems have continued, and have led to calls by Foreign Secretary William Hague for the adoption of "acceptable rules" for nation state behavior in the cyber realm.[29]

Halfway across the world in 2008, the Indian government announced that it was the target of cyber-espionage activities. The Times of India reported that Indian systems had suffered daily beaches, allegedly by the Chinese, for over a year and a half.[30] Officials indicated that while hacking is a common occurrence, the type conducted by the Chinese was "far more sophisticated and complete," aimed at not only gleaning content from the systems but also discerning vulnerabilities for future exploitation in the event of a broader conflict.[31] The Times of India article was met with some skepticism,[32] and the Chinese government unsurprisingly denied the accusations, going so far as to suggest other countries may be using Chinese systems to carry out such attacks.[33] While many countries treat attacks like those suffered by India as "security breaches," the Indian government considers them on par with "Internet-based terrorist attacks."[34] India has continued to experience exfiltration of sensitive information through cyber-espionage, including data

---

[27] Christopher Hope & David Blair, *Chinese Hackers 'Hit 10 Whitehall Departments'*, THE TELEGRAPH, Sept. 6, 2007, http://commcns.org/KbLmfq.

[28] Richard Norton-Taylor, *Titan Rain – How Chinese Hackers Targeted Whitehall*, THE GUARDIAN, Sept. 4, 2007, http://commcns.org/JylNrB (quoting Alex Neill, head of the Asia Security Programme at the Royal United Services Institute).

[29] Charles Arthur, *William Hague Reveals Hacker Attack on Foreign Office in Call for Cyber Rules*, THE GUARDIAN, Feb. 5, 2011, http://commcns.org/JSlshX.

[30] Indrani Bagchi, *China Mounts Cyber Attacks on Indian Sites*, TIMES OF INDIA (May 5, 2008), http://commcns.org/KjfPHS.

[31] Senior governmental officials publicly declare "hacking" to be a routine activity that inflicts many nations, yet they privately acknowledge the severe cyberwar threat faced by China in particular. *See id.*

[32] Richard Steinnon, *The Indian Front in the Chinese Cyber War*, STEINNON ON SECURITY – NETWORK WORLD (May 6, 2008), http://commcns.org/JNRATx (suggesting that the attacks on India were merely part of China's global espionage efforts).

[33] *Chinese Official Denies Government Hand in Cyber Attacks,* THAINDIAN NEWS (May 5, 2008), http://commcns.org/JNRzPz.

[34] Shamshur Rabb Kahn, *China's Cyber Warfare*, INSTITUTE FOR PEACE AND CONFLICT STUDIES, Article No. 2597 (June 16, 2008) *available at* http://commcns.org/JylNrC.

related to defense systems.[35]

Private industry is not immune from this type of conduct either and often presents a ripe target for cyber spies. In April of 2009, the Wall Street Journal reported that hackers were able to access computer systems containing data on the Joint Strike Fighter project, stealing "several terabytes of data related to design and electronics systems."[36] It was suspected that computer systems used by contractors on the project had been breached over a period of years, and former officials indicated China was likely the culprit behind the intrusions.[37] That same day, however, Pentagon officials and Lockheed Martin, the affected contractor, downplayed the story, claiming that the Wall Street Journal article misrepresented the facts.[38]

The following month, hackers broke into the Homeland Security Information Network, an unclassified but nevertheless sensitive data sharing system utilized by the Department of Homeland Security and state and local authorities.[39] Administrative data files—including "telephone numbers and email addresses"—were apparently the only files accessed,[40] even though this seemingly innocuous data could be used for other espionage efforts.[41]

The most recent and noteworthy incident of cyber-espionage involved a major intrusion into the computer systems of the International Monetary Fund (IMF).[42] While officials' initial statements were muted, they later disclosed that the breach was "sophisticated" and "involved significant reconnaissance prior to the attack."[43] Investigators have since indicated that the intrusion was "linked to a foreign government," and resulted in a major loss of data.[44]

---

[35] *Government Carefully Looking into Hacking of Sensitive Data*, INDIA TODAY (Apr. 8, 2010), http://commcns.org/KbLmfr. A 2010 Shadows in the Cloud Report, developed by the Information Warfare Monitor and Shadowserver Foundation, discusses in greater detail the continued espionage efforts aimed at Indian government systems. STEVEN ADAIR, ET AL., SHADOWS IN THE CLOUD: INVESTIGATING CYBER ESPIONAGE 2.0 JOINT REPORT: INFORMATION WARFARE MONITOR, SHADOWSERVER FOUNDATION (2010).

[36] Siobhan Gorman, August Cole, & Yochi Dreazen, *Computer Spies Breach Fighter-Jet Project*, Wall Street J. (Apr. 21, 2009), http://commcns.org/JSlsi2.

[37] *Id.*

[38] Jim Wolf, *Lockheed Says F-35 Classified Data Not Breached*, REUTERS (Apr. 21, 2009), http://commcns.org/Lau8Or.

[39] Ben Bain, *Information-Sharing Platform Hacked*, FEDERAL COMPUTER WEEK (May 13, 2009), http://commcns.org/Lfyavd.

[40] *Id.*

[41] Shane Harris, *Chinese Spies May Have Tried to Impersonate Journalist Bruce Stokes*, WASHINGTONIAN (Jan. 28, 2011), http://commcns.org/JVA7uf (discussing an incident of spear phishing).

[42] David E. Sanger & John Markoff, *I.M.F. Reports Cyberattack Led to 'Very Major Breach,'* N.Y. TIMES (June 11, 2011), http://commcns.org/KTnDmg.

[43] Sudeep Reddy, Siobhan Gorman & Evan Perez, *IMF Mum on Details of Network Cyberattack*, WALL ST. J. (June 13, 2011), http://commcns.org/J2Bi8x.

[44] Michael Riley & Sandrine Rastello, *IMF State-Backed Cyber-Attack Follows Hacks of*

These incidents demonstrate the prevalence of cyber-espionage, the wide range of information that can be stolen, and the resulting impetus on states to not only defend against these intrusions but also develop the means to conduct them. The following section provides some insight into how countries are gearing up to operate in the cyber realm.

II. CURRENT STATE OF THE LAW

A. Sources of International Law

J.L. Brierly defined international law as "the body of rules and principles of action which are binding upon civilized states in their relations with one another."[45] As John Perkins observed, "[i]nternational law develops in response to an inexorable logic of international relations. It is imposed by the realities of foreign policy. The roots of the law and of its legitimacy lie in this dynamic."[46]

The Statute of the International Court of Justice provides that the court shall consider four sources to decide cases.[47] These include treaties, "whether general or particular, establishing rules expressly recognized by the contesting states;" custom, consisting of *opinio juris* and general practice; "general principles of law recognized by civilized nations;" and "judicial decisions and the teachings of the most highly qualified publicists of the various nations."[48] Given the dearth of treaties and judicial decisions on the matter of peacetime espionage, the works of learned publicists serve an important role in addressing legal issues relating to espionage.

National laws, on the other hand, largely govern the conduct of states within their internal borders. Thus, when analyzing the legality of peacetime state-sponsored cyber-espionage, it is important to recognize the dynamic between national laws and international law, and how that can influence the conduct of states.

B. International Law Regarding Cyber-Espionage

Disagreement abounds as to whether peacetime espionage is permissible

---

Lab, G-20, BLOOMBERG (June 13, 2011), http://commcns.org/Kil8pB.

