ARTICLE

Rethinking Warfare: The Ambiguity of Cyber Attacks

Antonia Chayes*

Professor of Practice in International Politics and Law at the Fletcher School of Law and Diplomacy, Tufts University. Professor Chayes practiced law and served as mediator in many corporate disputes. She served on the Board of United Technologies Corporation, chaired its Public Issues Review Committee, and served on its Executive Committee. During the Carter Administration, Professor Chayes was Assistant and, later, Under Secretary of the U.S. Air Force, where she was awarded the Distinguished Service Medal. She is the author of a number of books and articles. Her most recent publication is *Chapter VII ½: Is Jus Post Bellum Possible?*, which appeared in the European Journal of International Law in 2013. Before that, her article *How American Treaty Behavior Threatens National Security* appeared in International Security in 2008.

Table of Contents

Introduction

Estonia was a highly-wired society, but its ability to function as such was nearly brought to a halt in less than a month because of three waves of cyber attacks between April 26 and May 18, 2007, likely carried out by Russian agents. These attacks, as well as recent attacks on private non-critical corporations such as Sony Pictures Entertainment, represent another type of grey area between war and peace, raising novel issues about civil-military roles and the inadequacy of the law underpinning this area. Widespread dependence on the Internet, combined with serious hardware and software flaws and overall system, weakness made for a compounded vulnerability of an entire nation.[1] Repeated attacks on banks and other commercial operations in the United States and Europe, and cyber attacks on Iran's nuclear facilities, underscore the blurred line between economic crimes and something closer to outright hostilities.

One of the relatively unsophisticated methods used with success during these attacks, Distributed Denial of Service (DDoS), "overloads a victim's server by exploiting communication protocols,"[2] transmitting a false address to a server, which then overloads the system by trying to respond, crowding out other legitimate requests. "Ping" attacks—or attacks that flooded the system with more information than it could handle—were also launched. The successive waves of attacks crashed Estonia's Internet system, leaving the government—including the president, parliament, police, and military—unable to communicate. The country's entire banking system had to shut down. Computers used in the attack were traced to 178 countries. The scope of global participation was breathtaking at the time.[3]

The effects of the attack on Estonia do not appear to be proportional to their cause, which indicates how easily petty disputes can lead to serious consequences in the cyber age. The Estonian government had removed a Russian, Soviet-era statue of the Bronze Soldier from its central location in Tallinn, and exhumed an adjacent war grave containing

---

[1] Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia,* THE GUARDIAN (May 16, 2007), http://www.theguardian.com/world/2007/may/17/topstories3.russiahttp://www.theguardian.com/world/2007/may/17/topstories3.russia.

[2] Jason Richards, *Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security,* INT'L AFFAIRS REVIEW, Vol. 18, No. 2 (2009), http://www.iar-gwu.org/node/65.

[3] Charles Clover, *Kremlin-Backed Group Behind Estonia Cyber Blitz*, FINANCIAL TIMES (Mar. 11, 2009); http://www.ft.com/intl/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html#axzz3TwGGCf83.

the remains of twelve Soviet soldiers and moved them all to a remote cemetery on the outskirts of the country's capital.[4] Verbal attacks from Russia against the Estonian government followed; the discontent suggested that the source of the cyber attack was from Russia as well. Yet it took longer than the two weeks the attacks lasted to pinpoint their source: most likely, the Russian government-sponsored youth group, Nashe.[5]

The ambiguity of the attack upon Estonia allows the imagination to create further baffling scenarios. Dr. Herbert Lin[6] has posed several; they all implicate temporary, reversible interference with military or critical infrastructure systems or the introduction of a "Trojan Horse" that is capable of exfiltrating classified data and more. But while it is useful to imagine hypotheticals to prepare against attacks, there are now real life examples. Amongst them since the Estonia attack are: Georgia (2008), in which a cyber attack on the government's network preceded a hot war, then continued during the war with Russia;[7] and cyber attacks against computer systems that operated Iran's nuclear enrichment facilities.[8] These

---

[4] Jari Tanner, *Estonia Reburies Soviet Troops' Remains*, WASH. POST (July 3, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/07/03/AR2007070300490.html.

[5] *See* Heather A. Conley & Theodore P. Garber, *Russian Soft Power in the 21st Century: An Examination of Russian Compatriot Policy in Estonia,* CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (Aug. 2011); Robert Coalson, *Behind The Estonia Cyberattacks*, RADIO FREE EUROPE (Mar. 9, 2009), http://www.rferl.org/content/Behind_The_Estonia_Cyberattacks/1505613.html; Charles Clover, *Kremlin-backed Group Behind Estonia Cyber Blitz*, FINANCIAL TIMES (Mar. 11, 2009), http://www.ft.com/intl/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html#axzz2bftgCwBY.

[6] Dr. Herbert Lin was Chief Scientist at the Computer Science and Telecommunications Board, National Research Council of the National Academies of Science; now Dr. Lin serves as a consulting scholar at the Center for International Security and Cooperation at Stanford University.

[7] The 2008 war between Russia and Georgia may represent the first time in history of "a coordinated cyberspace . . . attack synchronized with major combat actions in the other warfighting domains." The cyber attacks on Georgia's military and government networks, including DDoS and website defacements, began three weeks before the physical hostilities and continued throughout the war. Linked to Russia's "patriotic hackers/cyber militias," the attacks were timed with the Russian military's ground, air, and naval combat operations and closely coordinated with the "overall strategic objectives of the Russian government." By disabling Georgia's government and news websites, the attackers sowed panic and confusion among the Georgian civilian population because it was unable to communicate with its government. Cyber warfare also prevented Georgia from sending messages to the outside world, delivering Russia strategic communications victory. David Hollis, *Cyberwar Case Study: Georgia 2008*, SMALL WARS JOURNAL (Jan. 6, 2011), http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

[8] Code-named the "Olympic Games," the attacks were allegedly initiated by the administration of George W. Bush and significantly expanded under President Obama. David Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html; *see also* DAVID SANGER, CONFRONT AND CONCEAL-OBAMA'S SECRET WAR AND THE SURPRISING USE OF AMERICAN POWER 187–

cases illustrate how crippling and warlike this form of attack can be, even absent wounded or dead. Cyber warfare does not necessarily imply kinetic action, and that fact makes civil-military relationships and the legal framework within which responses must be formulated relatively novel and highly complex.

Yet it is only by using an analogy that the case of Estonia can be characterized as a hostile act approaching war, as there was none of the kinetic action usually associated with a conventional war. Yet it was certainly a hostile attack. Cyber attacks, based on revolutionary technological innovation, challenge traditional concepts about war perhaps more than any other type of hostile action. What constitutes an attack? When does an "attack" allow for self-defense? When might an attack be referred to the UN Security Council for response under Chapter VII? What law governs the appropriateness of response? To what extent do political and diplomatic concerns govern—or at least play in the mix? These are the questions now being addressed worldwide.

Cyber attacks and cyber warfare raise issues of self-protection, the ability to fend off (or deny) an attack, attribution about the source of attack, and effectiveness of response. It may be difficult to identify exactly when an "attack" has taken place; who has perpetrated the act; whether more than an internal response to repair and protect is appropriate; and, if so, what response is legal and proportionate. The problem of attribution alone raises novel issues different from those encountered in other grey area conflicts.

Many cyber intrusions are a form of commercial espionage—not an attack that might be a prelude to war. For example, "phishing"—literally requesting information by posing as legitimate organizations[9]—may be a commercial crime, to be dealt with by the domestic criminal justice system, to the extent it has jurisdiction and adequate attribution can be made.[10] Yet economic espionage has been committed by states, and might be a precursor to a system-wide attack to destroy or cripple critical

---

207 (2012); P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 114–20 (2014).

[9] Phishing attacks "use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts." UNITED STATES COMPUTER EMERGENCY READINESS TEAM, *Tips*, http://www.us-cert.gov/ncas/tips/ST04-014.

[10] According to the U.S. National Conference of State Legislatures, twenty-three states currently have laws specifically against phishing. "State Laws Addressing Phishing," National Conference of State Legislatures (last updated Dec. 30, 2013), http://www.ncsl.org/research/telecommunications-and-information-technology/state-phishing-laws.aspx.

infrastructure such as electric, water and transportation systems.[11] In fact, the definition of "critical infrastructure" under the Patriot Act of 2001 is very broad: "the term 'critical infrastructure' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[12]

Nations are acquiring experience and judgment to sort out what kind of response is appropriate to an incident that involves a large-scale, state-sponsored pilfering of data, but no shut-down of a system.[13] The waves of attacks on major U.S. banks, such as on Wells Fargo and JPMorgan Chase, are cases-in-point, with new cases reported weekly.[14]

---

[11] A cyber espionage "toolkit" called Snake, for example, is capable of both collecting information and "manipulating computer networks." David E. Sanger & Steven Erlanger, *Suspicion Falls on Russia as 'Snake' Cyberattacks Target Ukraine's Government*, N.Y. TIMES (Mar. 8, 2014), http://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html?_r=0. In one of the largest intrusions, hackers suspected of having ties with the Russian government infiltrated JPMorgan Chase's computer system in the summer of 2014. The hackers did not demonstrate any profit seeking intentions, but gained "the highest level of administrative privilege to dozens of the bank's computer servers," potentially setting up "vulnerabilities that would allow them re-entry into JPMorgan's systems." Jessica Silver-Greenberg et al., *JPMorgan Chase Hacking Affects 76 Million Households,* N.Y. TIMES (Oct. 2, 2014), http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/.

[12] 42 U.S.C. 5195(e)

[13] One response that has been discussed regarding private sector protection of intellectual property is allowing a private company to respond to a cyber intrusion, or to "hack back." While it is currently illegal under U.S. law, a 2013 report by a private commission addressed the possibility of changing the law to allow companies to respond. Max Fisher, *Should the U.S. Allow Companies to 'Hack Back' Against Foreign Cyber Spies?* WASH. POST (May 23, 2013), http://www.washingtonpost.com/blogs/worldviews/wp/2013/05/23/should-the-u-s-allow-companies-to-hack-back-against-foreign-cyber-spies/.

[14] *See* David Henry and Jim Finkle, *JP Morgan Warns 465,000 Card Users on Data Loss After Cyber Attack*, REUTERS (Dec. 5, 2013), http://www.reuters.com/article/2013/12/05/us-jpmorgan-dataexposed-idUSBRE9B405R20131205; Chris Strohm & Eric Engleman, *Cyber Attacks on U.S. Banks Expose Computer Vulnerability*, BLOOMBERG NEWS (Sept. 28, 2012), http://www.bloomberg.com/news/2012-09-28/cyber-attacks-on-u-s-banks-expose-computer-vulnerability.html; E. Scott Reckard, *Cyber Attacks on Banks Resume, Targeting Chase*, L.A. TIMES (Mar. 13, 2013), http://www.latimes.com/business/money/la-fi-mo-bank-cyber-attacks-chase-20130312,0,1903959.story. In October 2013, Army General Keith Alexander, leading the National Security Agency and the U.S. Cyber Command, noted, "over the last 14 months, we've seen over 350 distributed-denial-of-service attacks on Wall Street, with varying levels of success." Cheryl Pellerin, *Alexander: Defending Against Cyberattacks Requires Collaboration*, AMERICAN FORCES PRESS SERVICE (Oct. 30, 2013), http://www.defense.gov/news/newsarticle.aspx?id=121030.

Factual uncertainty about the origins and nature of a cyber attack almost guarantees legal uncertainty under both international and domestic law. Legal indeterminacy in turn spawns confusion or competition among civilian and military actors to distribute roles and relationships. For example, a phishing attack upon American telecommunications, if attributed to a private party, might be handled by state law enforcement; if attributed to a nation, might be handled by the FBI; if regarded as part of a series of attacks to bring down critical infrastructure, might be handled cooperatively by the Department of Homeland Security, NSA, Cyber Command, and perhaps other agencies. The demands for close cooperation, discussed further along, are unprecedented.

I. Defining "Attack"

With all these unanswered questions, it is not surprising that so much of the recent literature about cyber exploitation or espionage, cyber crimes, cyber attacks, and cyber war has been devoted to the effort to reach acceptable and widely accepted definitions. Most important is to clarify when a cyber attack constitutes a military attack. Defining and distinguishing among these categories theoretically should help elucidate what law, if any, applies and which government officials are expected to act. Definitions should help determine the allocation of responsibility among civil and military officials, and the private sector. But they are only a starting point.

In 2010, the U.S. Joint Chiefs of Staff defined a "cyber attack" as:

> A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber attack are not necessarily limited to the targeted computer systems or data themselves—for instance, attacks on computer systems, which are intended to degrade or destroy infrastructure or C2 capability. A cyber attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber attack may be widely separated temporally and geographically from the delivery.[15]

The definition realistically contemplates a wide temporal distance—lag time—between the action and its impact. But introducing the element of intent, which continues in military doctrinal writing, may

[15] The Vice Chairman of the Joint Chiefs of Staff, Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directorates: Joint Terminology for Cyberspace Operations (2010).

complicate the fact-finding process necessary to determine an appropriate response. A standard of proof of "reasonably expected consequences" might be more objective.

Yale Law Professor Oona Hathaway and her colleagues devised a simpler, broader definition of a "cyber attack." In their 2012 article, they write: "A cyber attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose."[16] The article goes on to say that "any action" includes "hacking, bombing, cutting, inflecting, and so forth," as long as the action has the objective of undermining or disrupting a computer network.[17] The word "purpose" seems to apply to the intent of the attacking party.

While this definition is not in conflict with that of the Joint Chiefs, its breadth and seeming simplicity seem attractive. At least both definitions help separate cyber attacks that harm the state—even through its private infrastructure—from those that are either commercial theft or espionage. But the very notion of "political purpose" in the Hathaway definition might blur the distinction between crime and war when emanating from a non-state group seeking funding or information.[18]

---

[16] Oona Hathaway et al., *The Law of Cyber-Attack*, 100 CALIFORNIA LAW REVIEW 817, 821 (2012).

