Cornell International Law Journal

Volume 48
Issue 3 *Issue* 3 - *Fall 2015*

Article 1

Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents

Oren Gross

Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents

Oren Gross†

Introduction

Computer networks and information and communication technologies (ICT) constitute the nerve system of modern society.[1] States, organizations, corporations, and individuals critically depend on information infrastructures for—among other things—commerce, communication, emergency services, energy production and distribution, mass transit, military defenses, and health services. The centrality of ICT in all facets of modern life—and the vulnerability of these technologies and infrastructures to threats and damage—necessitates close attention to issues of cybersecurity broadly understood. As a recent study states:

> Cybersecurity incidents, be it [sic] intentional or accidental, are increasing at an alarming pace and could disrupt the supply of essential services we take for granted such as water, healthcare, electricity or mobile services. Threats can have different origins—including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and uninten-

† Irving Younger Professor of Law and Director, Institute for International Legal & Security Studies, University of Minnesota Law School. I presented the first version of this Article in June 2013 in "Securing the Freedom and Stability of Cyberspace: The Role and Relevance of International Law," an international conference organized by the International Law Division of the Federal Foreign Office of the Federal Republic of Germany and the University of Potsdam. Special thanks to my dear friend, Andreas Zimmermann, who was one of the co-organizers of the conference and who pushed me to explore the issues discussed in this Article. I also thank Stephanna Szotkowski and Andrew Leiendecker for their excellent research assistance.

1. THE WHITE HOUSE, THE NATIONAL SECURITY STRATEGY TO SECURE CYBERSPACE vii (2003).

tional mistakes.[2]

In addition to the growing dependence on ICT, several other trends reinforce the concern about cybersecurity threats.[3] First is the growing dependence on computer networks by critical infrastructure systems (CIS),[4] defined in an Executive Order published by President Obama to include "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."[5] A second trend concerns the exponential growth in the complexity of com-

2. *Commission Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, at 3, COM (2013) 1 final (Feb. 7, 2013).

3. A November 2013 poll by the PEW Research Center found that seventy percent of Americans believed "cyber-attacks from other countries" represented a "major threat" to the United States, putting the fear of cyber incidents on par with domestic terrorist attacks and nuclear proliferation in Iran and North Korea. *Public Sees U.S. Power Declining as Support for Global Engagement Slips*, PEW RES. CTR. (Dec. 3, 2013), http://www.people-press.org/2013/12/03/public-sees-u-s-power-declining-as-support-for-global-engagement-slips/.

4. 1 NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 1 (2014). The National Institute of Standards and Technology explained:

> The national and economic security of the United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. Similar to financial and reputational risk, cybersecurity risk affects a company's bottom line. It can drive up costs and impact revenue. It can harm an organization's ability to innovate and to gain and maintain customers. *Id.*

5. Exec. Order No. 13,636, 78 Fed. Reg. 11,739, § 2 (Feb. 19, 2013). A further Presidential Policy Directive on critical infrastructure security and resilience identified sixteen critical infrastructure sectors, and specifically pointed to control systems, energy resources, finance, telecommunications, transportation, and water facilities as critical infrastructure targets. Office of the White House Press Secretary, *Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience* (Feb. 12, 2013), https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. *See* Peter Sommer & Ian Brown, *Reducing Systemic Cybersecurity Risk* (Jan. 14, 2011), http://www.oecd.org/gov/risk/46889922.pdf [hereinafter OECD]. *See also* Eric Luiijf & Marieke Klaver, *Governing Critical ICT: Elements That Require Attention*, 6 EUR. J. RISK REG. 263 (2015). To date, there is no internationally acceptable definition of what precisely constitutes CIS. As Kristen Eichensehr notes:

> The Department of Homeland Security lists as examples . . . professional sports leagues, casinos, campgrounds, and motion picture studios. Many countries might be surprised to discover that the United States considers the Iranian hack of the Las Vegas Sands Corporation and the North Korean hack of Sony Pictures to be attacks on 'critical infrastructure.'

Kristen Eichensehr, *"International Cyber Stability" and the UN Group of Governmental Experts*, JUST SECURITY (July 14, 2015, 9:21 AM), https://www.justsecurity.org/24614/international-cyber-stability-un-group-governmental-experts/. Interestingly, Congress has failed to agree on legislation to enforce minimum standards for equipment running critical infrastructure. *See also* Peter G. Neumann, *Risks to the Public in Computers and Related Systems*, 33 SOFTWARE ENGINEERING NOTES 15 (2008).