[45] J. L. Brierly, THE LAW OF NATIONS: AN INTRODUCTION TO THE INTERNATIONAL LAW OF PEACE 1 (Humphrey Waldock ed., 6th ed. 1963).

[46] John A. Perkins, *The Changing Foundations of International Law: From State Consent to State Responsibility*, 15 B.U. INT'L L. J. 433, 456 (1997).

[47] *See* Statute of the International Court of Justice art. 38 (1), June 26, 1945, 59 Stat. 1055 (1945).

[48] *Id.*

under international law.[49] Interestingly, international law has not evolved to address the finer aspects of the question—this has been the case during the height of the Cold War and even into the 21st century.[50]

Support for the permissibility of peacetime espionage under international law extends as far back as the 17th century to the writings of Grotius,[51] a major figure in the development of modern international law.[52] Though espionage conducted in wartime has received attention in international law, in particular the laws governing armed conflict,[53] peacetime espionage has not.[54] According to Roger Scott, "[e]spionage is not prohibited by international law as a fundamentally wrongful activity; it does not violate a principle of *jus cogens*."[55] A *jus cogens* norm is defined by the Vienna Convention on the Law of Treaties as "a norm accepted and recognized by the international community of States as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character."[56] Consequently, a prohibition of or limitation on peacetime espionage is largely governed by the domestic laws of nations.[57]

This view most comports with reality given the nature of statecraft and geopolitical necessities. As one scholar observed, "there has never been a war

---

[49] A. John Radsan, *The Unresolved Equation of Espionage and International Law*, 28 MICH. J. INT'L L. 595, 602 (2007).

[50] *See id.* ("[T]raditional international law is remarkably oblivious to the peacetime practice of espionage. Leading treatises overlook espionage altogether or contain a perfunctory paragraph that defines a spy and describes his hapless fate upon capture." (quoting Richard A. Falk, *Foreword to* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW, at v (Roland J. Stranger ed., 1962)).

[51] Geoffrey B. Demarest, *Espionage in International Law*, 24 DENV. J. INT'L L. & POL'Y 321, 331 (1996). *See also* HUGO GROTIUS, THE RIGHTS OF WAR AND PEACE, INCLUDING THE LAW OF NATURE AND OF NATIONS 331 (Cosimo, Inc. 2007) (1901) ("As the law of nations permits many things, in the manner above explained, which are not permitted by the law of nature, so it prohibits some things which the law of nature allows. Thus spies, if discovered and taken, are usually treated with the utmost severity. Yet there is no doubt, but the law of nations allows any one to send spies, as Moses did to the land of promise, of whom Joshua was one.").

[52] Boutros Boutros-Ghali, *The Role of International Law in the Twenty-First Century: A Grotian Moment*, 18 FORDHAM INT'L L. J. 1609, 1609 (1995).

[53] *See e.g.*, Convention (IV) Respecting the Laws and Customs of War on Land, Annex: Regulations Concerning the Laws and Customs of War on Land art. 29-31, Oct. 18, 1907, 36 Stat. 2277. *See also* Dieter Fleck, *Individual and State Responsibility for Intelligence Gathering*, 28 MICH. J. INT'L L. 687, 689 (2007); Demarest, *supra* note 51, at 334-35.

[54] Demarest, *supra* note 51, at 330.

[55] Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 46 A.F. L. REV. 217, 218 (1999). *See also* Fleck, *supra* note 54, at 688.

[56] Vienna Convention on the Law of Treaties art. 53, May 23, 1969, 1155 U.N.T.S. 331. To this author's knowledge, peacetime espionage has not been explicitly banned under any international judicial decisions or treaties.

[57] Demarest, *supra* note 51, at 330. *See also* Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, 37 HARV. INT'L L.J. 272, 276 (1996).

without spies, and there never has been a peace in which spies have not engaged in preparations for a future war."[58] Espionage serves a critical purpose in enabling states to acquire information on allies and enemies alike, information that may be difficult to discover through more conventional means. This information in turn allows states to effectively navigate the rough currents of international relations and preserve their individual security.

Despite having its share of supporters, the position that peacetime espionage is illegal under international law is ultimately misguided. Professor Radsan cited Manuel Garcia Mora's claim that "peacetime espionage is regarded as an international delinquency and a violation of international law,"[59] though Mora himself acknowledged the point is thoroughly contested.[60] Richard Falk argued espionage is illegal, but noted there is "considerable persuasive policy available to oppose" that conclusion.[61]

Quincy Wright, in a piece on espionage and aerial reconnaissance in peacetime, contended they were illegal, noting "both are illegitimate enterprises because they manifest a lack of respect for foreign territory."[62] Wright was referencing the 1960 incident in which the Soviets shot down American pilot Francis Powers as he flew over the U.S.S.R. in a U-2 spy plane.[63] Given the lack of clarity pertaining to espionage in international law, as evidenced by this incident and the related development of technologies, the 1960-61 regional meeting of the American Society of International Law ("ASIL") chose espionage as its focus.[64] Out of that meeting came a collection of writings entitled, "Essays on Espionage and International Law," which serve as the lens through which this Article examines the phenomenon of cyber-espionage.

Two authors from this collection of works are Quincy Wright and Julius Stone. Called "a founding father" in the academic field of international relations,[65] Wright wrote extensively on the subject and taught for many years

---

[58] Richard A. Falk, *Foreword to* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW, at v (Roland J. Stranger ed., 1962) (quoting Kurt D. Singer, THREE THOUSAND YEARS OF ESPIONAGE: AN ANTHOLOGY OF THE WORLD'S GREATEST SPY STORIES vii (1948)).

[59] Radsan, *supra* note 49, at 604 (quoting Manuel Garcia Mora, *Treason, Sedition and Espionage as Political Offenses Under the Law of Extradition*, 26 U. PITT. L. REV. 65, 79-80 (1964)).

[60] Manuel Garcia Mora, *Treason, Sedition and Espionage as Political Offenses Under the Law of Extradition*, 26 U. PITT. L. REV. 65, 80 n.78 (1964). *See also* Ingrid Delupis, *Foreign Warships and Immunity for Espionage*, 78 AM. J. INT'L L. 53 (1984); Myres S. McDougal et al., *The Intelligence Function and World Public Order*, 46 TEMP. L. REV. 365 (1973).

[61] Falk, *supra* note 58, at 45, 79-80 n.28.

[62] Quincy Wright, *Legal Aspects of the U2 Incident*, 54 AM. J. INT'L L. 836, 849 (1960).

[63] *Id.* at 836-37.

[64] Falk, *supra* note 58, at viii.