[17] *Id.* at 822. Presumably this would not include espionage or theft—pulling information from a network without damaging or compromising the network so long as the ultimate objective were not "undermining or disrupting a computer network."

[18] The International Red Cross's definition of cyber warfare is also very broad:

> Cyber operations can be broadly described as operations against or via a computer or a computer system through a data stream. Such operations can aim to do different things, for instance to infiltrate a system and collect, export, destroy, change, or encrypt data or to trigger, alter or otherwise manipulate processes controlled by the infiltrated computer system . . . . It is sometimes claimed that cyber operations do not fall within the definition of "attack" as long as they do not result in physical destruction or when its effects are reversible. If this claim implies that an attack against a civilian object may be considered lawful in such cases, it is unfounded under existing law in the view of the ICRC. Under IHL, attacks may only be directed at military objectives, while objects not falling within that definition are civilian and may not be attacked. The definition of military objectives is not dependent on the method of warfare used and must be applied to both kinetic and non-kinetic means; the fact that a cyber operation does not lead to the destruction of an attacked object is also irrelevant.

Thirty-first International Conference of the Red Cross and Red Crescent, *International Humanitarian Law and the challenges of contemporary armed conflicts,* REPORT BY THE INTERNATIONAL COMMITTEE OF THE RED CROSS (Oct. 2011), http://www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf.

Yet another definition is found in the Tallinn Manual on the International Law Applicable to Cyber Warfare, a document developed at the request of NATO's Cooperative Cyber Defense Centre of Excellence. According to the Manual, "a cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[19] Drawing a parallel to implanting landmines, the authors of the report conclude that a cyber operation can constitute an attack even before the damaging consequences of such an operation become evident, giving the example of implanting malware that will be activated at a later time, but for which the intended consequences meet the requisite threshold of harm' as an event that could be defined as an attack "irrespective of whether [the malware] are activated."[20] In a similar vein, a cyber attack that has been launched but defeated still amounts to an attack. The Manual does warn that great care should be exercised when identifying the perpetrator of the attack.

These definitional iterations help to refine the issues, although they cannot be expected to answer all questions. They do serve to narrow differences in approach somewhat and to help begin to assure that officials are addressing common issues. However, the lack of internationally accepted distinctions among "cyber crime," "cyber attack," and "cyber war" make concerted international action more difficult to achieve. The definitions alone do not delineate civilian and military roles, nor do they designate a legal framework under which to operate, since the issue of whether an attack warrants a military response—even in the military domain—remains ambiguous. Economic attacks may be handled through a variety of international means, judicial and diplomatic. But crippling economic attacks without serious casualties might not be sufficient to warrant acts in self-defense under Article 51 of the UN Charter nor, as in the case of Estonia, a collective response under Article 5 of the North Atlantic Treaty.[21]

---

[19] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 92 (Michael N. Schmitt gen. ed., 2013). NATO's Glossary of Terms and Definitions describes a computer network attack (CNA) as an "action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself." NATO Glossary of Terms and Definitions, http://nsa.nato.int/nsa/zPublic/ap/aap6/AAP-6.pdf.

[20] TALLINN MANUAL, *supra* note 19, at 94.

[21] Article 5 of the North Atlantic (Washington) Treaty states:

> The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary,

II. Framing a Response

Potential American responses to a cyber attack were outlined in the classified Presidential Policy Directive (PPD) 20, signed in October 2012, which was revealed by Edward Snowden's leaks of classified documents.[22] The Directive uses a complex vocabulary to describe attacks and potential responses. It described "the manipulation, disruption, denial, degradation, or destruction of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon," as a "cyber effect" operation. The Directive defined two types of cyber effects operations: Defensive Cyber Effects Operations (DCEO) and Offensive Cyber Effects Operations (OCEO).[23]

Joint Publication 3-12 (R) titled "Cyber Operations", published by DOD in unclassified version in February 2013, attempted to clarify military cyber doctrine for the public, even though it is riddled with abbreviations and acronyms. Cyber operations (CO) are divided into three categories—defensive cyber operations (DCO), DOD information networks operations (DODIN), and offensive cyber operations (OCO). [24]

> including the use of armed force, to restore and maintain the security of the North Atlantic area
>
> Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.

North Atlantic (Washington) Treaty, April 4, 1949. http://www.nato.int/cps/en/natolive/official_texts_17120.htm

[22] PPD-20 further stipulates that both defensive and offensive cyber operation must comply with the United States government's obligations under international law "including with regard to matters of sovereignty and neutrality, and as applicable, the law of armed conflict." The rules expressed in the Directive do not seek to affect cyber collection operations, unless they are likely to result in "significant consequence." White House, Presidential Policy Directive 20 (Oct. 16, 2012), https://epic.org/privacy/cybersecurity/presidential-directives/presidential-policy-directive-20.pdf. *See also* Ellen Nakashima, *Obama signs secret directive to help thwart cyberattacks*, WASH. POST (Nov. 14, 2012), http://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html.

[23] Both forms of operations are "intended to enable or produce cyber effects outside United States Government networks" and exclude network defense (protection of computers, networks, systems, and the infrastructure under their control, without affecting outside networks) and cyber collection (clandestine intelligence gathering). The purpose of DCEOs is to protect "against imminent threats or ongoing attacks or malicious cyber activity against U.S. national interests from inside or outside cyberspace." PPD-20.

[24] Joint Publication 3-12R (unclassified version: Feb. 5, 2013).

Defensive cyber operations or DCO are "intended to defend DOD or other friendly cyberspace." They are described as "passive and active cyberspace defense operations to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems." DCO include "internal defensive measures" taken within DOD information networks operations (DODIN) as well as "DCO Response Actions" taken outside DODIN to neutralize "ongoing or imminent threats to defend DOD cyberspace." The goal of DODIN operations is to maintain and mange "DOD communications systems and networks" to ensure their protection and sustainability.[25]

The U.S. military's interest in offensive cyber capabilities has continued to grow.[26] Military doctrine incorporates offensive operations (OCO) into its repertoire—but the content of and guidance for offensive cyber operations remain classified. The 2015 Cyber Strategy, in less opaque language, made the choices clearer:

> There may be times when the President or the Secretary of Defense may determine that it would be appropriate for the U.S. military to conduct cyber operations to disrupt an adversary's military-related networks or infrastructure so that the U.S. military can protect U.S. interests in an area of operations. For example, the United States military might use cyber operations to terminate an ongoing conflict on U.S. terms, or to disrupt an adversary's military systems to prevent the use of force against U.S. interests. United States Cyber Command (USCYBERCOM) may also be directed to conduct cyber operations, in coordination with other U.S. government agencies as appropriate, to deter or defeat strategic threats in other domains.[27]

But the strategy also emphasized that "[a]ny decision to conduct cyber operations outside of DoD networks is made with the utmost care and deliberation and under strict policy and operational oversight, and in accordance with the law of armed conflict."[28] Many geopolitical and domestic political and economic factors would have to be considered when

---

[25] *Id.*

[26] "U.S. military spending, depending on the measure, is 2.5 to 4 times as much on cyberoffense research and development as cyberdefense research." P.W. Singer & Allan Friedman, *Cult of the Cyber Offensive*, FOREIGN POLICY (Jan. 15, 2014), http://www.foreignpolicy.com/articles/2014/01/15/cult_of_the_cyber_offensive_first_strike_advantage.

[27] U.S. Department of Defense, *Cyber Strategy* (April 2015) http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

[28] *Id.*

calculating and making an effective response. But leaving uncertainty about the nature of a U.S. response is itself useful as a deterrent.

Denial and punishment—another way of characterizing defensive and offensive action—is a familiar analysis, drawn from nuclear deterrence,[29] although that analogy should be approached with caution. Several scholars offer a more comprehensive framework.[30] The approach is triadic: (1) denial, (2) punishment, and (3) international cooperation.

The first leg of the triad is prevention. Essential to preparedness, it is addressed in part by the Joint Staff in its discussion of "DCO." The ability to deny the success of a probable attack is a time-honored deterrent from the dawn of nuclear weapons. Effective prevention against cyber incursions is important in civil domains, and especially in critical infrastructure, but also for all cyber incursions that would seriously disrupt the ability of a nation to function normally. Reducing vulnerability in order to create effective prevention is one form of deterrence and would seem to be the wisest course to follow initially. Hardening systems to make them less vulnerable is optimal. Fast changing technology makes such an approach challenging, although not impossible. Improved defenses and system updates must be constant, so that a high degree of resilience can be achieved. These efforts deter by communicating that an attack will not achieve its objective. But government efforts are complicated by the fact that critical infrastructure is in the hands of private industry which remains in control of its preventive measures.[31] By contrast, nuclear weapons are controlled by the state, which controls their storage, safety from theft, their reliability, and resiliency from attack.

The second leg of a triadic model is the capability to punish, for which credible offensive capability is needed. The concept of "punishment" is part of classical nuclear deterrence, and the same pitfalls of vast expenditures of funds to assure balance with an opponent may

---

[29] *See, e.g.*, BERNARD BRODIE, STRATEGY IN THE MISSILE AGE (1959); THOMAS SCHELLING, ARMS AND INFLUENCE (1966); ALEXANDER GEORGE & RICHARD SMOKE, DETERRENCE IN AMERICAN FOREIGN POLICY: THEORY AND PRACTICE (1974); THOMAS SCHELLING, THE STRATEGY OF CONFLICT (1980); MANAGING NUCLEAR OPERATIONS, ASHTON B. CARTER, JOHN D. STEINBRUNER, AND CHARLES A. ZRAKET, EDS., 1987); KEITH PAYNE, THE GREAT AMERICAN GAMBLE: DETERRENCE THEORY AND PRACTICE FROM THE COLD WAR TO THE TWENTY-FIRST CENTURY (2008).

[30] Christopher Wrenn, "Strategic Cyber Deterrence" doctoral dissertation at the Fletcher School (July 2012), book forthcoming from Georgetown University Press (2015); Herbert Lin, *A virtual necessity: Some modest steps toward greater cybersecurity*, 68(5) BULLETIN OF THE ATOMIC SCIENTISTS 75–87 (2012).

[31] The possibility of removing some functions to local or meshed systems is now under experiment. The creation of closed systems has also been raised, but has gained no traction thus far. Carlotta Gall & James Glanz, *U.S. Promotes Network to Foil Digital Spying,* N.Y. TIMES (Apr. 20, 2014), http://www.nytimes.com/2014/04/21/us/us-promotes-network-to-foil-digital-spying.html?ref=us.

come into play with offensive cyber capability as it has with nuclear prowess. The consequences of punishment by the use of offensive cyber operations are not so disastrous as the use of nuclear weapons, and thus punishment is a more realistic response to attack to contemplate—but the deterrent effect might be weaker. Punishment in cyber warfare would not necessarily involve military measures, which raise legal issues under the UN Charter and issues of proportionality under the law of armed conflict. Response to attack might involve trying to develop regional or fully international sanctions if the facts warranted it and a coalition could be mounted. Alternatively, it might involve treating the cyber exploitation as a criminal offense, and pursuing law-enforcement responses under the Budapest Convention which provides measures to strengthen interstate cooperation in pursuit of cyber crimes.[32]

On the other hand, if the controls of a nuclear plant were undermined so that radiation killed people for miles around, that would certainly be the equivalent of an armed attack, and military measures might well be taken, if attribution were assured. But there are less immediate forms of lethal attack. If critical infrastructure systems were destroyed or crippled, death and illness might result—quickly or slowly. A full-scale attack on critical infrastructure theoretically could prove as much a military attack with kinetic effects over time as bombing raids on industrial production in traditional wars. It is not a stretch to treat a situation in which people are wounded or die as a consequence of a cyber attack as worthy of military response.[33] Although thus far hostile cyber events have not risen to the level of killing people, it is plausible that a cyber attack might do so. But attribution is always essential to response. A false accusation could trigger a diplomatic crisis, and one would hope no cautious leader would take retaliatory action taken without firm knowledge of the source of an attack.

The third and perhaps most promising element of the triadic construct is international cooperation, discussed at greater length in the final section of this Article. The scope of attacks already crosses many state boundaries and international cooperation is likely to be needed for a response to a cyber attack, as the Estonia case revealed. Post hoc cooperation was effective there, even though the restorative efforts were not only post hoc but also very much ad hoc. Experts from Finland, Slovenia, and Germany happened to be in Estonia and joined the effort to

---

[32] *See* Convention on Cybercrime, arts 16, 17 (storage and preservations of data including traffic data); 18, 19 (production of data); 23, 25 (international cooperation); 24 (providing for extradition). Council of Europe, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[33] Hon. Harold Koh, Remarks at the U.S. Cyber Command Inter-Agency Legal Conference (Sept. 18, 2012), http://www.state.gov/s/l/releases/remarks/197924.htm; Michael Schmitt, International Law in Cyberspace: *The Koh Speech and Tallinn Manual Juxtaposed*, 54 HARV. INT'L L.J. 13, 13 (2012).

undo the damage in a dramatic all-night session, countering the flaws that had left the Estonian system so vulnerable.[34] Of course, advance collaborative planning for a cooperative response is far preferable to reliance on post hoc efforts: NATO and the EU have moved in that direction. Yet further moves toward international agreements that restrain aggressive cyber action will likely be far in the future, given states' reluctance to relinquish potential weapons in the face of a threatening security climate.[35]

III. Implications for Civil-Military Relations

Both civilian and military actors are needed to prevent and respond to cyber exploitation and cyber attacks. Unlike other grey areas, any effort to respond involves cooperation of the private sector, since 85-90% of the critical infrastructure, by any definition, is privately owned and operated. Critical infrastructure is known to be vulnerable, including the electric grid, utilities—especially those fueled by nuclear energy—transportation, and all forms of communication.[36] Public reports indicate that most cyber intrusions and putative attacks have been against privately held critical infrastructure, both in America and Europe.[37]

Three distinct types of novel problems emerge from the demands that will be placed on civil-military relationship in the event of cyber attack. The first is this fact of private ownership of most critical infrastructure. The need to secure cooperation between government and the private sector on this presents serious obstacles. In the United States, efforts to legislate standards for the private sector, discussed in the next section, have been thwarted.[38] However the issues are not simply industrial

---

[34] Wrenn, *supra* note 30, at 220–21.