puter-based systems,[6] which makes these systems increasingly vulnerable to programming errors and bugs, as well as to malicious abuse and exploitation.[7] Complexity is not only limited to individual programs and software: it is inherent in the structure of ICT networks as a whole. This complexity results in system configurations that may simply be unrecognized by those who depend on such systems. In addition, the low costs of entry into the world of computer networks and the ability of cyber attackers to disguise themselves make the world of computer networks an attacker-friendly environment.[8] Third, the growing complexity of computer networks, and the data and information that they handle increases the reliance of such networks on Supervisory Control and Data Acquisition Systems (SCADA). Many SCADA devices communicate using Internet protocols, sometimes over the public Internet, making them susceptible to attack.[9] A fourth trend involves the move to cloud computing that entails the concentration of data and resources in infrastructures that are maintained by third-party providers while, at the same time, physically distributing those same infrastructures among a number—a potentially large number—of countries and jurisdictions.[10]

Legal scholarship about cybersecurity has focused on cyberspace as a new domain for warfare. As such, existing discussions have tended to concentrate on cyber "crime," cyber "espionage," cyber "attacks," and cyber "warfare" as willfully perpetrated, pre-meditated, and intentional actions. Furthermore, existing legal literature has focused almost exclusively on the legal obligations of, and possible sanctions against, states and non-state actors that orchestrated cyber attacks, and to a much lesser extent on the responsibilities of states whose own cyber infrastructure has been used by

---

6. One example is the growth in Source Lines of Codes (SLOC) in computer programs. The OECD study notes that while Windows NT 3.1 had 4.5 million SLOC, Windows XP had 40 million lines of code. OECD, *supra* note 5, at 22–23. More lines of code mean invariably a greater number of bugs in the software—even if we keep constant the ratio of bugs or lines.

7. *Id.*

8. *See id.* at 16–17. Cyber operations

> can take place in an instant and come from anywhere in the world. They can be orchestrated and conducted from the comfort of a home or office, without the risks of spies and undercover operations, physical break-ins, and the handling of explosives. The number of targets that potentially could be reached is staggering. Operations could be launched by state or nonstate actors, and by individuals or groups. The cost to the perpetrators might be negligible, the losses to the victims immeasurable. *Id.*

DOROTHY E. DENNING, INFORMATION WARFARE AND SECURITY 17 (1998). *See also* Nicolas Jupillat, *Armed Attacks in Cyberspace: The Unseen Threat to Peace and Security That Redefines the Law of State Responsibility*, 92 U. DET. MERCY L. REV. 115, 116 (2015) ("Cyberspace is an equalizing factor that empowers non-State actors to cause heavier damage than they would in conventional war fighting domains, at considerably lower costs.").

9. OECD, *supra* note 5, at 21–22; Alan T. Murray & Tony H. Grubesic, *Fortifying Large Scale, Geospatial Networks: Implications for Supervisory Control and Data Acquisition Systems*, *in* 1 CRISIS MANAGEMENT: CONCEPTS, METHODOLOGIES, TOOLS, AND APPLICATIONS 224, 239–40 (2014).

10. *See* Jorge L. Contreras, Laura DeNardis & Melanie Teplinsky, *Mapping Today's Cybersecurity Landscape*, 62 AM. U. L. REV. 1113, 1117 (2013).

another state or by non-state actors to carry out harmful cyber operations against a third state. This Article offers radically different perspectives on both counts. First, the Article recognizes that the harm to computer networks and physical systems interconnected with them may be just as catastrophic when the source of damage is not intentional, but rather, the result of human error or conventional threats. Second, the Article offers the first exploration and analysis of possible bases for, and scope of, responsibilities and obligations that may be imposed not on the state or non-state actor that originated the attack, but rather, on the directly affected state (DAS)—in other words, the state that is the *target* of the attack or the cyber incident that endangers their own ICT systems and CIS. The Article suggests that imposing legal and technological responsibilities on the state that has been, or indeed may be, exposed to a cyber incident is warranted both as a matter of conceptualizing state sovereignty, and due to the state's various obligations to other states and the global community. Part I examines briefly the range of possible cyber threats. Part II analyzes the possible bases for imposition of responsibility on DAS in the context of cybersecurity incidents. Part III more closely examines the nature and scope of such responsibility before, during, and after a cybersecurity incident materializes.

I. Cyber Threats

Much has been written in recent years about cyberspace as a new domain for warfare.[11] The magnitude of the threats cannot be underestimated. Cyber attacks can "bring whole nations to their knees" and "disable companies."[12] While the cost of executing a cyber attack is relatively small, its financial consequences can be significant.[13] The November 2014