[65] Inis L. Claude, *The Heritage of Quincy Wright*, 14 J. OF CONFLICT RESOL. 460, 461 (1970).

at the University of Chicago.[66] Wright's contribution to the ASIL meeting reflected much of what he had written on the U-2 incident. He emphasized that such conduct amounted to a "violation of the rule of international law imposing a duty upon states to respect the territorial integrity and political independence of other states."[67] He further wrote, "[i]n principle, all peacetime espionage in foreign territory is illegal," conceding that "when all are engaging in it, it seems unreasonable to single out one state for utilizing a particular form of espionage, even though that form carries possibilities of hostile action going beyond espionage."[68]

In contrast to Wright's conclusions, Julius Stone took a more pragmatic view of peacetime espionage under international law. Stone taught at the University of Sydney for thirty years, focusing on jurisprudence and international law, and is widely considered to have been "one of the premier legal theorists."[69] He strongly advocated for the establishment of a hotline between the governments of the U.S.S.R. and the United States during the Cold War, a tool crucial for the nuclear age as well as the cyber age.[70] With respect to this topic, Stone contested Wright's condemnation of aerial espionage during peacetime as illegal under international law, undertook his own analysis of the matter, and ultimately concluded that, absent any collateral illegality, no prohibition on peacetime espionage exists.[71]

He began by positing "a view of espionage which transcends that of traditional international law," one born out of the Cold War stand-off that could benefit both sides of that divide.[72] Stone contrasted his era of technological revolution with the period over which the laws of espionage evolved, where communication was largely conducted "face to face, or by physical writing, by carriage, on foot, or on horseback."[73]

Stone analyzed espionage at a time in which the world witnessed the utilization of sophisticated radio communication and satellite technology, along with high altitude surveillance aircraft.[74] He observed how this technological growth altered espionage and the types of information sought by

---

[66] *See generally* William T.R. Fox, *"The Truth Shall Make You Free": One Student's Appreciation of Quincy Wright*, 14 J. OF CONFLICT RESOL. 449 (1970).

[67] Quincy Wright, *Espionage and the Doctrine of Non-Intervention in Internal Affairs*, *in* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW 3, 12 (Roland J. Stranger ed., 1962).

[68] *Id.* at 21.

[69] *About Professor Julius Stone*, U. SYDNEY L. SCH., http://commcns.org/Ja6dmE (last visited Apr. 15, 2012).

[70] *Id.*

[71] Julius Stone, *Legal Problems of Espionage in Conditions of Modern Conflict*, *in* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW 29, 34 (Roland J. Stranger ed,. 1962).

[72] *Id.* at 31.

[73] *Id.* at 36-37.

[74] *Id.* at 37.

countries.[75] Stone cautioned that "our very survival now depends on being contemporaneous in our thinking, and not pretending that we can either govern or preserve ourselves in a transformed world, by the use of notions no longer applicable."[76] To that end, he recognized that espionage would evolve to depend on means such as satellite reconnaissance or sea-based surveillance, which would diminish collateral illegality like territorial intrusion.[77]

Stone's underlying argument rested in the context of the Cold War. He argued that the failure to achieve an inspection regime for the United States and U.S.S.R. meant that such information needed to be acquired by some other means, and the imperfect solution was reciprocal espionage.[78] He argued that "a good system of international inspection must be basically a system of reciprocal espionage, with a seal of international umpireship on it."[79] Thus, without an officially accepted system in place, the only recourse to stave off disaster is mutually tolerated reciprocal espionage.[80]

Stone conceded that this approach posed difficulties. If one were to accept his premise, a major obstacle would be distinguishing between what he termed "red light" and "green light" espionage.[81] Red light espionage is the sort which "served the common-interest function" of espionage and would give warning of the spied-upon state's preparation for an impending surprise attack.[82] Green light espionage, on the other hand, serves "the divisive and destructive function" in offering the spying state knowledge that the spied-upon state was vulnerable to a first-strike, thus inviting an attack.[83] Whether each country would only conduct "red light espionage" and how other states could verify this is an issue under his framework on which he did not elaborate.

Stone's view has some modern descendants. Christopher Baker fixes espionage in functional roots, arguing that espionage facilitates state cooperation and ultimately international security.[84] Baker premises his argument on the idea that treaty enforcement methods, namely verification and assurance measures, are limited in their ability to accomplish their stated purposes.[85] He points to the Comprehensive Nuclear Test-Ban Treaty and how its procedure allows for states to take precautions prior to scheduled

---

[75] *Id.*
[76] *Id.* at 38.
[77] *See* Stone, *supra* note 71, at 34.
[78] *Id.* at 40-41.
[79] *Id.* at 41-42.
[80] *Id.* at 42.
[81] *Id.*
[82] *Id.*
[83] *See* Stone, *supra* note 71, at 42-43.
[84] Christopher D. Baker, *Tolerance of International Espionage: A Functional Approach*, 19 AM. U. INT'L L. REV. 1091, 1091-92 (2004).
[85] *Id.* at 1102-03.

inspections and thus obscure the extent of their treaty compliance.[86]

As a result, Baker sees espionage as a back-up measure of sorts for building cooperation among states. He argues that espionage allows states to "enjoy greater certainty that they will be able to validate international compliance, or at least detect when other participants are failing to comply with the treaty."[87] He suggests that espionage allows states involved in complex negotiations to better understand one another. As a result, espionage "creates a cooperative opportunity for parties with similar functional interests to negotiate mutually-beneficial outcomes."[88]

The justifications proffered by Stone and Baker offer a compelling defense of espionage under international law; however US law is not so amenable. This next section briefly discusses the status of national law on the matter.

C. U.S. Law

1. Espionage Act of 1917

Enacted following America's entrance into World War I,[89] the Espionage Act of 1917 is a far-reaching statute that Congress devised to address issues related to interference in U.S. foreign affairs and commerce, in addition to espionage.[90] The Act criminalizes conduct involving the illicit acquisition of information relating to national security that is intended to either harm the United States or benefit a foreign nation.[91]

According to Herbert Packer, the "legislative trend has been to increase the scope of these provisions, to provide severer penalties, and to lengthen the time within which prosecutions may be commenced."[92] Post-World War II discoveries of the extent of Soviet espionage efforts against the U.S. during the war in part prompted that legislative effort.[93]

The statute's provision on the gathering of defense information describes various methods of illicit acquisition, namely when an individual "goes upon, enters, flies over, or otherwise obtains information. . . ."[94] The statute's definition of defense information itself is comprehensive and covers

---

[86] *Id.* at 1103.
[87] *Id.* at 1104.
[88] *Id.* at 1106.
[89] Charles Cheney Hyde, *The Espionage Act*, 12 AM. J. INT'L. L. 142, 142 (1918).
[90] *Id.*
[91] Espionage Act of 1917, 18 U.S.C. §§ 792-799 (2000 & Supp. 2005).
[92] Herbert Packer, *Offenses Against the State*, 339 ANNALS AM. ACAD. POL. & SOC. SCI. 77, 85 (1962).
[93] *Id.* at 85-86.
[94] 18 U.S.C. § 793 (2006).

information related to military systems and structures, civil infrastructure, and many other items of strategic significance to the United States, in addition to virtually anything connected with "the national defense."[95] A case brought under this law for cyber-espionage could fit under the statute's catch-all "otherwise obtains information" provision. However, given the unique characteristics of cyber-espionage, an issue regarding the application of U.S. law abroad arises.

In *United States v. Zehe*, a district court addressed the extraterritoriality of the Espionage Act.[96] Zehe was an East German national accused of committing acts of espionage against the United States while in foreign countries. In its memorandum opinion, the court found that, as espionage is a crime threatening national security, it "can therefore be punished by Congress even if committed by a noncitizen outside the United States."[97] The court noted that the statutory language did not distinguish between citizens and noncitizens, and that the crime would probably occur as often outside the United States borders as it would within.[98] The court also found the removal of the territorial limitation on the scope of the Act indicative of Congress's intent to have the Act apply extraterritorially.[99] The value of *Zehe* is unclear, and as of this Article's publication, no case involving prosecution for extra-territorial cyber-espionage under the Espionage Act has taken place or been documented.