[35] The United States has still not acceded to the Biological Weapons Convention, for example; nor is there much movement towards a Comprehensive Test Ban Treaty. A Fissile Material Cut-Off Treaty has not been accomplished since first proposed in 1993. G.A. Res. 48/75L. http://www.nti.org/treaties-and-regimes/proposed-fissile-material-cut-off-reaty/.

[36] In the United States, the private sector "owns and operates approximately 85% of the nation's critical infrastructure." *Critical Infrastructure Sector Partnerships*, Department of Homeland Security, https://www.dhs.goR/critical-infrastructure-sector-partnerships. Likewise, in Europe, "approximately 85% [of the critical infrastructure] are owned by the private sector." Bernard Haemmerli & Andrea Renda, "Protecting Critical Infrastructure in the EU," Regulatory Policy, CEPS Task Force Reports (Dec. 16, 2010), http://www.ceps.be/book/protecting-critical-infrastructure-eu.

[37] According to Verizon's Data Breach Investigations Report, there were 548 cyber espionage incidents in 2014: "two thirds of the incidents in this pattern had no attacker attribution information whatsoever." Verizon, Wireless Data Breach Investigations Report (2015) 52, http://www.verizonenterprise.com/DBIR/2015.

[38] *Banks Say Efforts to Bolster U.S. Cyber Defenses Should Complement Industry Practices,* AMERICAN BANKER (Apr. 12, 2013), http://www.americanbanker.com/issues/178_70/banks-say-efforts-to-bolster-u-s-cyber-defenses-should-complement-industry-1058220-1.html

reluctance to cooperate with all of government: fear of antitrust prosecution also plays a role. Moreover, resistance to NSA overreach in monitoring telecommunications and the Internet have helped create deep concerns about government regulation within the private sector and civil liberties groups alike.[39] The same issue arises in Europe, where cooperation across state lines is even more important, given the interdependence of much of its critical infrastructure. Lack of resilience in one nation's infrastructure immediately affects its neighbors: a failure of the electric grid in Germany triggered power outages in France, Italy, and parts of Spain.[40]

The second problem is the joinder of the intelligence and military domains, and the potential intertwining of operations. U.S. Cyber Command is co-located with the National Security Agency, and headed by the same person. This has led to questions about oversight and control of both intelligence activities and military responses.[41] In cyber war, as in targeted killing, intelligence services may be performing essentially military operations. The President's Independent Review Group recommended separating the agencies and their leaderships, with the NSA clearly designated as a foreign intelligence agency, but as of this writing, leadership is still shared.[42] U.S. Cyber Command reports through Strategic Command to the Secretary of Defense. NSA, a critical (and much criticized) part of America's intelligence network, reports both to the Secretary of Defense and to the Director of National Intelligence.[43]

The third problem is to secure effective and timely collaboration of the essential civil departments and levels of government below the federal level in the United States. In the event of a crippling attack, an effective response will require all levels of government and industry to function together smoothly and with unprecedented speed. In both the United States

---

[39] Privacy and Civil Liberties Oversight Board, *Report of the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014), http://www.pclob.gov/library.html; *see also* Ellen Nakashima, *NSA Thwarted in Cybersecurity Initiative*, WASH. POST (Feb. 28, 2012), http://www.washingtonpost.com/national/major-internet-service-providers-cooperating-with-nsa-on-monitoring-traffic/2011/06/07/AG2dukXH_story.html.

[40] Haemmerli & Renda, *supra* note 36, at 3.

[41] Richard A. Clarke et al., *The NSA Report: Liberty and Security in a Changing World, The President's Review Group on Intelligence and Communications Technologies,* Dec. 12, 2013, http://press.princeton.edu/titles/10296.html.

[42] Ellen Nakashima, *White House to preserve controversial policy on NSA, Cyber Command leadership*, WASH. POST (Dec 13, 2013), http://www.washingtonpost.com/world/national-security/white-house-to-preserve-controversial-policy-on-nsa-cyber-command-leadership/2013/12/13/4bb56a48-6403-11e3-a373-0f9f2d1c2b61_story.html.

[43] National Security Agency, "Frequently Asked Questions: Oversight," https://www.nsa.gov/about/faqs/oversight.shtml#oversight1.

and Europe, many departments and agencies have only partial responsibility.

Efforts are underway in the U.S. government to develop effective collaboration and to deal with the three types of civil-military problems outlined here. Presidential Policy Directive (PPD) 21 of February 2013[44] (together with Executive Order 13636[45]) requires "a national unity of effort pursuant to strategic guidance from the Secretary of Homeland Security."[46] A documentary review indicates government awareness of the complexity of coordinating the many relevant agencies and departments sprawled over the federal system. As indication of the difficulties, the President created a Cyber Threat Intelligence Integration Center under the auspices of the Director of National Intelligence to connect and coordinate the intelligence gathered by other agencies, rather than to engage in programmatic efforts.[47] But whether such coordination will work in a cyber crisis remains to be proven.

IV. The Wide Array of Civil and Military Actors

PPD-21 allocated important cyber responsibilities to many departments and agencies.[48] The State Department is given the lead in securing foreign cooperation and in negotiating formal or informal international agreements.[49] The Department of Justice is given responsibility for counterterrorism investigation and law enforcement activities pertaining to infrastructure, although its investigatory relationship to the intelligence community is unclear in PPD-21.[50] The

---

[44] White House, Presidential Policy Directive - Critical Infrastructure Security and Resilience [hereinafter "PPD-21"] (Feb. 12, 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[45] Exec. Order No. 13636, 78 C.F.R. §11739 (2013).

[46] According to PPD-21, the primary responsibility for the security of the Nation's critical infrastructure belongs to the Secretary of Homeland Security, who is appointed to "provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure." Various sectors of critical infrastructure benefit from the expertise of the sector-specific agencies, which among other duties "provide, support, or facilitate technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents." PPD-21, *supra* note 44.

[47] Memorandum from President Obama on Establishment of the Cyber Threat Intelligence Integration Center (Feb. 25, 2015) https://www.whitehouse.gov/the-press-office/2015/02/25/presidential-memorandum-establishment-cyber-threat-intelligence-integrat.

[48] PPD-21, *supra* note 44.

[49] The State Department has created the Office of the Coordinator for Cyber Issues to encourage "global diplomatic engagement." Department of State, *Cyber Issues*, http://www.state.gov/s/cyberissues/.

[50] *Id.*; *see also* U.S. Department of Justice, *Overview*, http://www.justice.gov/sites/default/files/jmd/legacy/2014/08/25/fy13-bud-summary-request-performance.pdf; PPD-21, *supra* note 44.

Department of Treasury is also essential both for the banking area and in imposing financial sanctions on any offending state.[51] Other agencies, such as the departments of Commerce and Interior, also have designated roles, as does the Nuclear Regulatory Commission.[52] The intelligence community, whose cyber operations unclassified budget in 2013 totaled 1.02 billion dollars,[53] has a major role, especially in determining the origin of an attack.

Wide Array of Government Actors

Civil	*Military*
President (Nat'l Command Authority)	Secretary of Defense
Homeland Security	Combatant Commands (including CYBERCOMM)
State	Armed Forces
Treasury	Reserves and Nat'l Guard
Interior	Coast Guard
Intelligence Community (NSA, CIA)	
Justice (including FBI)	
Commerce	
Nuclear Regulatory Commission	
States and Cities	

To this wide array of governmental actors, many other civil actors would be affected by a cyber attack, and many would have to be involved in reconstitution efforts, just as they should be involved in preventive efforts: providers of internet technology (IT) products and services, internet service providers (ISP), security services, and IT-dependent providers of goods and services, to name a few.[54] In addition to the many layers of collaboration within the United States, international cooperation will certainly be required to prevent attacks and to repair damage.

---

[51] The Department of Treasury:

> works with other Federal agencies, including the intelligence community and DHS, to assess physical and cyber threats that are identified as specifically directed at the sector or at an asset on a national, regional, or local level. Relationships with DHS, the intelligence community, and other [sector-specific agencies] provide real-time information regarding these threats. Additionally, when threats are identified, frequent communications between the FBIIC and the private sector facilitate efficient and effective transfer of potential threat information, permitting the sector to mitigate the associated vulnerabilities.

Department of Homeland Security, *Banking and Finance Sector: Specific Plan An Annex to the National Infrastructure Protection Plan* (2010).

[52] PPD-21, *supra* note 44.

[53] Barton Gellman & Ellen Nakashima, *U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents Show*, WASH. POST (Aug. 30, 2013), http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html?hpid=z3.

[54] Thanks to Dr. Herbert Lin for these additions.

The Department of Homeland Security (DHS) is responsible for coordinating all government efforts in protecting infrastructure and coordinating efforts with state and local government organizations. It has primary responsibility for securing cooperation with the private industry that controls critical infrastructure.[55] However, without the legislative authority to require compliance, DHS can only "jawbone"—urge cooperation, assist, and advise. Moreover, increasing foreign private ownership of American infrastructure further complicates efforts at government-business collaboration.[56]

The effort made by PPD-21 and Executive Order 13636 to create a "whole of government" approach did not provide a blueprint for the complex collaboration required, leaving it to the Department of Homeland Security to develop a model, and to evaluate its progress.[57] DHS has been implementing its mandate, starting with an Integrated Task Force, to coordinate the disparate elements within it, and to involve other departments, and state and local governments.[58] Numerous studies and recommendations have been made. It is a work in progress of ongoing bureaucratic and organizational efforts, which may change over time with experience and different personnel.[59]

---

[55] PPD-21, *supra* note 44.

[56] Committee on Foreign Investment in the United States, *Annual Report to Congress*, Dec. 2013, http://www.treasury.gov/resource-center/international/foreign-investment/Documents/2012 CFIUS Annual Report PUBLIC.pdf.; William R. Vigdor & Adrianne L. Goins, *Trends in U.S. National Security Review: A More Active CFIUS*, VINSON & ELKINS LLC, Mar. 2011; James A. Lewis, *New Objectives for CFIUS: Foreign Ownership, Critical Infrastructure, and Communications Interception*, 57 FED. COMM. L. J. 457 (2005).

[57] PPD-21 directs the Secretary of Homeland Security to lead the effort of developing the "Critical Infrastructure Security and Resilience Functional Relationships" and to evaluate the public-private model. Presidential Policy Directive 21, *supra* note 42; *see also* Exec. Order 13636, *supra* note 45.

[58] *Hearing Before the S. Comm. on Cybersecurity, Infrastructure, Infrastructure Protection and Security Technologies,* 113th Cong. (2013) (statement of Robert Kolasky, Director, Integrated Task Force, United States Department of Homeland Security). http://docs.house.gov/meetings/HM/HM08/20130718/101151/HHRG-113-HM08-Wstate-KolaskyR-20130718.pdf; *see also Integrated Task Force*, Department of Homeland Security Website, http://www.dhs.gov/sites/default/files/publications/EO-PPD%20Fact%20Sheet%2018March13.pdf.

[59] Incentives Study Analytic Report, *Executive Order 13636: Improving Critical Infrastructure Cybersecurity,* Department of Homeland Security Integrated Task Force (June 12, 2013), http://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf; *see also* Michael Daniel, *Incentives to Support Adoption of the Cybersecurity Framework*, The White House (Aug. 6, 2013), http://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.

Implementation of PPD-21 and Executive Order 13636 has been underway, but its effectiveness has yet to be tested.[60] Sequestration, stringent budgets, and staff turnover have strained the capability of DHS.[61] According to the Center for Strategic and International Studies, for FY 2015, the Department of Homeland Security requested 1.25 billion dollars for "cybersecurity activities, an increase from the $792 million enacted in the 2014 Consolidated Appropriations Act." By contrast, "the Department of Defense (DoD) request includes $5.1 billion, or about four times the DHS request, to support cyber operations."[62] In the event of an attack on critical infrastructure, it seems likely that DoD's capacity will lead to its predominant role in managing the problems.

Early reports on implementation of PPD-21 and Executive Order 13636 by the report of the DHS National Infrastructure Advisory Council (NIAC)[63]—composed primarily of business and outside counsel—

---

[60] *See* Global Institute for Cyber Security and Research - Global Situation Awareness Center, *National-Critical-Infrastructure-Resilience Analysis Report,* http://www.nhisac.org/wp-content/uploads/NH-ISAC-Advisory-Report-201.13_National-Critical-Infrastructure-Resilience.pdf.

[61] Jerry Markon et al., *Top-level Turnover Makes it Harder for DHS to Stay On Top of Evolving Threats*, WASH. POST (Sept. 21, 2014), http://www.washingtonpost.com/politics/top-level-turnover-makes-it-harder-for-dhs-to-stay-on-top-of-evolving-threats/2014/09/21/ca7919a6-39d7-11e4-9c9f-ebb47272e40e_story.html.

[62] Stephanie Sanok Kostro & Garrett Riba, *Major Takeaways from the President's FY 2014 Budget Request for DHS*, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (Mar. 13, 2014), http://csis.org/publication/major-takeaways-presidents-fy-2015-budget-request-dhs. Peter Singer, in a public lecture at the Fletcher School, stated that the budget of the Department of Defense and the NSA combined, not counting the classified budget, was twelve times that of the Department of Homeland Security. In 2014, the Cyber Command budget doubled to $447 million. Brian Fung, *Cyber Command's exploding budget, in 1 chart,* WASH. POST (Jan. 15, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/15/cyber-commands-exploding-budget-in-1-chart/. The suggested 2015 Defense budget allocates $5.1 Billion to cyber. Department of Defense, *DoD Releases Fiscal 2015 Budget Proposal and 2014 QDR*," (Mar. 4, 2014), http://www.defense.gov/releases/release.aspx?releaseid=16567. According to U.S. Chief Information Officer Steven VanRoekel, "the 2014 President's Budget devotes over $13B to cyber- related programs and activities." White House, "Federal Information Technology FY 2014 Budget Priorities." https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/2014_budget_priorities_20130410.pdf. The Department of Homeland Security FY 2015 budget request includes $1.25 billion for Safeguarding and Securing Cyberspace. U.S. Department of Homeland Security, *Budget-in-Brief Fiscal Year 2015*, http://www.dhs.gov/publication/fy-2015-budget-brief. The Department of Justice FY 2015 budget "provides a total of $722 million" for cyber security. U.S. Department of Justice, *FY 2015 Budget Summary*, http://www.justice.gov/jmd/2015summary/pdf/fy15-bud-sum.pdf#p4.

[63] *See* DEPARTMENT OF HOMELAND SECURITY, NATIONAL INFRASTRUCTURE ADVISORY COUNCIL (NIAC) FINAL REPORT AND RECOMMENDATIONS (2013), http://www.dhs.gov/publication/national-infrastructure-advisory-council-strengthening-regional-resilience.

suggested the need to set priorities and provide milestones for measuring outcomes. It criticized redundancy and over-classification.[64] The report also reiterated the search for a "safe harbor" against antitrust violations, adding a request for limiting liability in case of a cyber event. It discussed the need for training funds for smaller business entities to respond to cyber exploitation. Although couched in a bland vocabulary, the report suggests to the reader that the desired collaboration between government and business was far from achieved. Greater federal-state cooperation was called for in the sixteen "lifeline" areas identified as critical infrastructure, as different geographic areas had different priorities. The report emphasized the general need for modernization and the lack of capital investment made, suggesting vulnerability not only to cyber attacks but to major weather events. Over time, advisers and researchers may be more satisfied with the complex structure that is constantly being adjusted under a snowstorm of memoranda, department directives, and organizational changes, but lack of investment is a persistent theme.

A. How Good are the Precedents for Collaboration?

A look at the history of inter-agency and intergovernmental cooperation during a crisis is not very encouraging. To illustrate, consider the impossibly slow, clumsy governmental response to Hurricane Katrina in 2005 and the complex interagency, intergovernmental, private sector management issues following the Deepwater Horizon oil spill of 2010. Hurricane Katrina was one of the most tragic environmental disasters the United States has ever suffered. Predictable and predicted, the break in the levies that flooded parts of New Orleans killed between 1,500 and 1,800 people and caused many more thousands of displaced persons and 100 billion dollars in damage.[65] Despite a new National Incident Management System, the worst-hit states, Louisiana, Mississippi, and Alabama, were unused to collaboration, as was the Federal Emergency Management Agency (FEMA) and the Coast Guard—despite their co-location within the Department of Homeland Security. The National Guard of three states also attempted to help, but the lack of unified command precluded timely and useful cooperation.[66] The human disasters mounted while the government agencies floundered.

---

[64] *Id.*

[65] Lise Olson, *Five Years After Katrina, Storm's, Death Toll Remains a Mystery*, HOUSTON CHRONICLE (Aug. 30, 2010), http://www.chron.com/news/nation-world/article/5-years-after-Katrina-storm-s-death-toll-remains-1589464.php; Eric Iverson, *Networked Resilience: Achieving Inter-organizational and Intergovernmental Collaboration*, Fletcher School Doctoral Dissertation (Jan. 6, 2013).

[66] *Id.*; DEPARTMENT OF HOMELAND SECURITY, OFFICE OF INSPECTOR GENERAL, A PERFORMANCE REVIEW OF FEMA'S DISASTER MANAGEMENT ACTIVITIES IN RESPONSE TO HURRICANE KATRINA (2006), http://www.oig.dhs.gov/assets/Mgmt/OIG_06-32_Mar06.pdf.

By April 2010, when the Deepwater Horizon explosions and oil spill occurred, there was improvement in coordination, at least in the U.S. Coast Guard's ability to respond to the largest marine spill in the history of the petroleum industry—nearly five million barrels spread across the waters of many states.[67] Many of the same problems of interagency and intergovernmental collaboration had to be faced as after the Katrina landfall. Although the circumstances were different, and the toll in human lives vastly lower, five years' practice with the National Response System[68] did somewhat improve collaborative efforts.

However, another important difference was a twenty-year experience with federal legislation. The Oil Pollution Act of 1990 (OPA90)—created after the Exxon Valdez spill—firmly established that the federal government had supreme authority over oil spills (primarily delegated to the Coast Guard), and provided severe penalties for failure to meet prescribed standards.[69] Although commentators disagree about the effectiveness of the law's implementation, it does appear that oil spills were reduced after its passage, and that potential punishment helped create a somewhat higher standard of care.[70] Although there was an improvement in performance over the period between the two crises, both examples suggest the complexity of developing collaboration when responsibilities must be divided among so many agencies and levels of government.

Disputes and mistakes may be inevitable. In 2010, U.S. Central Command dismantled an online forum created by the CIA and the Saudi government as part of an intelligence-gathering effort to identify dangerous terrorists because they had concluded that extremists' use of the site constituted a threat to the United States. The journalist Ellen Nakashima quoted a former national security official: "The point of the story is it hasn't been sorted out yet in a way that all the persons involved in cyber-operations have a clear understanding of doctrine, legal authorities and policy, and a clear understanding of the distinction between what is considered intelligence activity and wartime [Defense Department]

---

[67] NATIONAL OCEANIC AND ATMOSPHERIC ASSOCIATION, *B.P. Oil Spill,* http://www.gulfspillrestoration.noaa.gov/oil-spill/, (last visited April 1, 2015).

[68] The National Response System is the federal mechanism developed to prepare for and respond to environmental disasters. It is designed to coordinate the resources of federal, state, and local authorities and to organize an efficient and effective response to such a disaster, i.e. to seek improvement over past responses.

[69] ENVIRONMENTAL PROTECTION AGENCY, SUMMARY OF KEY PROVISIONS OF THE OIL POLLUTION ACT OF 1990, PUB. L. NO. 101-380, 104 STAT. 484 (1990), http://www.epa.gov/oecaagct/lopa.html.

[70] Jeffrey D. Morgan, *The Oil Pollution Act of 1990: A Look at its Impact on the Oil Industry*, 6 FORDHAM ENV. L. REV. 1, 10–12 (1994).

authority,"[71] Such inter-agency conflicts need sorting out before, not after, attack.

Other examples cast doubt on achieving a smooth "whole of government" response. Hurricane Sandy in 2012 left many residents homeless for a long time, with some plaudits and many complaints about the responses.[72] And the inconsistent federal-state and civil-military responses to the travelers from Liberia, Guinea, and Sierra Leone who might be carrying the Ebola virus in October 2014 also serve as a warning about the difficulties of collaboration.[73]

Many obstacles remain before an effective response to a cyber attack against public or private assets can be assured. First, one can only speculate as to how long—if ever—it will take to assess whether the intrusion is more likely to be espionage (commercial or political)—or a precursor to attack against the state. Problems with attribution will continue to complicate response potential. Pinpointing Chinese intrusions into U.S. infrastructure to a physical location and specific officials in the Chinese military in Shanghai is encouraging in that sources of intrusion may not be permanently elusive.[74] Even when attribution is certain, the United States wisely has not yet treated intrusions into critical infrastructure as a prelude to a system shutdown. Although it is conceivable that significant tensions might alter the diplomatic calculus, at least there should be reliable, tested interagency and intergovernmental mechanisms that would allow for rapid reconstitution.

The assessment process itself requires a system of collaboration to avoid agencies tripping over each other, waiting for another to make an assessment, or performing the task separately and competitively. The issues of resources, experience, and capability apply even more strongly to

---

[71] Ellen Nakashima, *Dismantling of Saudi-CIA Web site illustrates need for clearer cyberwar policies*, WASH. POST (Mar. 19, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/03/18/AR2010031805464.html.

[72] Tim Starks, *Katrina's Lessons Seen In Response to Sandy*, CONG. QUARTERLY (Dec. 29, 2012), http://public.cq.com/docs/weeklyreport/weeklyreport-000004197197.html.

[73] *See* Jon Swaine & Dan Roberts, *New Federal Ebola Guidelines Issued in US After Criticism from UN*, THE GUARDIAN (Oct. 27, 2014), http://www.theguardian.com/world/2014/oct/27/ban-ki-moon-concerned-ebola-restrictions; Ellen Wulfhorst & David Morgan, *U.S. CDC Says Returning Ebola Medical Workers Should Not be Quarantined*, REUTERS (Oct. 27, 2014), http://www.reuters.com/article/2014/10/27/us-health-ebola-usa-newyork-idUSKBN0IG12920141027; Abby Phillip, *Why Hasn't the U.S. Closed Its Airports to Travelers from Ebola-ravaged Countries*, WASH. POST (Oct. 4, 2014), http://www.washingtonpost.com/news/to-your-health/wp/2014/10/01/why-hasnt-the-u-s-closed-its-airports-to-travelers-from-ebola-ravaged-countries/.

[74] *Hello, Unit 61398*, THE ECONOMIST (Feb. 2013), http://www.economist.com/blogs/analects/2013/02/chinese-cyber-attacks.

attribution, and thus it is likely that Cyber Command and NSA would take the lead. [75]

Second, once there is adequate certainty about attribution—and that might take months, not days—a course of action must be determined. Since a decision to act or refrain from acting is highly political, a collaborative recommendation to the President would presumably be made about the choices available for action. This is a cumbersome process requiring inputs from all relevant agencies to offer viable options. The process changes as administrations change, but it has involved options developed for the Deputies' Committee, then rehashed and refined in the Principals' Committee, and finally honed for NSC with the President.[76] Hopefully, a process would be accelerated in an emergency. But a further element—collaboration with allies for attribution, response, and repair—will also take time and effort.

In a 2012 article, Professor Mary Ellen O'Connell notes her concern about over-militarization of cyber issues that could well be handled by civilian authorities, with a different formulation of the problem—relying on economic regulation. She argues that instead of drawing upon analogies from nuclear deterrence, the government should rely on international legal norms of non-intervention and countermeasures. She suggests the danger from cyber attacks be treated much as chemical weapons were handled—by an international agreement that reduces stockpiles and gradually eliminates the threat of chemical warfare by international regulation of universal proportions, or by actions against piracy.[77] She argues:

> In the USA and other States where the thinking is in conventional military terms respecting responses to cyber problems, the advocates of such thinking appear to be trapped by an ideology of militarism. The vast majority of cyber security incidents are carried out not by government-sponsored hackers causing deaths and brick and mortar destruction. The major challenge to Internet security is by

---

[75] *Liberty and Security In a Changing World*, *supra* note 41; *see also* Ellen Nakashima, *White House to preserve controversial policy on NSA*, *Cyber Command leadership*, WASH. POST (Dec. 13, 2013), http://www.washingtonpost.com/world/national-security/white-house-to-preserve-controversial-policy-on-nsa-cyber-command-leadership/2013/12/13/4bb56a48-6403-11e3-a373-0f9f2d1c2b61_story.html.

[76] "An NSC Deputies Committee (NSC/DC) shall serve as the senior sub-Cabinet interagency forum for consideration of policy issues affecting national security." The Principals' Committee involves the Cabinet members: agency heads. WHITE HOUSE, PRESIDENTIAL DECISION DIRECTIVE PDD 2 (1993), http://fas.org/irp/offdocs/pdd/.

[77] Mary Ellen O'Connell, *Cyber Security without Cyber War*, 2 J. OF CONFLICT & SECURITY L. 187, 190 (2012), http://jcsl.oxfordjournals.org/content/17/2/187.full.pdf?ijkey=T6J6KDRCRcHM4Ao&keytype=ref%2520.

> private criminals interested in private gain. International law supports cyber security that is achieved through law enforcement cooperation, supported by shared legal norms governing the use of the Internet.[78]

Professor O'Connell's worry about over-militarization is one that deserves consideration, given budgetary disparities between DoD and other government agencies, especially the combination of Cyber Command with NSA. The President's initial decision to continue joint control perpetuates the imbalance with DHS, but even if those agencies were separated, the budgetary imbalance would exist.[79]

A move toward broad regulation of cyber exploitation that includes military and non-military offenses is an important ultimate approach. But Professor O'Connell's suggested analogy to piracy does not take account of the difficulties of securing deep regulatory regimes. The Convention for the Suppression of Unlawful Acts Against Safety of Maritime Navigation (SUA) came into force in a somewhat more treaty-friendly era,[80] but today, the SUA Protocol of 2005 which bans transport of such dangerous materials as nuclear, chemical, and biological precursors to weapons lacks signatories from critical nations such as the United States, China, and Russia.[81] The Chemical Weapons Convention, which came into force in 1997, created a robust international organization, the Organization for the Prohibition of Chemical Weapons (OPCW), which is the instrument of intrusive verification. As discussed below, many steps will have to precede deep regulation, even if that could ultimately be accomplished. Meanwhile, security problems need to be addressed effectively, with attacks on critical infrastructure numbering in the hundreds in 2013 and growing.[82]

B. Simulations and Exercises

In the absence of international regulation, and even should it be developed, nations will still be responsible for internal agency collaboration to deal with a disastrous cyber event. Without many

---

[78] *Id*. at 191.
[79] *Liberty and Security In a Changing World*, *supra* note 41.
[80] SUA came into force in 1988.
[81] International Maritime Organization, Protocol of 2005 to the Convention for Suppression of Unlawful Acts Against the Safety of Maritime Navigation (2005), https://imo.amsa.gov.au/public/parties/sua05prot.html.
[82] According to the Department of Homeland Security's industrial control systems cyber emergency response team (ICS-CERT) annual report, in the fiscal year 2013, 257 incidents were reported to ICS-CERT. This is an increase from both fiscal years 2012, with 197 incidents reported, and 2011, with 140 incidents reported. The largest percentage of sector specific incidents was in the energy sector at 56%. DEPARTMENT OF HOMELAND SECURITY, ICS-CERT YEAR IN REVIEW (2013), http://ics-cert.us-cert.gov/sites/default/files/documents/Year_In_Review_FY2013_Final.pdf.

rehearsals and clear delineation of roles, critical departments are unlikely to collaborate effectively with instant and effective communication in a crisis. The existence of a government-wide alert or management system, Hurricane Katrina demonstrated, is not sufficient without experience using it.[83] Effective collaboration has to be planned for, and exercised, especially where the private sector is not compelled by legislation to cooperate.