2. *Computer Fraud and Abuse Act*

The Computer Fraud and Abuse Act ("CFAA") is particularly relevant for cyber-espionage. The CFAA was first enacted in 1984, at a time when legislators did not fully grasp the scope of computer crime.[100] With regard to espionage activities, the legislation was crafted so as "not [to] extend liability beyond existing espionage laws."[101]

The Act contains two provisions potentially applicable to cyber-espionage. The first prohibits accessing without authorization any computer, thereby acquiring sensitive information, and subsequently disseminating that information to persons unauthorized to receive it.[102] The second provision forbids accessing without authorization a US government computer in such a

---

[95] *Id.* § 793(a)-(b).
[96] United States v. Zehe, 601 F. Supp. 196, 197 (D. Mass. 1985).
[97] *Id.* at 198.
[98] *Id.* at 200-01.
[99] *Id.* at 200.
[100] Dodd S. Griffith, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453, 455-56 (1990).
[101] *Id.* at 462.
[102] Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(1) (2006).

way as to "affect" the use of that computer by the government.[103] The Act also grants the Federal Bureau of Investigation primary authority to investigate crimes under (a)(1) involving espionage, indicating that cyberexploitation was a focus of the Act.[104]

There are no indications that the CFAA has been applied extraterritorially. However, not all acts of cyber-espionage may necessarily be conducted from abroad, and the placement of a malware-infected flashdrive on an unsecured computer could yield the same result as an online cyber-espionage operation.[105] Hence, the CFAA may allow the U.S. to prosecute some cyber-espionage, but only to a limited degree.

Having examined the international and national legal landscapes for peacetime espionage, the next section analyzes the extent to which the Stone and Baker justifications of espionage can withstand the continuing evolution of cyber-espionage.

III. CYBER EFFORTS ABROAD

In the face of these phenomena, many countries are developing cyber-capabilities to help them detect and neutralize this increasing threat.

A. China and the Koreas

The threat of Chinese cyber-espionage has been a subject of immense interest to governments and researchers alike.[106] The Chinese military established its first cyberwarfare units in 2003,[107] though it was not until 2010 that the Chinese unveiled what has been dubbed the "[People's Liberation Army] cyber command."[108] The command's purpose is to "address potential

---

[103] 18 U.S.C. § 1030(a)(3) (2006).

[104] *Id.* §§ 1030(a)(1), (d)(2).

[105] Clay Dillow, *Pentagon: 2008 Cyber Breach, Considered the Biggest Ever, Was Caused By a Simple Flash Drive,* POPULAR SCIENCE (Aug. 25, 2010), http://commcns.org/JNRzPA.

[106] STEVEN ADAIR, ET AL., SHADOWS IN THE CLOUD: INVESTIGATING CYBER ESPIONAGE 2.0 (2010), http://commcns.org/JiD614; RONALD DEIBERT, ET AL., TRACKING GHOSTNET: INVESTIGATING A CYBER ESPIONAGE NETWORK 9 (2009), http://commcns.org/Lfy9Hw; Jeremy Kirk, *'Night Dragon' Attacks from China Strike Energy Companies,* NETWORKWORLD (Feb. 10, 2011), http://commcns.org/LWN3iy; MCAFEE FOUNDSTONE PROF'L SERVS. & MCAFEE LABS, GLOBAL ENERGY CYBERATTACKS: "NIGHT DRAGON" (2011), http://commcns.org/KDvhSo.

[107] JOHN TKACIK, JR., HERITAGE FOUND., TROJAN DRAGON: CHINA'S CYBER THREAT 2 (2008), www.heritage.org/research/AsiaandthePacific/bg2106.cfm.

[108] L.C. Russell Hsiaso, *China's Cyber Command?*, CHINA BRIEF (July 22, 2010), http://commcns.org/Jj7r0q.

cyber threats and to safeguard China's national security."[109] Curiously, the creation of this command is aimed at strengthening China's ability to defend its networks from intrusions and attacks.[110]

This claim, though somewhat audacious given China's reputation in this field, is substantiated at least in part by a recent report conducted by the Chinese technology development firm Rising. The report indicated that the United States, Japan, and South Korea bore responsibility for ninety percent of attacks on Chinese classified networks originating outside the country.[111] Along with several related personnel changes in the upper ranks of the Chinese military, this development suggests that the cyber arena is having more influence on Chinese military strategy.[112]

More recently, former U.S. Secretary of State Henry Kissinger issued calls for China and the United States to reach what was characterized as "cyber détente" in the face of the tremendous cyber capabilities both countries possess.[113] Around this time, it was reported that the People's Liberation Army's official newspaper called for the acceleration of cyberwar capability development in the face of growing U.S. military aggression on the Internet.[114]

A week later, however, Chinese officials spoke in a much less alarmist tone, claiming that no state of "cyber war" exists between the two countries, adding that the two governments were not responsible for any hacking against either country.[115] Given the tight control China exerts over its media,[116] it is unclear whether such conflicting messages were the result of backtracking or strategic doublespeak, but regardless of the explanation China will continue to develop its cyber capabilities to counter any perceived threats.

The Korean peninsula has also featured a cyber element in the midst of tension between the Republic of Korea (ROK) and the Democratic People's Republic of Korea (DPRK). The DPRK's cyber capabilities were in the spotlight back in 2009 when ROK intelligence officials indicated that the DPRK had dispatched cyber teams overseas to China to carry out operations,

---

[109] *Id.*

[110] Peng Pu, *PLA Unveils Nation's First Cyber Center*, GLOBAL TIMES (July 22, 2010), http://commcns.org/JiD615.

[111] Scott Henderson, *US # 1 Perp Attacking China's Classified Networks*, THE DARK VISITOR (Mar. 11, 2011), http://commcns.org/KoyQsP.

[112] *See* Hsiaso, *supra* note 108.

[113] Paul Eckert and Daniel Magnowski, *Kissinger, Huntsman: U.S., China Need Cyber Detente*, REUTERS (June 14, 2011), http://commcns.org/Jm6cXC.

[114] Chris Buckley, *China Military Paper Urges Steps Against U.S. Cyber Threat*, REUTERS (June 16, 2011), http://commcns.org/LWN3iB.

[115] Don Durfee, *China Says No Cyber Warfare Between It, U.S.*, THE GLOBE AND MAIL (June 22, 2011), http://commcns.org/Jj7rgE.

[116] ISABELLA BENNETT, COUNCIL ON FOREIGN RELATIONS, MEDIA CENSORSHIP IN CHINA (2011), http://commcns.org/JSlq9O.

though there was disagreement as to the veracity of the intelligence apparatus' claims.[117]

The following year, the ROK established its own "cyber command" aimed at defending against cyber threats while simultaneously developing offensive capabilities for use presumably against the DPRK.[118] The ROK has also established various "cybersecurity centers" to help agencies defend against the threat posed by DPRK hackers, based in part on information from DPRK defectors.[119]

B. The Middle East and India-Pakistan

Middle Eastern countries are also bolstering their cyber capabilities, though not all are doing so in the conventional sense. Israel has significant capabilities both in terms of offensive attacks as well as infiltration measures, and is even ranked as the sixth on a list of "cyberwarfare threats" by a U.S. consultancy firm.[120] In addition to having military teams allocated to this field, the Israelis announced the creation of their own "cyber command" aimed at defending "critical computer systems."[121] There is widespread speculation that Israel may have been responsible for the development of Stuxnet, though no dispositive proof has been produced.