Some issues may arise in exercises, and their identification and careful joint planning for correction is necessary. Constant and penetrating exercises are needed that test suspected weakness in inter-agency, intergovernmental, and public-private cooperation. Exercises have been conducted to test the effectiveness of the National Cyber Incident Response Plan (NCIRP), whose purpose is to provide "a blueprint for cybersecurity incident response."[84] The National Cyber Security Division (NCSD), an arm of the Department of Homeland Security, has conducted a number of simulations in recent years.[85] One exercise was an attempt by the Obama Administration to demonstrate to Senators the vulnerability of the Nation's critical infrastructure and to persuade them to pass the CyberSecurity Act of 2012 that set performance standards for the industry. The Senators were shown how an attack on the electrical grid could be

---

[83] Eric Iverson, NETWORKED RESILIENCE: ACHIEVING INTER-ORGANIZATIONAL AND INTERGOVERNMENTAL COLLABORATION, Fletcher School Doctoral Dissertation (Jan. 6, 2013).

[84] DEPARTMENT OF HOMELAND SECURITY, CYBER STORM: SECURING CYBER SPACE (June 24, 2014), http://www.dhs.gov/cyber-storm-securing-cyber-space.

[85] In 2006, the DHS initiated a series of biennial exercises, aptly-named "Cyber Storm," to test and monitor public and private sector preparedness in the event of a cyber attack. The fourth installment concluded in 2012, with the final report unavailable at the time writing. *See also id.* Attack exercises include the 2012 National Level Exercise (NLE) that simulated a cyber attack on critical infrastructure systems that had a physical impact. As part of the exercise, President Obama held a Cabinet meeting "with his leadership team the time-sensitive decisions that would have to be made if a significant cyber event affected critical infrastructure systems." *See* WHITE HOUSE, STATEMENT BY THE PRESS SECRETARY ON THE 2012 NATIONAL LEVEL EXERCISE, (June 5, 2012), http://www.whitehouse.gov/the-press-office/2012/06/05/statement-press-secretary-2012-national-level-exercise. Additionally, the National Cyber Security Division (NCSD), an agency of the Department of Homeland Security, plans and conducts cyber exercises to protect the critical infrastructure on state, federal, regional, and international levels. These exercises typically involve a number of different actors, including emergency managers, homeland security advisors, state and local government officials, law enforcement officials, private sector actors, as well as academia, media, and community groups. *See* National Cyber Security Division Cyber Exercise Program, US-CERT Website, https://resources.sei.cmu.edu/asset_files/Podcast/2011_016_102_67885.pdf. On July 18, 2013 the financial service sector carried out a cyber attack simulation, Quantum Dawn 2, to "test incident response, resolution and coordination processes." The exercise involved some fifty financial service and government entities and "gave participants the opportunity to run through their crisis response procedures, practice information sharing and refine their protocols relating to a systemic cyber attack." *See* SIFMA, Statement on Quantum Dawn 2 Cybersecurity Exercise (July 18, 2013) http://www.sifma.org/newsroom/2013/sifma-statement-on-quantum-dawn-2-cybersecurity-exercise/.

initiated by a phishing email. The scenario included deaths and billions of dollars in losses. According to accounts, about four dozen senators attended, but apparently were not convinced enough to pass the proposed legislation.[86]

A number of CyberStorm Exercises continue to be held by DHS involving relevant partners, including foreign governments. The published critiques, however, seem to "paper over" problems with such statements as, "[a]lthough public–private interaction around cyber response is continually evolving and improving, it can be complicated by the lack of timely and meaningful shared situational awareness; uncertainties regarding roles and responsibilities; and legal, customer, and/or security concerns."[87]

DoD is engaged in a parallel effort to test concerted government approaches to cyber defense. In February 2014, General Keith B. Alexander, who then headed the United States Cyber Command, described its exercises in testimony before the Senate Armed Services Committee, emphasizing the focus on military services and National Guard units, though many other agencies and international partners were included. General Alexander indicated Cyber Command's goal of developing strong working relationships among DOD/NSA, DHS, and FBI in defending critical infrastructure, including water treatment facilities, gas pipeline, and electrical grids.[88]

---

[86] Brendan Sasso, *White House Simulates Cyberattack for Senators in Push for More Regulation*, THE HILL (Mar. 8, 2012), http://thehill.com/blogs/hillicon-valley/technology/214951-white-house-simulates-cyber-attack-for-senators-as-part-of-push-for-legislation; Jennifer Martinez, *White House tries cyber scare demonstration to spur Senate*, POLITICO (Mar. 8, 2012), http://www.politico.com/news/stories/0312/73800.html.

[87] DEPARTMENT OF HOMELAND SECURITY, CYBERSTORM III, FINAL REPORT (July 2011), http://www.dhs.gov/sites/default/files/publications/CyberStorm%20III%20FINAL%20Report.pdf.

[88] Col. Rivers Johnson, *Cyber Guard exercise focuses on defensive cyberspace operations*, UNITED STATES ARMY, (Aug. 16, 2012), http://www.army.mil/article/85786/. In 2014, the same actors exercised their support to Department of Homeland Security and FBI responses to foreign-based attacks on simulated critical infrastructure networks to further promote collaboration and critical information sharing. DEPARTMENT OF DEFENSE, CYBER GUARD EXERCISE TESTS PEOPLE, PARTNERSHIPS (July 17, 2014), http://www.defense.gov/news/newsarticle.aspx?id=122696. In 2014, the same actors exercised their support to Department of Homeland Security and FBI responses to foreign-based attacks on simulated critical infrastructure networks, to further promote collaboration and critical information sharing. *Id.* Exercises convened DHS, FBI, USCYBERCOM, state government officials, National Guard, Information Sharing and Analysis Centers, and private industry participants. Statement of General Keith B. Alexander Commander of United States Cyber Command Before The Senate Committee on Armed Service (Feb. 27, 2014), http://www.armed-services.senate.gov/imo/media/doc/Alexander_02-27-14.pdf.

Both departmental exercises seem to be useful. The DHS Cyber Storm exercise series involved a wider variety of participants, including more than a dozen federal government entities, state authorities, and a large number of private companies. [89] Nevertheless Cyber Command simulations with a more inclusive military cast are equally important since the National Guard has long been important in disaster relief.[90]

The fact that the European Union is also engaged in bi-annual detailed exercises means that the chance for more effective civil-military multi-level and multi-national response may be enhanced.[91] NATO has held a large exercise in Estonia.[92] All of these exercises contribute to experience in handling a real crisis, but greater transparency in exercise evaluations would help the Congress and the public, in both the United States and allied nations, better understand how effective the current response system is likely to be and what kind of improvements might be made.

V. Legal Implications

Since the very concept of cyber attacks as a form of warfare is so novel, it is unsurprising that legal guidance has not caught up with technological possibilities. In the absence of international agreements and domestic legislation in the United States and Europe, creative attempts have been made to bring cyber attacks under the umbrella of existing international and domestic legal doctrines. Yet analogies, however creative and persuasive, are not infinitely elastic.

The Tallinn Manual represents an important international step in attempting to state current international treaty and customary law that pertains to cyber exploitation. In 2009, the NATO Cooperative Center of

---

[89] *See* Annex A. Participant List, DEPARTMENT OF HOMELAND SECURITY, CYBER STORM III FINAL REPORT, (July 2011), http://www.dhs.gov/sites/default/files/publications/CyberStorm%20III%20FINAL%20Report.pdf.

[90] These simulations focus on how DOD/NSA and the National Guard interact in cyberspace in support of DHS and the FBI. The role of non-governmental participants in Cyber Guard is unclear. On the one hand, they are described as "partners" who "completed" the exercise. On the other hand, it is suggested that they took part as observers. *See* DEPARTMENT OF DEFENSE, CYBER GUARD EXERCISE TESTS PEOPLE, PARTNERSHIPS (July 17, 2014), http://www.defense.gov/news/newsarticle.aspx?id=122696.

[91] *Biggest EU cyber security exercise to date: Cyber Europe 2014 taking place today*, EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (Apr. 18, 2014), http://www.enisa.europa.eu/media/press-releases/biggest-eu-cyber-security-exercise-to-date-cyber-europe-2014-taking-place-today.

[92] Sam Jones, *NATO holds larges cyber war games*, FINANCIAL TIMES (Nov. 20, 2014), http://www.ft.com/intl/cms/s/0/9c46a600-70c5-11e4-8113-00144feabdc0.html#axzz3TwGGCf83.

Excellence commissioned a broad international group of legal and technical experts to explain the relevant law and practice as it stood at the time. Under the leadership of its editor, Professor Michael N. Schmitt, it chose the format of rules with explanations, not unlike the judicious approach taken by the American Law Institute in its Restatements of Law in various fields. It is not meant to express an official interpretation, as a disclaimer makes clear,[93] but it is an influential document toward that end, and it has been treated as such. It did not create new law, nor suggest possible international agreements that might be adopted. It did create a consensus, non-binding document that could form the basis for future negotiations. However, the process has not stimulated perceptible international movement since its completion in 2012. Unfortunately, a life raft that is being constructed very slowly—one nail at a time—may not be finished before the storm hits.

A. U.S. Domestic Legal Issues

While questions of international law and use of force may be at the forefront of scholarly discussion, domestic steps to cope with cyber incidents are of immediate importance in view of the vulnerability of critical infrastructure in the United States. The U.S. President has war powers to deal with an unmistakable cyber attack with kinetic effects under the AUMF of 2001,[94] limited to those responsible for 9/11, and under Article II of the U.S. Constitution. In the event of a cyber attack on critical infrastructure, what powers would an American president have to intervene to step in to restore and manage the problem if the private company were not cooperating?

Any president must be mindful of the caveats of the *Youngstown* "Steel Seizure" case and its progeny.[95] In 1952, the United States was in the middle of the Korean War and steelworkers unions were about to go on strike. The President, concerned that a work stoppage in such a critical industry would adversely affect the conduct of the war, decided to place the steel mills under government control by drafting the workers and having them continue production. In the most cited concurring opinion, Justice Jackson offered a three-part test for determining the scope of presidential power.[96] Justice Jackson described the third situation, which

[93] TALLINN MANUAL, *supra* note 19.

[94] Authorization for the Use of Military Force, Pub. L. No. 107-40, 50 U.S.C. § 1541 (2001) states that "the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons".

[95] Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952).

[96] First, the strongest case for permitting the President's intervention, Justice Jackson argued, is government seizure under facts that are supported by legislation. A seizure

fit the facts of the *Youngstown* case, in the following terms: "[W]hen the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter."[97] Justice Jackson argued that, in seizing the steel mills, presidential power was exercised, "not because of rebellion, but because of a lawful economic struggle between industry and labor;" thus "it should have no such indulgence."[98] Congress had prescribed a method of resolving labor disputes in the Taft-Hartley Act[99] and as, Justice Black's opinion of the Court stated, "When the Taft-Hartley Act was under consideration in 1947, Congress rejected an amendment which would have authorized such governmental seizures in cases of emergency."[100] Instead, it prescribed detailed methods for dispute resolution by "customary devices" such as mediation and conciliation.[101]

If a future president should determine that it is necessary for the government to interfere with or even partly manage and operate privately-owned infrastructure that has been crippled by a cyber attack, government counsel would need to review both the legislative history of all legislation then on the books, and proposed bills to see whether Congress had considered and rejected government takeover. Counsel would have to closely examine the facts to also opine on inherent presidential Commander-in-Chief powers. In that way, counsel could advise the President whether any government seizure would likely be upheld.[102] The composition of the Supreme Court at the time would also be crucial. Prediction is so fraught with uncertainty that few people would venture a definitive answer. Judicial precedents, even during a war, offer limited guidance. Nevertheless, without a specific congressional mandate, and short of a national emergency, the Supreme Court might not support

---

executed by the President pursuant to an Act of Congress would be supported by the strongest of presumptions and the widest latitude of judicial interpretation, and the burden of persuasion would rest heavily upon any who might attack it. A second situation, in which government seizure might be permissible, involved presidential action without legislative support or expression of congressional direction. That situation would turn on the facts. In Justice Jackson's words: "[W]hen the President acts in absence of either a congressional grant or denial of authority, he can only rely upon his own independent powers, but there is a zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain. Therefore, congressional inertia, indifference or quiescence may sometimes, at least as a practical matter, enable, if not invite, measures on independent presidential responsibility." *Id.* at 636–37.

[97] *Id.* at 637.

[98] *Id.* at 645.

[99] NATIONAL LABOR RELATIONS ACT OF 1947, http://www.nlrb.gov/resources/national-labor-relations-act.

[100] Youngstown, 343 U.S. at 586.

[101] *Id.* at 604.

[102] *See* Hamdan v. Rumsfeld, 548 U.S. 557, 586 (2006) (holding inter alia that absent specific congressional authorization, not offered by the AUMF, the defendant could not be tried by military commission).

government seizure and operation of critical infrastructure. Even though the "tests" of Justice Jackson have already been somewhat modified with time and new case facts,[103] it would nonetheless take a major cyber catastrophe for a president to take control of critical infrastructure. [104]

Thus, absent congressional action, and before a crippling cyber attack on critical infrastructure, the government needs to heighten its efforts to achieve a degree of civilian, military, and private sector cooperation and coordination that has so far been elusive.