Iran has bolstered its capabilities in this area in the aftermath of the Stuxnet affair. The Iranians responded by undertaking a massive recruitment effort for a cyberwar force, which serves within the Iranian Revolutionary Guards.[122] Despite Iranian rhetoric suggesting sophisticated abilities, much of their efforts in this area appear to be focused on taking down opposition websites and blogs that are critical of the current government.[123] However, in June of 2011 an Iranian military official discussed the country's efforts in developing a cyber command to counter what it sees as growing Western incursions into its

---

[117] Jung Hyo-sik, *North Korea Fingered in Cyber Attack*, KOREA JOONGANG DAILY (July 11, 2009), http://commcns.org/LWN3iC.

[118] LLD and AEF, *Chinese Cyber Army Shows its True Face, Secrets of U.S., Japan, and Korea's Cyber Armies Revealed*, BEIJING DAILY (May 29, 2011), http://commcns.org/JNRzPB (translation of original article provided by ChinaScope).

[119] Sangwon Yoon, *Is the Inter-Korean Conflict Going Cyber?*, AL JAZEERA (June 24, 2011), http://commcns.org/J0EoIF.

[120] Dan Williams, *Spymaster Sees Israel as World Cyberwar Leader*, REUTERS (Dec. 15, 2009), http://commcns.org/KoyQsR.

[121] Calev Ben-David, *Israel to Establish Command Center for Cyber Threat Defense*, BLOOMBERG (May 18, 2011), http://commcns.org/JylNrE.

[122] Kevin Fogarty, *Iran Responds to Stuxnet by Expanding Cyberwar Militia*, IT WORLD (Jan. 12, 2011), http://commcns.org/KbLony.

[123] Nasser Karimi, *Report: Iran's Paramilitary Launches Cyber Attack*, WASH. POST, Mar. 14, 2011, http://commcns.org/MobuYS.

political sovereignty, what it deems "soft warfare."[124]

Syria has also made strides in developing offensive cyber capabilities, but those capabilities appear focused on attacking foreign websites and cracking down on domestic dissidents in the wake of the Arab Spring.[125] Additionally, Turkey has undergone cyberattack drills aimed at assessing the government's ability to respond to such threats.[126]

Meanwhile, cyber threats against India have led the country to begin developing its own Cyber Command & Control Authority.[127] The centralized organ was deemed necessary, as ad-hoc responses by individual agencies were seen as ineffective in countering attacks and intrusions into government systems.[128] The most recent cyber spats involved hackers located in India attacking Pakistani websites, ostensibly in remembrance of the victims of the Mumbai terrorist attacks of 2008, but that is arguably part of a larger underlying tension between the two countries.[129] India has also increasingly cooperated with the United States on cybersecurity issues, with the goal of developing a peaceful and secure Internet.[130]

Not much is known of Pakistan's cyber capabilities. Though India has been engaged with Pakistan in cyber conflict, it has largely consisted of vandalism of various websites and efforts to control other sites.[131] However, in May 2011, the Hindustan Times reported that an officer of the Inter-Services Intelligence (ISI), Pakistan's intelligence service, hacked into an Indian Army major's email account and in the process secured "many sensitive documents."[132] Compounding the severity of the breach was that the victim had secret and top secret documents that he was not authorized to access, multiplying the potential intelligence coup for the ISI.[133]

---

[124] *Iran to Boost Soft Power Through Establishing New Cyber Command*, FARS NEWS AGENCY (June 15, 2011), http://commcns.org/JNRzPD.

[125] Helmi Noman, *The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army*, INFOWAR MONITOR (May 30, 2011), http://commcns.org/Ja6dmG.

[126] *Turkey to Conduct Cyber Attack Drills*, TODAY'S ZAMAN (Jan. 21, 2011), http://commcns.org/JLfyQm.

[127] Harish Gupta, *As Cyber Attacks Rise, India Sets Up Central Command to Fight Back*, DAILY NEWS & ANALYSIS (May 15, 2011), http://commcns.org/Jm6cXF.

[128] *Id.*

[129] Jahanzaib Haque, *Cyber Warfare: Indian Hackers Take Down 36 Gov't Websites*, THE EXPRESS TRIBUNE (Dec. 1, 2010), http://commcns.org/JSlsia.

[130] *Close Cooperation with India on Cyber Security Issues: US*, THE ECONOMIC TIMES (May 19, 2011), http://commcns.org/Lau94G.

[131] Sandeep Unnithan, *Inside the Indo-Pak Cyber Wars*, INDIA TODAY (Mar. 18, 2011), http://commcns.org/Ja6dmJ.

[132] Sanjib Kr Baruah, *ISI Major Hacked Army Officer's Mail*, HINDUSTAN TIMES (May 16, 2011), http://commcns.org/L31sXX.

[133] *Id.*

C. Russia and Europe

Information on Russia's cyber-espionage institutions and doctrines is scant. Russia and the US are equally active in cyber intelligence gathering from the other, as well as keeping those cyber capabilities obscured.[134] Russia is estimated to spend approximately $127 million on its cyberwarfare programs, with a force size of more than 7,300 personnel.[135] The Federal Protection Service is chiefly responsible for the gathering of signals intelligence, though the Foreign Intelligence Service (SVR) and Military Intelligence (GRU) play a role in this area as well.[136] Russia's precise capabilities in terms of cyber-espionage are also unclear, but two incidents reveal a certain level of sophistication.

During the weeks prior to the Russian-Georgian conflict in 2008, Russian hackers engaged in "information exfiltration activities conducted to accumulate military and political intelligence from Georgian networks."[137] The intelligence gathering conducted by the hackers represented a complex and highly coordinated operation, and illustrates the blurring of the lines between routine cyber-espionage and espionage as a precursor to cyber and conventional warfare.[138]

The following year Russian "hacktivists" were accused of orchestrating an intrusion into the computer systems of the University of East Anglia's Climatic Research Unit and subsequently leaking thousands of emails incriminating scientists in a data manipulation scandal.[139] No firm link between the act and the Russian government was established. The selection of emails and complexity of the data in question led to speculation that the incident was not one conducted by average computer hackers but likely involved in some capacity Russian intelligence.[140] If the accusations are well-founded, this incident indicates Russia's willingness to use cyber-espionage as a means of influencing policy at the international level.

European nations have also been spurred to act in the face of this evolving

---

[134] FRANZ-STEFAN GADY AND GREG AUSTIN, EASTWEST INSTITUTE RUSSIA, THE UNITED STATES, AND CYBER DIPLOMACY – OPENING THE DOORS 1 (2010), http://commons.org/KDvkNP.

[135] Kevin Coleman, *Russia's Cyber Forces*, DEFENSE TECH (May 27, 2008), http://commons.org/LWN5qs.

[136] ROLAND HEICKERÖ, SWEDISH DEFENCE RESEARCH AGENCY EMERGING CYBER THREATS AND RUSSIAN VIEWS ON INFORMATION WARFARE AND INFORMATION OPERATIONS, 28, 34 (2010), http://commons.org/KoyQsS.

[137] David Hollis, *Cyber Case Study: Georgia 2008*, SMALL WARS JOURNAL 3 (Jan. 6, 2011), http://commons.org/Kw5a0L.

[138] *Id.*

[139] Shaun Walker, *Was Russian Secret Service Behind Leak of Climate-Change Emails?*, THE INDEPENDENT (Dec. 7, 2009), http://commons.org/L31sY0.