The Cybersecurity Act of 2012, introduced by Senators Lieberman, Collins, Feinstein, and Rockefeller, would have provided for risk assessment, set standards for critical infrastructure, such as energy, transportation, water, and food, and dealt with both private industry and public agencies.[105] Unlike earlier proposed legislation, Internet freedom and civil liberties advocates raised few objections to this piece of draft legislation.[106] Their opposition had provided impetus to shelving the Protecting Cyberspace as a National Asset Act ("Kill-Switch") Act of

---

[102] An interesting comment was made by Justice Rehnquist in his majority opinion in *Dames & Moore v. Regan*, a case about government seizure of Iranian assets: "Although we have in the past found and do today find Justice Jackson's classification of executive actions into three general categories analytically useful, we should be mindful of Justice Holmes' admonition, quoted by Justice Frankfurter in *Youngstown* . . . that '[the] great ordinances of the Constitution do not establish and divide fields of black and white.'" 453 U.S. 654, 670 (1981) (quoting *Springer v. Philippine Islands*, 277 U.S. 189, 209 (1928) (dissenting opinion). "Justice Jackson himself recognized that his three categories represented 'a somewhat over-simplified grouping', 343 U.S., at 635 , and it is doubtless the case that executive action in any particular instance falls, not neatly in one of three pigeonholes, but rather at some point along a spectrum running from explicit congressional authorization to explicit congressional prohibition." *Dames*, 453 U.S. at 670. "This is particularly true as respects cases such as the one before us, involving responses to international crises the nature of which Congress can hardly have been expected to anticipate in any detail." *Id.*

[104] That, of course, leaves ordinary federal action under criminal law. *See Prosecuting Computer Crimes*, DEPARTMENT OF JUSTICE (last visited Mar. 29, 2015), http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf; *Kaspersky Lab publishes an article entitled 'Cybercrime and the Law: a review of UK computer crime legislation'*, KAPERSKY LAB (May 29, 2009), http://www.kaspersky.co.uk/about/news/virus/2009/Kaspersky_Lab_publishes_an_article_entitled_Cybercrime_and_the_Law_a_review_of_UK_computer_crime_legislation; *United Kingdom of Great Britain and Northern Ireland Cybercrime Legislation - Country profiles*, COUNCIL OF EUROPE (May 2011), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp.

[105] Cybersecurity Act of 2012, S. 2105, 112th Cong. (2011-2012). An amended version, S. 3414, was introduced on July 19, 2012.

[106] Jon Swartz, *'Kill Switch' Internet bill alarms privacy experts*, USA TODAY (Feb. 15, 2011), http://usatoday30.usatoday.com/tech/news/internetprivacy/2011-02-15-kill-switch_N.htm

2010.[107] Their concerns were addressed by the creation of an oversight board.

The original Cybersecurity Act of 2012, and less so its revised version, was not aggressive. The later version mandated the creation of a cybersecurity council and reinforced the provisions of PPD-21 and Executive Order 13636, deepening its effect and making reversibility more difficult.[108] The second version required the Council to develop an inventory of critical infrastructure.[109] Furthermore, the second version even softened the provision providing that the Department of Homeland Security set sector performance standards by allowing the industry to set standards voluntarily, but—while technical assistance and even security clearance would also be offered—the standards had to be approved by the Council.[110] It provided oversight through required reporting.

The original legislation and its revision suggested that in times of "national cyber emergency," the President would retain the power to require providers of critical infrastructure to implement emergency response plans.[111] But neither version of the bill provided strong enforcement powers. Although its supporters asserted that the legislation did not give the President power to completely shut down the Internet, the vagueness in defining a "cyber emergency" and the measures flowing from that declaration alone were enough to defeat the bill.[112] Given the potential chaos that a cyber incident could cause, the Cybersecurity Act of 2012 was far from draconian in its requirements. Nevertheless, Republican Senators led by Senator McCain, with pressure from business interests,[113] prevented

---

[107] Protecting Cyberspace as a National Asset Act of 2010, S. 3480, 111th Cong. (2010).
[108] S. 3414, 112th Cong. (2012).
[109] Ibid § 102
[110] Ibid §103–05
[111] Cybersecurity Act of 2012, S. 2105, 112th Cong. (2011-2012).
[112] S. 3414, 112th Cong. (2012). Note that § 249 of the Cybersecurity and Internet Freedom Act of 2011 bill provided that the "President may issue a declaration of a national cyber emergency to covered critical infrastructure" empowering "measures or actions necessary to preserve the reliable operation, and mitigate or remediate the consequences of the potential disruption, of covered critical infrastructure." Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong. (2011). The bill did include safeguards in a governmental body and time limits—all of which could have been strengthened and clarified. *Id.*
[113] *See* Siobhan Gorman, *Cybersecurity Plan Faulted*, WALL STREET JOURNAL (May 27, 2011), http://online.wsj.com/article/SB10001424052702303654804576345772352365258.html. The U.S. Chamber of Commerce, in opposing S-3414, stated:

> Cybersecurity relies on the business community and the federal government working collaboratively. The regulatory approach provided in S. 3414 would likely create an adversarial relationship, which should be unacceptable to lawmakers. The Chamber urges Congress to not complicate or duplicate existing industry-driven security standards

its passage. Even its moderate requirements were regarded as too burdensome.[114]

Even weaker legislation than the Cybersecurity Act of 2012 was introduced in 2013 to strengthen research efforts and to cement the efforts made under PPD-21 and Executive Order 13636.[115] Although such

---

> with government mandates and bureaucracies, even if they are couched in language that would mischaracterize these standards as 'voluntary'. The Chamber believes Congress can move the needle in a meaningful way on cybersecurity by approving the SECURE IT Act. The Chamber urges you to support amendments expected to be offered that would strike the text of S. 3414 and replace it with the SECURE IT Act of 2012. The Chamber strongly opposes S. 3414, the Cybersecurity Act of 2012 and may consider votes on, or in relation to S. 3414 in our annual How They Voted scorecard.

Key Vote letter on S. 3414, the "Cybersecurity Act of 2012", U.S. CHAMBER OF COMMERCE (Jul. 30, 2012), https://www.uschamber.com/letter/key-vote-letter-s-3414-cybersecurity-act-2012%E2%80%9D. *See also* Ken Dilanian, *U.S. Chamber of Commerce leads defeat of cyber-security bill*, L.A. TIMES (Aug. 3, 2012), http://articles.latimes.com/2012/aug/03/nation/la-na-cyber-security-20120803.

[114] Michael S. Schmidt, *Senators Force Weaker Safeguards Against Cyberattacks*, N.Y. TIMES, (July 27, 2012), http://www.nytimes.com/2012/07/28/us/politics/new-revisions-weaken-senate-cybersecurity-bill.html.

[115] At the time of this writing, the bill had been reported by committee in the Senate. *See* Cybersecurity Act of 2013, S.1353, 113th Cong. (2013). Later, the Chamber of Commerce wrote in support of S. 1353, the Cybersecurity Act of 2013—a much less stringent form of the previous bill:

> Cybersecurity Act of 2013 - Title I: Public-Private Collaboration on Cybersecurity - (Sec. 101) Amends the National Institute of Standards and Technology Act to permit the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology (NIST), to facilitate and support the development of a voluntary, industry-led set of standards and procedures to reduce cyber risks to critical infrastructure. Requires the Director, in carrying out such activities, to: (1) coordinate continuously with, and incorporate the industry expertise of, relevant private sector personnel and entities, critical infrastructure owners and operators, sector coordinating councils, Information Sharing and Analysis Centers, and other relevant industry organizations; (2) consult with the heads of agencies with national security responsibilities, sector-specific agencies, state and local governments, governments of other nations, and international organizations; (3) identify a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, that may be voluntarily adopted by owners and operators of critical infrastructure to help identify, assess, and manage cyber risks; and (4) include methodologies to mitigate impacts on business confidentiality, protect individual privacy and civil liberties, incorporate voluntary consensus standards and industry best practices, align with international standards, and prevent duplication of regulatory processes.

legislation would have greater permanence than an executive order, it did not amount to effective regulation. Without legislation and the uncertainty of presidential powers, the American people must rely on progress made in voluntary compliance. It is hard not to be skeptical of an effort that can do no more than seek to persuade reluctant industry to implement the standards and procedures on a voluntary basis that they worked so hard to defeat as a statutory requirement. Only the experience of crippling attack will reveal whether the voluntary measures and exercised collaboration will prove sufficient to obviate the need for legislation. And without legislation that at least has the power to set and implement standards, the constitutionality of presidential seizure in a cyber crisis affecting infrastructure remains in doubt.

B. International Legal Issues

A key international legal question in cybersecurity is whether and when a cyber attack should be treated as a move towards war or as something else—an economic crime or political or commercial espionage. Although under many circumstances characterization of cyber exploitation turns on the facts, any characterization is likely to be speculative until the next moves occur. Thus far, just as with targeted killing, doctrinal thinking has wavered between legal alternatives. Since ambiguity is likely to continue, definitive allocation of governmental responsibility among civilian and military agencies will remain a question in many situations, mandating collaboration, regardless of the characterization.

Professor Mary Ellen O'Connell, in the article mentioned, argues that the balance has tipped in favor of militarization, although remedies, such as countermeasures, are available through existing international legal means. She suggests augmentation by "dual use" treaties, patterned on the Chemical Weapons Convention or the Nuclear Proliferation Treaty.[116] No such deep international regulatory treaties dealing with cyber attacks exist to clarify international law, nor are any under serious negotiation in the West.

The same issues of imminence of attack and legality of response are present as in the other new grey areas of warfare. International legal doctrine is understandably in the process of formation since there are few, if any, examples thus far of cyber attacks that resulted in death or permanent destruction. Harold Koh, then State Department Legal Adviser,

---

Letter supporting S. 1353. The "Cybersecurity Act of 2013", U.S. CHAMBER OF COMMERCE, (July 28, 2013), https://www.uschamber.com/letter/letter-supporting-s-1353-%E2%80%9Ccybersecurity-act-2013%E2%80%9D. This bill had the support of the Chamber of Commerce, which regarded it as "sensible and nonregulatory" as well as industry focused. *Id.*

[116] O'Connell, *supra* note 77, at 203, 205.

in speaking to Cyber Command in 2012, noted that a cyber operation would constitute a use of force if damage were done that approximated damage by the use of conventional weapons; in other words, if death, or significant destruction resulted from cyber activities. He stated:

> In assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors: including the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and intent, among other possible issues. Commonly cited examples of cyber activity that would constitute a use of force include, for example: (1) operations that trigger a nuclear plant meltdown; (2) operations that open a dam above a populated area causing destruction; or (3) operations that disable air traffic control resulting in airplane crashes. Only a moment's reflection makes you realize that this is common sense: if the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force.[117]

But as Professor Jack Goldsmith points out, the cyber attack that causes deaths is not the hard case:

> The challenges arise mainly because the [UN] Charter focuses its prohibitions on military means of inflicting damage on another state, but does not prohibit economic or political means of inflicting damage on another state.[118]

But, that may be the case that ultimately will have to be addressed. It is not an easy matter to find a current legal basis to treat an economic attack as an armed attack when no loss of lives has occurred. Nor can the concept of imminence be stretched to include intrusions that might result in physical harm at some future date.[119] The full impact of a cyber attack

---

[117] Koh, *supra* note 33.

[118] Jack Goldsmith, *How Cyber Changes the Laws of War*, 24 EUROPEAN J. INT'L L. 129, 133 (2013), http://ejil.oxfordjournals.org/content/24/1/129.short?rss=1.

[119] The United Nations rejected a proposal to extend the scope of Article 2(4) of the UN Charter to "economic coercion." *See* Michael Gervais, *Cyber Attacks and the Laws of War*, 30 BERKELEY J. INT'L L. 525 (2012), http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1422&context=bjil; Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBER ATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY (last visited Mar. 29, 2015), http://www.lawfareblog.com/wp-content/uploads/2012/02/schmitt.pdf. Estonian Defense Minister Jaak Aaviksoo has compared the effects of cyber warfare to the effects of economic blockades: "The analogy

may not be easy to ascertain just after it occurred. Thus far, the United States has not treated intrusions into critical infrastructure as a prelude to a shutdown. Some of the novel legal questions that cyber attacks pose can only be reached by tortured interpretations—or creative lawyering.

To redefine attack under the UN Charter in order to treat an economic attack as a prelude to an attack with kinetic consequences would create enormous political as well as legal problems. It is not clear, out of a specific context, what response would be legally or politically appropriate. Harold Koh left the issue of response deliberately open: "A State's national right of self-defense, recognized in Article 51 of the UN Charter, may be triggered by computer network activities that amount to an armed attack or imminent threat thereof."[120] He added, "[a]s the United States affirmed in its 2011 International Strategy for Cyberspace, 'when warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country.'"[121] Although current cyberspace doctrine does allow for the possibility of anticipatory response, it may be more a deterrent statement than expected policy if circumstances were ambiguous.[122]

In May 2014, the United States unveiled charges of economic cyber espionage against five officers from the Chinese People's Liberation Army for infiltrating six American firms and stealing trade secrets to provide a competitive advantage to their Chinese counterparts.[123] Further indictments and an actual arrest of a young Chinese scientist arriving in the United States to attend a conference was reportedly made in Los Angeles in May 2015.[124] The potential for treating such acts as crimes, when there

---

raises questions about whether cyber attacks should now be categorized amongst conventionally regarded acts of war." Sverre Myrli, *173 DSCFC 09 E BIS-NATO and Cyber Defense*, NATO PARLIAMENTARY ASSEMBLY (June 2008), http://www.nato-pa.int/default.asp?SHORTCUT=1782.

[120] Koh, *supra* note 33.

[121] *Id.*

[122] *Department of Defense Strategy for Operating in Cyberspace*, DEPARTMENT OF DEFENSE, (July 2011), http://www.defense.gov/home/features/2011/0411%5Fcyberstrategy/docs/DoD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf.

[123] Attorney General Eric Holder described the indictment as "the first ever charges against a state actor" for economic espionage through hacking. *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, DEPARTMENT OF JUSTICE (May 19, 2014), http://www.justice.gov/opa/pr/2014/May/14-ag-528.html. This case demonstrates the enormous legal complexity of responding to cyber attacks. Hackers who work for the Chinese military (a state actor) attack commercial entities (non-state actors) in the United States to steal trade secrets for the benefit of Chinese businesses. At the same time, some of the Chinese companies receiving the stolen information are owned by the Chinese state. The case combines the elements of both commercial espionage and national security.

[124] Edward Wong , *Chinese Scientists Indicted by U.S. Are Seen as Stars at Home*, N.Y.

is neither a treaty nor working arrangement for extradition, provides public relations value, rather than concrete value as punishment.[125] However, the U.S. Cybersanctions Executive Order of April 1, 2015 may offer a serious deterrent for states, companies, or individuals whose assets could be frozen on the basis of an Executive finding alone.[126] Whether that would include acts by states using non-state surrogates, as Russia reportedly did with Nashe in the Estonia attack of 2007, complicates any sort of retaliation, since state responsibility is deliberately unclear. Cyber attacks by terrorist organizations are the most elusive of all. In those cases, what form of punishment can be fashioned, and against whom?

The Tallinn Manual addresses the question of what constitutes a threat or use of force in its detailed discussion in Rule 10 through 12, [127] and provides guidance in Rule 13 and 14 for appropriate countermeasures. It states that countries can implement cyber "countermeasures" when exercising the right to self-defense, in accordance with the principle of proportionality, only for the purpose of compelling the attacking state to adhere to its international legal obligations and those measures should "have temporary or reversible effects."[128]

Proportionality, as used in the Tallinn Manual and more generally in the threshold before war (*ius ad bellum*), remains a guide to legitimate action, although that issue has not been tested in a cyber attack at present. Should the most appropriate or "proportionate" Iranian response to Stuxnet have been a cyber attack, as a retaliation in kind? That route portends escalating tit-for-tat. The borrowed concepts of *jus ad bellum* and *jus in bello* for response to an economic cyber attack need much further articulation through exercises that play out countermeasures. By 2016, when the Tallinn Manual is to be updated, perhaps more international experience may sharpen the international legal analogies now relied upon.

Dispute settlement through existing treaty mechanisms may offer some possibilities for clarification about incursion and harm done to

---

TIMES (May 20, 2015), http://www.nytimes.com/2015/05/21/world/asia/chinese-scientists-indicted-by-us-are-seen-as-stars-at-home.html?_r=0 ("Several of the six Chinese scientists who were charged with economic espionage by the United States this week are young stars in their fields. . . . The indictments announced by the United States Justice Department on Tuesday were widely reported in the Chinese news media, and they surprised many people here, especially those who know the six accused men."

[125] *Id.*

[126] U.S. Executive Order Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities (Apr. 1, 2015), https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

[127] TALLINN MANUAL, *supra* note 19, at 45–53.

[128] *Id.* at 42.

aviation, telecommunication, or international trade.[129] Sanctions under Chapter VII of the UN Charter offer a politically difficult but sound international legal avenue for punishment of non-life threatening cyber attacks. However, until international agreements alter the law, or the International Court of Justice rules on such issues, many of the novel legal questions that cyber attacks pose will be answered by creative, if contrived, adaptation of historic doctrines.

VI. Shuffling Towards International Cooperation

Efforts to institutionalize international cooperation are rudimentary. In 2011, the Department of Homeland Security negotiated a memorandum of understanding with India on cyber attack cooperation, and in 2012 negotiated a cooperative arrangement with the Canadian government to integrate "respective national cyber-security activities and improved collaboration with the private sector."[130] This is a bare beginning.[131]

The attacks on Estonia prompted some interesting beginnings in NATO's cooperative effort, not only for cooperation after an attack, but also in attack prevention. Both Estonia and NATO treated those attacks under Article 4, which provides for member state consultations after an attack; no action is promised.[132] In contrast, Article 5 of the NATO Charter states that "the Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against all."[133] The potential for NATO collective action does exist if a cyber

---

[129] *Understanding the WTO: Settling Disputes*, WORLD TRADE ORGANIZATION (last visited Mar. 29, 2015), http://www.wto.org/english/thewto_e/whatis_e/tif_e/disp1_e.htm; Jon Bae, *Review of the Dispute Settlement Mechanism Under the International Civil Aviation Organization: Contradiction of Political Body Adjudication*, 4 J. INT'L DISPUTE SETTLEMENT 65, 65–81 (2013); *Dispute Resolution in the Telecommunications Sector: Current Practices and Future Directions*, WORLD BANK WORKING PAPER (Feb. 2006), http://www.itu.int/ITU-D/treg/publications/ITU_WB_Dispute_Res-E.pdf.

[127] *United States and India Sign Cybersecurity Agreement,* Department of Homeland Security (Jul. 7, 2011), https://www.dhs.gov/news/2011/07/19/united-states-and-india-sign-cybersecurity-agreement; *Cyber Security Action Plan : Between Public Safety Canada and the Department of Homeland Security*, Public Safety Canada, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cybrscrt-ctn-plan/index-eng.aspx (last visited Mar. 29, 2015).

[131] For example, in June 2013, the State Department hailed the achievement of an international "landmark consensus" on cyber security issues. The United Nations Group of Government Experts on cyber security agreed to advance stability and transparency in cyberspace. They also agreed "that existing international law should guide state behavior with regard to the use of cyberspace." *Statement on Consensus Achieved by the UN Group of Governmental Experts On Cyber Issues*," U.S. DEPARTMENT OF STATE (June 7, 2013), http://www.state.gov/r/pa/prs/ps/2013/06/210418.htm.

[132] *Building a Secure Cyber Future: Attacks on Estonia, Five Years On,* Atlantic Council (May 23, 2012), http://www.atlanticcouncil.org/news/transcripts/building-a-secure-cyber-future-transcript-5-23-12.

[133] *Washington Treaty*, NATO, http://www.nato.int/terrorism/five.htm (last visited Mar. 29, 2015).

attack were part of a traditional attack, or produced similar kinetic effects, which was not arguably the case in Estonia, where the damage was economic and relatively short-term.

In September 2014, at its summit in Wales, NATO announced an enhanced cyber strategy recognizing that a cyber attack might be as harmful as a conventional attack. It affirmed that cyber defense "is part of NATO's core task of self-defense,"[134] but added that the decision to intervene would be made on a case-by-case basis. Thus, it was left ambiguous what kind of attack might prompt NATO to respond under Article 5, and left unaddressed the issue of widespread economic harm.

At present, NATO has put in place an institutional structure to deal with cyber attacks: the Cyber Defense Management Board, creating *inter alia* a Computer Incident Response Capability (NCIRC) to protect its own systems[135] and the NATO Cooperative Cyber Defense Center of Excellence in Tallinn. The Cyber Defense Policy is now integrated into the NATO Defense Planning Process. There are conferences and membership training to defend against cyber attack, which has included NATO training the Jordanian army to defend against ISIS cyber attacks.[136] It is not yet clear how effective any of these developments may turn out to be, but they are part of a developing institutional framework.[137]

The European Union issued a proposal for an EU-wide directive on February 7, 2013 in order to improve cooperation on cyber-security. The European Parliament adopted the Directive in March 2014.[138] The proposal

---

[134] *Wales Summit Declaration*, NATO, para. 72 (last visited Mar. 29, 2015), http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

[135] *Cyber Security*, NATO (last visited Mar. 29, 2015), http://www.nato.int/cps/en/SID-856984FF-06F9E6E7/natolive/topics_78170.htm. *See also* James Andrew Lewis, *Thresholds of Uncertainty: Collective Defense and Cybersecurity*, WORLD POLITICS R. (June 11, 2013), http://www.worldpoliticsreview.com/articles/13009/thresholds-of-uncertainty-collective-defense-and-cybersecurity; Marcin Terlikowski & Jozef Vyskoč, *Coming to Terms with a New Threat: NATO and Cyber-Security*, CENTRAL EUROPEAN POLICY INSTITUTE (Feb. 17, 2013), http://www.cepolicy.org/publications/coming-terms-new-threat-nato-and-cyber-security.

[136] *NATO helps Jordan fend off ISIL cyber threat*, NATO YOUTUBE CHANNEL, https://www.youtube.com/watch?v=-TpIouWHNLA (last visited Mar. 29, 2015).

[137] However, of NATO's twenty-eight countries, the Cyber Defense Center only includes eleven: Estonia, Latvia, Lithuania, Germany, Hungary, Italy, Poland, Slovakia, Spain, the Netherlands, and the United States. *See About Cyber Defence Centre*, NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, https://ccdcoe.org/about-us.html (last visited Mar. 29, 2015). Although, France and the United Kingdom have indicated they will join. *Id.*

[138] *Great news for cyber security in the EU: The EP successfully votes through the Network & Information Security (NIS) directive*, EUROPEAN COMMISSION (Mar. 13, 2014) http://europa.eu/rapid/press-release_STATEMENT-14-68_en.htm; *Network & Information Security Directive*, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0244+0+DOC+XML+V0//EN&language=EN.

unsurprisingly notes that the "current situation in the European Union, reflecting the purely voluntary approach followed so far, does not provide sufficient protection" against cyber attacks. Therefore, the Directive would (1) require EU states to "ensure that they have in place a minimum level of national capabilities by establishing competent authorities . . . setting up Computer Emergency Response Teams (CERTs)," and adopting national strategies; (2) encourage national authorities "to cooperate within a network enabling secure and effective coordination, including coordinated information exchange as well as detection and response at EU level;" and (3) "ensure that a culture of risk management develops and that information is shared between the private and public sector."[139] These provisions may do little more than urge member states to reach a minimum level of sensible cyber defense capabilities, but it is a beginning. Moreover, if and when a more robust regulatory scheme might be adopted, the European Union has strong monitoring capabilities to assure adequate implementation

The Council of Europe's Budapest Convention on Cybercrime, which came into force in 2004, bans a wide variety of criminal activity such as illegal interception, system and data interference, and a range of other acts including child pornography and intellectual property theft. It does not deal with cyber attacks amounting to an act of war.[140] Its structure, requiring signatories to create domestic legislation to criminalize the defined activities, is a less threatening model to potential state signatories than a treaty that would set clear standards internationally.[141] It provides for retention of data and methods for cooperation among its signatories. The Budapest Convention permits some variance in how crimes are defined, although it does develop some definitional models. Nevertheless, it is a binding treaty. It has been criticized for lack of enforcement mechanisms and, thus far, lacking the accession of major states such as Russia and China.[142] Although it does not have a dedicated international organization to monitor compliance of the states parties, it is under the aegis of the Council of Europe, which has considerable persuasive power. Though far from universal, the Budapest Convention has the potential to grow in strength, cementing the norms it created.

---

[139] Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union (Feb. 7, 2013) COM(2013) 48, http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/docs/1_directive_20130207_en.pdf; *see also* Haemmerli & Renda, *supra* note 36, at 13.

[140] Convention on Cybercrime, *supra* note 32.

[141] *Id.* at art. 13.

[142] Jack Goldsmith, "Cybersecurity Treaties: A Skeptical View" in *Future Challenges in National Security Law* (Peter Berkowitz ed., Feb. 2011), http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf; PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY, *supra* note 119.

Nevertheless, it may simply remain a weak treaty that only partially develops cooperative behavior.[143]

Regional organizations have cooperated in developing some form of association to prevent cyber intrusions and attacks. The efforts seem piecemeal and, in some cases, more conversational than operational.[144] The 2007 Association of Southeastern Asian Nations (ASEAN) Convention on Counter-Terrorism (ACCT) includes "cyber terrorism" as an "area of cooperation."[145] ASEAN and Japan issued a ministerial-level statement emphasizing the importance of "strengthening [their] collective efforts in cyber security" and encouraging further cooperation.[146] The Asia-Pacific Economic Group (APEC) has a telecommunications and information working group.[147] In Central and Latin America, the Organization of American States (OAS) members have adopted the Inter-American Comprehensive Strategy for Cybersecurity.[148] The African Union was in final discussion stages before signing the Convention on Cyber Security.[149]

The Shanghai Cooperation Organization's (SCO) treaty on cooperation in cyber space provides the "legal and organizational framework"[150] for information security cooperation and has been described

---

[143] In fact, more than forty Council of Europe members and non-members have become signatories. *See* Convention on Cybercrime, "Status as of 29/5/2015," http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG.

[144] Caitríona H. Heinl, *Enhancing ASEAN-Wide Cybersecurity: Time For A Hub Of Excellence?* EURASIA REVIEW (July 19, 2013), http://www.eurasiareview.com/19072013-enhancing-asean-wide-cybersecurity-time-for-a-hub-of-excellence-analysis/.

[145] ASEAN Convention on Counter Terrorism, http://www.iom.int/pbmp/PDF/ASEAN_Convention_Counter_Terrorism_2007.pdf.

[146] "Joint Ministerial Statement of the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation," ASEAN (Sept. 13, 2013), http://www.asean.org/images/Statement/final_joint_statement%20asean-japan%20ministerial%20policy%20meeting.pdf.

[147] APEC's Telecommunication and Information Working Group (TEL) is to support security efforts associated with the information infrastructure of member countries through activities designed to strengthen effective incident response capabilities, develop information security guidelines, combat cybercrime, monitor security implications of emerging technologies, and foster international cooperation on cybersecurity. According to APEC, the working group has pursued some of these activities by collaborating with other international organizations, such as the Association of Southeast Asian Nations, the International Telecommunication Union, and the Organization for Economic Cooperation and Development. UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE, *United States Faces Challenges in Addressing Global Cybersecurity and Governance* (Aug. 2, 2010), http://www.gao.gov/products/GAO-10-606.

[148] Organization of American States, *A Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity*, http://www.oas.org/juridico/english/cyb_pry_strategy.pdf.

[149] African Union, *Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa*, http://au.int/en/cyberlegislation.

[150] *Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security* (June 16, 2009), http://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf.

as one of the most prominent efforts by governments to understand the "scope of the threat pose by cyber attacks."[151] A treaty served as a basis for the International Code of Conduct for Information Security that China, Russia, Tajikistan, and Uzbekistan submitted to the UN General Assembly in 2011.[152] However, SCO may include some serious cyber offenders, and the organization's efforts may seem cynical to other nations, or as efforts to control information flows internally. All these efforts provide beginning models for wider measures that should include all the nations who might suffer cyber attacks or initiate them. Due to the wide gaps in both political systems and similar gaps in trust across so many nations, any beginnings will be slow to spread and to gain effectiveness even within a regional compass.[153]

Any such efforts must address the question: are major powers such as the United States, China, and Russia ready to relinquish offensive cyber capabilities?[154] No regulation is politically realistic so long as offensive capabilities are being employed as an instrument of policy. While there is growing interest in international cooperation, corresponding interest has not been expressed in curbing offensive power.