[140] *Id.*

threat. In 2009, the United Kingdom's government created two organizations, the Cyber Security Operations Centre (CSOC) and the Office of Cyber Security (OCS), which are tasked with analyzing trends in cyberspace and working on preventing threats against British systems.[141] Some reports indicated that the OCS would have offensive capabilities, including "exploiting opportunities in cyber space,"[142] though officials did not explain what that meant in greater detail.[143]

In 2009, France formed the French Network and Information Security Agency ("FNISA") to safeguard government information systems and react to cyber threats.[144] FNISA resides under the authority of the General Secretary for National Defense, though the agency also plays a role working with the private sector in keeping it abreast of security threats.[145]

Germany, in response to numerous incursions into its systems—over 1600 cyber attacks in 2010 alone—established its own National Cyber Defense Center ("NCDC") in Bonn in June 2011.[146] With the creation of the NCDC, the newly appointed Interior Minister referred to cyber security as "a central issue."[147] The NCDC actually comprises many agencies working together to defend against cyber threats.[148]

The Swiss are developing an outfit for Computer Network Operations within their existing Centre for Electronic Operations of the Armed Forces Command Support Organisation ("CEO").[149] Swiss legal opinions preclude the use of Computer Network Exploitation for any purpose other than defensive measures, though the CEO plans to fully develop attack and exploitation capabilities.[150]

At the intergovernmental level, the North Atlantic Treaty Organization (NATO) has also taken steps to develop cyberwarfare defense, including the creation of the Cooperative Cyber Defence Center for Excellence, the mission

---

[141] ALEX MICHAEL, DEFENSE ACADEMY OF THE UNITED KINGDOM, CYBER PROBING: THE POLITICISATION OF VIRTUAL ATTACK 20 (2010), http://commcns.org/KjfPI2.

[142] UK OFFICE OF CYBER SECURITY, CYBER SECURITY STRATEGY OF THE UNITED KINGDOM 15 (2009), http://commcns.org/LauaWl.

[143] Tom Espiner, *U.K. Cybersecurity Office to Have Attack Role,* CNET (June 25, 2009), http://commcns.org/LfyaLu.

[144] MISSION—AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION, http://commcns.org/JylQnk.

[145] Peter Sayer, *France Creates New National IT Security Agency,* CIO (July 10, 2009), http://commcns.org/Jj7s4m.

[146] Sebastian Fischer and Ole Reissmann, *Germany Arms Itself for Cyber War*, SPIEGEL ONLINE (June 16, 2011), http://commcns.org/JyYyiS.

[147] *Id.*

[148] Filippa von Stackelberg, *Germany Prepares for Cyber War*, NEW SECURITY LEARNING, http://commcns.org/LfyaLv.

[149] Cavelty, *supra* note 17, at 3.

[150] *Id.*

of which is to "enhance the capability, cooperation and information sharing among NATO, NATO nations and Partners . . . ."[151] Another NATO organization, the Cyber Defence Management Authority, is tasked with "coordinating cyber defence across the Alliance," and operates under the authority of the NATO Consultation, Control and Command Board.[152] The extent to which these organizations are equipping NATO countries to conduct cyber-espionage or other activities is unclear, though defending against cyber-espionage will likely factor into their efforts.

IV. UNIQUE ASPECTS PRESENTED BY CYBER

Unlike the political atmosphere of the Cold War, the current international climate is not one dominated by two superpowers with an arsenal of nuclear weapons poised for global annihilation. Rather, the means and modes of wreaking havoc are in many hands.[153] With human rights abuses and political revolutions coming into greater importance for foreign policy, access to reliable intelligence through a variety of means is increasingly necessary. Indeed, information pertaining to allies and adversaries is even more crucial in today's environment.

Espionage—and in particular cyber-espionage—is a balance of trade-offs. States have a vested interest in having as much reliable information as possible at their disposal. That information comes at a cost, however, whether in manpower, treasure, or the potential loss of amicable relations with fellow countries. No doubt Stone and Baker raise compelling arguments supporting the merits of espionage, in particular as it benefits international security and cooperation. But the calculus for the espionage trade-offs is altered when it takes place in the cyber domain, and whether Stone's and Baker's constructs of espionage can withstand the changes presented is another matter.[154] There has

---

[151] NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, *Mission and Vision*, http://commcns.org/Kw5a0N.

[152] JEFFREY HUNKER, CYBER WAR AND CYBER POWER – ISSUES FOR NATO DOCTRINE 8, 9 (2010), http://commcns.org/LfyaLx.

[153] John J. Kruzel, *Cybersecurity Poses Unprecedented Challenge to National Security, Lynn Says,* AMERICAN FORCES PRESS SERVICE (June 15, 2009), http://commcns.org/Jm6cXG ("'Once the province of nations, the ability to destroy via cyber means now also rests in the hands of small groups and individuals: from terrorist groups to organized crime, hackers to industrial spies to foreign intelligence services,' [Deputy Secretary of Defense William Lynn] told the Center for Strategic and International Studies here."). *See also* COMMISSION ON THE PREVENTION OF WEAPONS OF MASS DESTRUCTION PROLIFERATION AND TERRORISM, PREVENTION OF WMD PROLIFERATION AND TERRORISM REPORT CARD (2010), http://commcns.org/JNRzPI.

[154] Major Arie J. Schaap argues that despite the changes cyber presents, "at its core, it is still espionage and should be looked at differently then (sic) cyber warfare operations when attempting to establish lawful or unlawful activities under international law." Major Arie J.

been little scholarship on the evolution of technology and its effect on the legality of peacetime espionage. Stone and Baker thus provide a stepping stone to analyze the issues presented by cyber-espionage.

At the time Stone made his assertion, the technological frontier for espionage involved satellites, specialized aircraft and sea vessels, all of which could collect intelligence without ever crossing into the territory of another country.[155] He also noted, with respect to the issues raised by space technology, that "territorial sovereignty in the old sense of full psychological sacrosanctity is no longer with us."[156] His forecast proved accurate, as the technical means put into use rapidly evolved throughout the Cold War and proved a useful means for the United States to acquire intelligence.[157]

Cyber-espionage exponentially increases those changes contemplated by Stone. The 1960 U-2 crisis was a relatively straightforward situation involving a US aircraft breaching the territorial sovereignty of the USSR, albeit for reconnaissance purposes only. The flights were motivated by a desire to respond to significant espionage effort put forth by the Soviets, who utilized both an extensive personnel network in the United States, as well as their nascent but effective satellite reconnaissance capabilities.[158] The flights were further justified on the grounds that they were not armed and therefore not provocative in nature.[159] Despite these considerations, their revelation still caused a massive international crisis.

The U-2 over-flights also revealed that the Soviet Union's military was much weaker than previously suggested.[160] This knowledge arguably contributed more to stability than did reliance on less accurate means of intelligence. This is consonant with "Eisenhower's dictum that intelligence on 'what the Soviets *did not* have' was often as important as information on what they did."[161]

Furthermore, the frontier of what Stone referred to when speaking of espionage that would require no collateral illegality is very nearly reached with cyber-espionage. It can be done from anywhere and often through surreptitious

---

Schaap, *Cyberlaw Edition: Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121, 141 (2009).

[155] Stone, *supra* note 72, at 37, 43.

[156] *Id.* at 36.

[157] Kristie Macrakis, *Technophilic Hubris and Espionage Styles During the Cold War*, 101 ISIS 378, 378 (2010).