Even before the publication of military doctrine in Joint Publication 12-3, which provides for offensive operations, as indicated, American interest in offensive action was its putative involvement in offensive cyber action in the "Olympic Games." One element of the Olympic Games was a complex computer worm, "Stuxnet," designed to obstruct the operation of Iran's centrifuges at the uranium enrichment facility in Natanz.[155] In the

---

[151] Hathaway, *supra* note 16.

[152] Letter from the Permanent Representative of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations addressed to the Secretary General, (Sept. 14, 2011), http://cs.brown.edu/courses/csci1800/sources/2012_UN_Russia_and_China_Code_o_Conduct.pdf.

[153] James Andrew Lewis, *Thresholds of Uncertainty: Collective Defense and Cybersecurity*, WORLD POLITICS REVIEW (June 11, 2013), http://www.worldpoliticsreview.com/articles/13009/thresholds-of-uncertainty-collective-defense-and-cybersecurity.

[154] The Washington Post reported that in 2011 the Intelligence Community conducted 231 offensive cyber operations. The newspaper argued that the large numbers of operations signaled that the Obama Administration did not show as much interest in working to "preserve an international norm against acts of aggression in cyberspace" as it did towards engaging in offensive cyber operations against potential adversaries: China, Russia, Iran, and North Korea. Barton Gellman & Ellen Nakashima, *U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents Show*, WASH. POST (Aug. 30, 2013), http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html.

[155] Stuxnet was developed with the assistance of NSA's Israeli counterpart, Unit 8200, and tested at Israel's nuclear facility in Dimona. Stuxnet had two variants. The older version infiltrated the system that operated the valves, which regulated the outflow of gas

summer of 2010, Stuxnet had moved to an Iranian engineer's computer due to programming error and subsequently spread around the world through the Internet, causing embarrassment to the United States and Israel and dislocation for many users.[156] While the full impact of the first known cyber weapon on Iran's nuclear program remains largely unknown, it appears to have achieved only limited success.[157]

It remains a question how long resisting regulation of offensive acts will continue to be effective policy. Even now, American offensive cyber capabilities may not be superior to those of potential rivals, despite vast expenditures.[158] Russia and China have already demonstrated their cyber prowess. Attacks range from crime, to commercial to political espionage, launched by hackers for thrills or for hire, by terrorists, or by states. As one commentator has observed, our conceptual frameworks have not yet grasped the full implications of this global domain, how to deal with the threats it poses, or the potential for its regulation.[159] Nevertheless, it may be too politically difficult to make the case for self-limitation of such an efficient instrument until a catastrophe has occurred on native soil. Further, despite the many intrusions into commercial sites and acts of espionage through 2014, neither the United States nor Europe has suffered a crippling infrastructure attack. Even the computer virus that destroyed data on 30,000 computers belonging to the world's largest oil producer, Saudi Aramco in 2012, was not close to a crippling event—corporate records were affected, but oil production was not seriously affected.[160]

---

from the cascades of centrifuges. Blocking the outflow of gas increased the pressure on centrifuges, causing them damage. The second variant harmed the centrifuges by controlling their operating speed and causing them to crash. Sanger, *supra* note 8, at 190, 197; *see also* Ralph Langner, *Stuxnet's Secret Twin*, FOREIGN POLICY (Nov. 19, 2013), http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack.

[156] David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0.

[157] Langner, *supra* note 155; *see also* Joby Warrick, *Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack*, WASH. POST (Feb. 16, 2011), http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html?sid=ST2011021404206; Ivanka Barzashka, *Are Cyber-Weapons Effective?*, 158 THE RUSI JOURNAL 48, 48–56, http://www.tandfonline.com/doi/pdf/10.1080/03071847.2013.787735.

[158] According to David Sanger, the United States government's annual spending on offensive cyber weapons amounts to billions. *See* CONFRONT AND CONCEAL, *supra* note 8, at 191.

[159] Thanks to Col. Michael Sullivan for this approach.

[160] The United States blamed Iran, describing the attack as "a significant escalation of the cyber threat." Nicole Perlroth, *In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back*, N.Y. TIMES (Oct. 23, 2012), http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html. According to Aramco, the attack was a failed attempt to disrupt oil production. *See Aramco Says Cyberattack Was Aimed at Production* N.Y. TIMES (Dec. 9, 2012), http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-

In general, moreover, the American political climate has not been conducive to the ratification of treaties, particularly those curbing offensive capabilities, since 2001. Recent arms control failures, such as American reluctance to ratify the bioweapons protocol and the Ottawa Land Mine Treaty,[161] suggest high barriers beyond the supermajority required for a Senate vote to ratify.[162] Even ratification of the New START Treaty in 2011[163] revealed powerful political obstacles. Facing strong opposition within the Senate, President Obama was forced to increase spending on costly nuclear weapon-related modernization programs in exchange for reductions in the U.S. arsenal.[164]

Nevertheless, the history of nuclear arms control negotiations and agreements with the Soviet Union is not a totally discouraging precedent, even if developments were slow and included high levels of mutual suspicion. Interest in nuclear arms limitation and creating a test ban treaty was kindled when the Soviet Union developed threatening nuclear capability in the 1950s. The interest grew as it became clear that even numerical superiority was not de facto superiority. Both superpowers had

---

took-aim-at-its-production.html. Iran was also blamed for hacking into the U.S. Navy Marine Corps Internet—an "unclassified network used by the Department of the Navy to host websites, store non-sensitive information and handle voice, video and data communication"—and compromising communications on the network. *See* Siobhan Gorman & Julian R. Barnes, *Iranian Hacking to Test NSA Nominee Michael Rogers*, WALL STREET JOURNAL (Feb. 18, 2014), http://online.wsj.com/news/articles/SB10001424052702304899704579389402826681452?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052702304899704579389402826681452.html. In Israel, a cyber attack took down cameras at the Carmel Tunnels Toll Road, shutting down one of the country's most important highways for two days. *See* Daniel Estrin, *AP Exclusive: Israeli tunnel hit by cyber attack*, USA TODAY (Oct. 17, 2013), http://www.usatoday.com/story/tech/2013/10/27/ap-exclusive-israeli-tunnel-hit-by-cyber-attack/3281133/.

[161] *See* Chairman's Text of Bioweapons Convention Protocol, Apr. 3, 2001, http://www.fas.org/bwc/papers/chairtxt.htm; Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction, Sept. 18, 1997, 2056 U.N.T.S 211. http://www.icrc.org/ihl.nsf/385ec082b509e76c41256739003e636d/d111fff4b9c85b0f41256585003caec3.

[162] Although the Obama Administration has taken steps in mid-2014 to sign the Ottawa Treaty, including production and acquisition limits, ratification is a remote goal. Rick Gladstone, *U.S. Lays Groundwork to Reduce Land Mines and Join Global Treaty*, N.Y. TIMES (June 27, 2014), http://www.nytimes.com/2014/06/28/us/us-to-cut-its-land-mine-stockpile.html?_r=0.

[163] New Strategic Arms Reduction Treaty (New START), signed April 8, 2010, http://www.state.gov/t/avc/newstart/c44126.htm.

[164] Hearing before The Committee on Foreign Relations of the U.S. Senate, June 12, 2010 "Implementation of the New Start Treaty and Related Matters" (Statement of Senator Richard Lugar); Nikolai Sokov & Miles A. Pomper, *New Start Ratification: A Bittersweet Success*, MONTEREY INSTITUTE OF INTERNATIONAL STUDIES (Dec. 22. 2010), http://cns.miis.edu/stories/101222_new_start_ratified.htm.

the capability to effectively wipe out large swaths of the adversary's populations. The reductions—to the present—in nuclear weapons have only marginally curbed effective destructive capability, but the ongoing process of dialogue and efforts to continue to reduce weapons have been as important as the physical reductions themselves.[165]

That ongoing dialogue, as difficult as it has been, has led to the evolution of norms that discourage use of nuclear weapons. It is true, however, that existing binding arms control agreements depend on verification for reassurance. The Chemical Weapons Convention[166] and the various nuclear arms agreements with the former Soviet Union[167] provide demanding technical means of verification—even intrusive verification—by a robust treaty organization, such as the Organization for the Prohibition of Chemical Weapons. One of the stated objections to the bioweapons protocol, if not decisive, was that it could not be verified by traditional means, such as intrusive inspections, or technical means that provide visibility. The demands for adequate verification cannot be met in such an easily concealed means of attack as cyber offers. Moreover, the numbers of non-state actors who could act on behalf of a state—such as Russia's Nashe in Estonia—or on their own behalf, further compound the verification problem.[168]

Professor Goldsmith, in expressing doubt about the feasibility of cyber arms control, states, "One prerequisite to a treaty—at least among powerful nations—is the possibility of mutual gain. Otherwise, there is no incentive to enter into the contract or to comply with it. For most cyber-security issues, it is not clear that a mutually beneficial deal is possible in theory, even assuming that the massive verification problems . . . can be overcome."[169] Yet if many nations persistently suffer from cyber

---

[165] *See* MCGEORGE BUNDY, DANGER AND SURVIVAL: CHOICES ABOUT THE BOMB IN THE FIRST FIFTY YEARS 617 (1988) ("[T]here is work enough in smaller steps toward safety. Good choices are not easy but the record shows that they are not impossible.").

[166] *See* Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (Chemical Weapons Convention), Organization for the Prohibition of Chemical Weapons, http://www.opcw.org/chemical-weapons-convention/.

[167] *See, e.g.*, Interim Agreement Between the United States of America and the Union of Soviet Socialist Republics on Certain Measures with Respect to the Limitation of Strategic Offensive Arms, Federation of American Scientists, http://www.fas.org/nuke/control/salt1/text/salt1.htm; Strategic Arms Limitation Talks (SALT II) Texts, Federation of American Scientists, http://www.fas.org/nuke/control/salt2/text/index.html.

[168] *See* Herbert Lin, *A Virtual Necessity: Some Modest Steps Toward Greater Cybersecurity*, BULLETIN OF ATOMIC SCIENTISTS May 2013, at 82–85.

[169] Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View*, HOOVER INSTITUTION TASK FORCE ON NATIONAL SECURITY AND LAW (Mar. 2011), http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf.

exploitation and feel threatened by cyber attacks, they may come to recognize the potential for mutual gain.

How then to enter a dialogue about restraint and reduction? Voluntary non-binding efforts (or "pledges") might begin to create confidence that other nations share concerns about intrusive attacks.[170] Such confidence building measures (CBMs) might develop as the discomfort of intrusiveness and potential harm from attack begin overshadowing the desirability of maintaining offensive capability. CBMs, however mild, can move toward shifting norms until there is a "cascade" that creates an environment in which binding agreements can be developed. Herbert Lin suggests one approach to CBMs: a group of nations might trade hacking devices that may have but a single use before a defense is possible—a trade in perishable devices—what has come to be known as "zero day vulnerability." These perishable devices now often are bought and sold by hackers.[171]

Another model is a Code of Conduct, or a confidence-building measure (CBM), of the kind that the Fletcher School of Law and Diplomacy students and faculty have been working on for Lincoln Laboratories. Its preamble sets forth its objectives:

> The purpose of this Code is to help facilitate unimpeded access to cyberspace, based upon principles enshrined in the UN Charter and the International Convention on Civil and Political Rights, subject to appropriate international and domestic legal requirements. Cyberspace should be reserved for peaceful purposes. This Code is further designed to establish a widely accepted norm that States shall refrain from the threat or use of force consistent with the principles of international law, subject to the international law of self-defense. It further provides that States shall cooperate with each other in assisting in the

---

[170] Kal Raustiala, *Form and Substance in International Agreements* (Feb. 2004, http://ssrn.com/abstract=505842. Many writers in the midst or toward the end of the Cold War were moving toward the idea that the ongoing process of negotiation itself lessened danger. Some, like McGeorge Bundy, relied on the fact of reduction, more than the scope of reduction of nuclear weapons as lessening danger. He said, in discussing U.S.-Soviet relations in 1988: "Both great governments have learned to respect the nuclear danger and to practice, if not preach coexistence. They have been slow about arms control and still have much to learn about it, but both are now doing better than they were. We are in danger still, but the risk of catastrophe at the end of the 1980s is much lower than in earlier decades." Bundy, *supra* note 165, at 616. *See also* T.V. PAUL ET AL., THE ABSOLUTE WEAPON REVISITED: NUCLEAR ARMS AND THE EMERGING INTERNATIONAL ORDER (2000).

[171] Interview with Herbert Lin, Senior Research Scholar for Cyber Policy and Security at the Center for International Security and Cooperation and Research Fellow at the Hoover Institution, Stanford University (May 3, 2014) (notes in possession of author).

> defense of states threatened by cyber exploitation or under cyber attack. Adherence to this Code of Conduct is voluntary and open to all states.[172]

The draft Code of Conduct includes provisions concerning unimpeded access, prevention of harm, mutual cooperation, measures for domestic protection and privacy, and procedures for peaceful dispute settlement.

If such a CBM were accepted by the United States and even a small core group of nations, it might signal a shift in norms that would begin to attract more nations. This has been the approach of the non-binding Proliferation Security Initiative (PSI). The PSI began in 2003 with eleven like-minded nations and, as of 2013, expanded to 102 with its binding additional ship-boarding agreements bringing some success in preventing trafficking in items designed to facilitate nuclear weapons development and proliferation. Admittedly, even weak measures such as those embodied in CBMs or voluntary pledges may take a long time, and much pain may be suffered before the potential of norm development can be achieved. But strong and ongoing diplomatic presence and dialogue, together with improved civil-military collaboration within democratic nations, offer the most constructive and rational approach.

---

[172] Draft Code of Conduct (in possession of the International Security Studies Program at the Fletcher School of Law and Diplomacy, Tufts University).