[158] E. Bruce Geelhoed, *Dwight D. Eisenhower, the Spy Plane, and the Summit: A Quarter-Century Retrospective*, 17 PRESIDENTIAL STUDIES QUARTERLY – PROVIDE FOR THE COMMON DEFENSE: CONSIDERATIONS ON NATIONAL SECURITY POLICY 95, 98 (1987).

[159] *Id.* at 99.

[160] Mackrakis, *supra* note 158, at 381.

[161] Christopher Andrew, *Intelligence and International Relations in the Early Cold War*, 24 REV. OF INT'L STUD. 321, 328 (1998).

means. This method avoids the risks accompanied by in-person espionage or aerial over-flights.

Personnel are often put in harm's way with traditional forms of espionage, whether they are on the ground clandestinely, flying high above in an aircraft, or within foreign territory conducting maritime surveillance. With cyber-espionage, the "spy" can operate from the relative safety of his or her home country, using technology as the means of acquiring intelligence.[162] If the means employed work as intended, the spied-upon target won't know anything is amiss; if they malfunction or otherwise fail the risk of harm to the "spy" or host state is relatively minimal.

As the examples of cyber-espionage in Section I demonstrate, the acts are often traced back to servers in foreign countries—meaning the act of gathering this information is occurring outside of the target states.[163] Additionally, an intrusion traced to a server in a particular country may nonetheless have been committed by another country, either through technical means such as routing[164] or by physically conducting an incursion from that particular country.[165] These measures, though not necessarily immune from investigation and attribution, can make those tasks much more difficult for the target state, as well as host countries.[166]

Moreover, Stone's "green light espionage" can be much more problematic in the cyber realm. Lieutenant Commander Paul Walker discusses the use of "positioning of forces" in conventional warfare as a means of achieving strategic surprise over an adversary, and explains how that concept translates into the cyber realm.[167] Walker identifies two components of force positioning in cyberspace: 1) "exploit a vulnerability in the system in order to get inside the system" and 2) "information-based action" from within the system to facilitate broader action.[168]

Examples of this second prong could include "altering data, destroying data,

---

[162] Wolfgang McGavran, *Intended Consequences: Regulating Cyber Attacks*, 12 TUL. J. TECH. & INTELL. PROP. 259, 262 (2009).

[163] Jonathan A. Ophardt, *Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield*, 3 DUKE L. & TECH. REV. 1, 23 (2010).

[164] WILLIAM A. OWENS, KENNETH W. DAM, & HERBERT S. LIN, NAT'L ACAD. PRESS, NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 138-41 (2009) (discussing complexity of technical attribution).

[165] Hyo-sik, *supra* note 118.

[166] Martyn Williams, *North Korea's Chinese IP Addresses*, NORTH KOREA TECH (June 26, 2011), http://commcns.org/JLfyQs.

[167] Paul A. Walker, *Traditional Military Activities in Cyberspace: Preparing for "Netwar"*, 22 FLA. J. INT'L. L. 333, 349 (2010).

[168] *Id.* at 349.

sending false messages, or causing systems to malfunction or stop working."[169] Walker further observes that positioning in the cyber context "will often involve peacetime access, either through remote or close means, in preparation for later actions during hostilities."[170]

This ambiguity is not too different from what the Soviets faced with the U-2 over-flights, or even the traditional conduct of espionage involving persons instead of technology. The aforementioned discussion between US and Soviet diplomats regarding the differences between spy planes potentially armed with weaponry and "secret agents" equipped with explosive charges demonstrates this parallel. One could point to the dual-payload pieces of code discussed by Lin and find that a threshold has been crossed, that cyber is different than anything previously encountered. After all, with some sophisticated malware, one country could secure battle plans, infrastructure schematics, and other sensitive material from an adversary, all as a prelude to a massive attack.

Such a claim is too attenuated, despite the potential for significant harm that could result from offensive cyber measures directed at the United States. While it is true that the concerns raised by Stone regarding the distinction between green light espionage and red light espionage are amplified in the cyber realm, those concerns persist with the other forms of espionage previously discussed. Spies infiltrating the country and hiding in plain sight working for sensitive facilities can commit sabotage and wreak havoc. Surveillance aircraft and reconnaissance satellites could be equipped with volatile weapons to deploy and deceive the surveilled until it is too late. Yet espionage by those means persists and the international community appears to tolerate it.

Based on those analogies, cyber-espionage should not be treated any differently. The benefits to international stability and cooperation as outlined by Stone and Baker are as relevant today as they ever have been. The altered calculus can be viewed in two ways—as making the threat of harmful cyber-attacks much more real, and as increasing the ease by which countries can ascertain one another's intentions and activities. To the extent that the former threat exists, the benefits offered by the latter far exceed it.

Thus, cyber-espionage, like other forms of espionage, should persist unabated. States should respond to it as they do any other attempts to acquire sensitive information: making best efforts to secure that information, and when possible, to pursue elements operating within their territory who are facilitating the conduct of cyber-espionage. But in spite of the increased use of cyber-espionage by many states, there are proposals that seek to limit its scope or use

---

[169] *Id.* at 350.
[170] *Id.*

altogether.

The following section examines some of these proposals and analyzes their relative merits.

V. HOW THE U.S. CAN RESPOND

A. Continued Application of Existing Law

The Espionage Act and, more directly, the CFAA provide the legal basis to prosecute instances of cyber-espionage. However, there has been a dearth of prosecutions under these laws despite the sheer number of attacks against US government systems.[171] Even if the current law was suitable for prosecuting instances of cyber-espionage, intelligence agencies must confront another critical issue in responding to the espionage—whether to track and gain more information about those activities, or to arrest and prosecute, and thereby close a potential source of information.[172]

B. Development of New Law to Account For Differences in the Cyber Realm

1. Cyber Espionage Act

One proposal calls for Congress to pass a Cyber Espionage Act (CEA), which would "criminalize acts of hacking intended to disrupt American economic or military computer infrastructure, military secrets, or trade secrets."[173] The scope of the CEA would be limited to acts that are done for the benefit of foreign governments, and intrusions originating outside the United States would fall under the jurisdiction of the Pentagon "or a related agency."[174]

The CEA is premised on the idea that, although 18 U.S.C. § 1030(a) already criminalizes these types of acts, it is somehow ineffective in combating the increasing threat of cyber-espionage.[175] The author claims that the CEA serves three critical needs: first, it would allow prosecutors to go after hackers located in the US who are operating on behalf or in support of foreign governments;

---

[171] I contacted the Office of Intergovernmental and Public Liaison for assistance in researching this information as my personal efforts have netted few results. For instance, the Cybercrime Page for the DOJ has very few prosecutions involving the espionage provision.

[172] *Frontline: From China With Love—Interview: Edward Appel*, http://commcns.org/JiD6hr (former FBI Special Agent discussing issues counter-intelligence officers confront in tackling espionage).

[173] Jonathan Eric Lewis, *The Economic Espionage Act and the Threat of Chinese Espionage in the United States*, 8 CHI. KENT J. INTELL. PROP. 189, 231-32 (2009).

[174] *Id.* at 232.

[175] *Id.* at 232-33.

second, it would be a wake-up call to the Chinese that the United States takes the threat seriously and will respond, by prosecution if possible; and third, the CEA would impose stiffer penalties than those currently provided for in section 1030.[176]

Given that the CFAA has been largely inadequate for addressing acts of cyber-espionage committed from outside the territory of the United States, the advantage to be gained by passing the CEA is unclear. To the extent that foreign nationals are conducting cyber-espionage within US borders, the CFAA and or Espionage Act may presumably be utilized. Otherwise this proposal would amount to little more than political posturing.

C. Non-Judicial or Countermeasure Responses

1. Diplomatic Efforts and Information Sharing

Another proposal in the context of economic cyber-espionage has been to exercise diplomatic power in an effort to stem espionage. Aaron Burnstein has suggested that in order to foster an atmosphere of measured trust and transparency, nation states could informally exchange information as to what scientific and technological projects each respective country is funding and the amount of resources being devoted to those projects.[177] The exchange of this information would promote transparency by allowing countries to verify, to some extent, that technological developments in those countries are "not cast under suspicions raised by economic espionage prosecutions in the United States."[178]

The proposal is not without flaws, as Burnstein acknowledges, with the most obvious one being that countries are likely unwilling to share any sensitive information with other countries.[179] He nonetheless points to current practices of information sharing among countries as a foundation upon which some future exchange could take place.[180] Regardless of whatever information is willingly shared, countries will always seek to access more, and through whatever means available.

If the United States is particularly troubled by an act of cyber-espionage by another country, it may still utilize many of the other tools in its possession.

---

[176] *Id.* at 232-34.

[177] Aaron J. Burnstein, *Trade Secrecy as an Instrument of National Security? Rethinking the Foundations of Economic Espionage*, 41 ARIZ. ST. L.J. 933, 986-87 (2009).

[178] *Id.* at 987.

[179] *Id.*

[180] *Id.*

Given the prevalence of espionage in its multitude of forms[181] and the adept nature of counterintelligence services, it is probable that the FBI could make an arrest under preexisting laws, or deport an operative already under surveillance, as retaliation for the cyber activities of the respective country.[182] Alternatively, the United States government could apply diplomatic pressure in a completely unrelated area as "soft retaliation" for the perceived wrongdoing. The United States could also take a more direct approach and publicly out espionage-committing countries like China for their activities, as the Atlantic Council's Jason Healey suggests.[183] These responses assume that the culprit could be readily identified.

2. *Counter-Espionage*

Another option available to the United States, and one it in all likelihood already engages in, is reciprocal espionage.[184] As discussed above, espionage in many respects is the practice of nation states. Under Executive Order 12333, the National Security Agency (NSA) is tasked with the collection of "signals intelligence information and data" and is thus the primary apparatus through which the United States engages in its cyber-espionage.[185] In addition to preexisting activities, the NSA could probe the suspected country's computer systems as a means of responding to the conduct. Yet, depending on the nature of the information accessed, the identity of the suspected country (if the conduct can be attributed to a country), as well as other factors, no response or a very subtle response may be more appropriate than any sort of blatant reaction. The chosen response will likely depend on the message desired to be sent, if any.

D. Assessment of Options

Despite the relative merits and drawbacks of the aforementioned measures,

---

[181] Bill Gertz, *Inside the Ring: Counterspies Hunt Russian Mole Inside National Security Agency*, WASH. TIMES, Dec. 1, 2010, http://commcns.org/LWN5qu.

[182] There is precedent for the latter option, as was seen during Operation Famish, in which the United States rolled up an extensive network of Soviet spies operating in the US under diplomatic cover. Bernard Gwertzman, *U.S. Expels 25 Soviet Diplomats; Denies Link With Daniloff Affair*, N.Y. TIMES, Sept. 18, 1986, at A1.

[183] Philip Ewing, *Has the 'Cyber Pearl Harbor' Already Happened?*, DoD BUZZ (Mar. 26, 2012), http://commcns.org/LauaWn.

[184] A statement by Michael Hayden suggests this is the case. Kim Zetter, *Former NSA Director: Countries Spewing Cyberattacks Should Be Held Responsible*, WIRED (July 29, 2010), http://commcns.org/JNRA5W ("[w]ithout going into great detail, we're actually pretty good at [cyber-espionage], and the Chinese aren't the only ones doing this.").

[185] Exec. Order No. 12,333, 46 Fed. Reg. 59947 (Dec. 4, 1981).

none of them individually or even taken together will prevent cyber-espionage or encourage states to cease carrying it out. Moreover, many of these proposals are in tension with one another. The proposed CEA, were it able to yield some success at stemming espionage, would likely inspire similar laws in other countries and those nations would make best efforts to intercept and prosecute U.S. "cyber spies." In all likelihood, the CEA or a similar piece of legislation would duplicate existing federal law and do little to address persistent cyber-espionage conduct.

An information sharing proposal similar to the one suggested by Burnstein would probably not be accepted. It is in every country's interest to preserve the integrity of information systems and the sensitive data they contain. Despite sharing that countries do for strategic and cooperative purposes, when this is done, it is done voluntarily (and therefore selectively). In the case of actual intelligence data, the information is likely sanitized, to avoid revealing the sources and methods of its collection. This is all the more true in the wake of the Wikileaks-State Department scandal in 2010, in which thousands of sensitive communiqués and documents were placed on the Internet.[186] No matter the value of the norms that may develop in terms of international cooperation or transparency, states will continue to engage in cyber-espionage.

Although an outright information-exchange regime may not be too likely in the near-term, there is cause for hope. The governments of the United States and Russia are making efforts to ensure open channels of communication exist so as to prevent potentially harmful consequences resulting from the misreading of an incident.[187] Such arrangements could allow for states to continue intelligence gathering activities while averting a potentially hostile response.

Reciprocal espionage likely does nothing to stop ongoing espionage committed against the United States. As demonstrated above, one difficulty of cyber-espionage is that it offers all of the benefits of traditional espionage (arguably more so, given the sheer amount of information that can be collected in a relatively short period of time) with few of the consequences attendant with "traditional modes" of intelligence collection. If countries can engage in this type of behavior with impunity, cyber-espionage is unlikely to abate in the future.

---

[186] Kim Zetter, *Former NSA Director: Countries Spewing Cyberattacks Should Be Held Responsible*, WIRED (July 29, 2010), http://commcns.org/JNRA5W.

[187] Nate Anderson, *US and Russia "Reset" Their Cybersecurity Relationship*, ARS TECHNICA (July 13, 2011), http://commcns.org/Kil8pG.

VI. CONCLUSION

One principle that should inform any response in this area is that espionage, cyber or otherwise, serves valuable purposes for nation states.[188] The costs of losing sensitive information or strategic advantages are certainly great, but having access to such information from one's adversaries is crucial to effectively operating in the international community. Because of this value, calls for haphazard action at the international level for "moratoriums" on cyber-espionage should be resisted. Efforts should focus on countermeasures, capabilities, and open lines of communication to thwart potential escalations through misunderstandings.

Cyber-espionage by its nature has fewer safeguards for the surveilled states than traditional forms of espionage. As Lin suggests, this can put states in a tense position when ascertaining the threat and identifying potential responses.[189] If the United States seeks to reduce the pervasiveness of cyber-espionage, it should focus on making its computer networks less attractive a target, thereby forcing its counterparts to engage in alternative collection measures that allow for more effective enforcement.

---

[188] Glenn Sulmasy and John Yoo, *Counterintuitive: Intelligence Operations and International Law*, 28 MICH. J. INT'L L. 625, 634 (2007) (claiming intelligence can "promote the potential for peace and reduce international tension); Scott, *supra* note 56, at 225-26 (claiming intelligence gathering for "self-defense" purposes can help prevent armed attacks).

[189] Lin, *supra* note 14, at 84.