11. *See, e.g.*, JEFFREY CARR, INSIDE CYBER WARFARE: MAPPING THE CYBER UNDERWORLD (2011); PAUL ROSENZWEIG, CYBER WARFARE: HOW CONFLICTS IN CYBERSPACE ARE CHALLENGING AMERICA AND CHANGING THE WORLD (2013); P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 67–165 (2014); Erik Gartzke, *The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth*, 38 INT'L SECURITY 41 (2013). *See also* Michael N. Schmitt, *Cyber Operations in the Jus in Bello: Key Issues*, *in* INTERNATIONAL LAW AND THE CHANGING CHARACTER OF WAR 89 (Raul Pedrozo & Daria Wollschlaeger eds., 2011); Harold Hongju Koh, *International Law in Cyberspace*, 54 HARV. INT'L L.J. ONLINE 1 (2012); Michael N. Schmitt, *Classification of Cyber Conflict*, 17 J. CONFLICT & SEC. L. 245 (2012); Michael N. Schmitt, *Cyber Operations and the Jus Ad Bellum Revisited*, 56 VILL. L. REV. 569 (2011); Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?*, 25 STAN. L. & POL'Y REV. 269 (2014); Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421 (2011); United States Cyber Command, *Beyond the Build: Delivering Outcomes through Cyberspace*, DEP'T OF DEFENSE (June 3, 2015), http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/docs/US-Cyber-Command-Commanders-Vision.pdf.

12. John E. Dunn, *Cyberwar Risks Calamity, Eugene Kaspersky Warns UK Government and Spooks*, TECHWORLD (Apr. 26, 2013), http://www.techworld.com/news/security/cyberwar-risks-calamity-eugene-kaspersky-warns-uk-government-spooks-3444419/ (quoting Eugene Kaspersky, the founder and CEO of Kaspersky Lab).

13. Defense Secretary Ash Carter, United States Department of Defense, Remarks by Secretary Carter at the Drell Lecture Cemex Auditorium, Stanford Graduate School of Business, Stanford, California (Apr. 23, 2015), http://www.defense.gov/News/News-

Sony hack resulted, by some accounts, in total costs to the company of nearly one hundred million dollars.[14] PricewaterhouseCoopers (PWC) has put the average total cost of a cyber attack on a broker-dealer firm at $22 million,[15] and the World Economic Forum (WEF) has estimated that up to $3.06 trillion in projected U.S. economic growth between 2014 and 2020 could be lost if the United States fails to take effective steps to safeguard against cyber threats.[16] Moreover, cybersecurity incidents "in sectors such as communications, finance, transportation[,] and utilities" can have catastrophic consequences.[17] WEF estimates the risk of a major "critical information infrastructure breakdown" in the next decade at ten percent.[18] Until a decade or two ago, cybersecurity incidents could have been regarded as mere "black swan" events that mostly occurred unexpectedly.[19] Their occurrence, however—at some point in time and in some format—is now all too predictable.[20] The number of cybersecurity incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team has increased by 782% from 2006 to 2012—from 5,503 in 2006, to 48,562 in 2012.[21] Similarly, a 2014 PWC survey of "more than 9,700 security, IT, and business executives"[22] investigating cybersecurity trends

---

Transcripts/Transcript-View/Article/607043 [hereinafter Carter] (noting that "[l]ow-cost and global proliferation of malware have lowered barriers to entry and made it easier for smaller malicious actors to strike in cyberspace").

14. Lisa Richwine, *Cyber Attack Could Cost Sony Studio as Much as $100 Million*, REUTERS (Dec. 9, 2014, 5:58 PM), http://www.reuters.com/article/2014/12/09/us-sony-cybersecurity-costs-idUSKBN0JN2L020141209. Sony has not confirmed final costs from the 2014 hack. While Sony initially expected costs of the hack to be only $15 million, in April 2015 that estimate was revised up to $41 million. There have since been no updates to the estimated cost. Mike Snider, *Sony Forecasts Profit for Next Year*, USA TODAY (Apr. 30, 2015, 11:51 AM), http://www.usatoday.com/story/tech/2015/04/30/sony-hack-expenses-41-million/26625671/.

15. Peter Feltman, *Cyberattacks Inevitable, SIFMA Told*, CQ ROLL CALL, 2015 WL 575039 (Feb. 12, 2015).

16. WORLD ECON. FORUM, RISK AND RESPONSIBILITY IN A HYPERCONNECTED WORLD 25 (2014), http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf [hereinafter RISK AND RESPONSIBILITY]. It is estimated that cyberattacks that expose or compromise trade secrets produced a global loss ranging "from $749 billion to as high as $2.2 trillion annually," while the annual cost of cybercrime to the global economy ranged from $375 billion to as much as $575 billion. MANAGING CYBER RISK IN AN INTERCONNECTED WORLD, PRICEWATERHOUSE COOPERS 10–11, 16 (2014), http://www.dol.gov/ebsa/pdf/erisaadvisorycouncil2015security3.pdf [hereinafter PWC].

17. Dunn, *supra* note 12 (quoting Eugene Kaspersky, Kaspersky Lab founder and CEO, in a speech to UK police, politicians, and CSOs).

18. WORLD ECON. FORUM, GLOBAL RISKS 2015 10TH EDITION 45 (2015), http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf. "Critical information infrastructure breakdown" refers to "[s]ystemic failures of critical information infrastructure" such as Internet and satellites that "negatively impact industrial production, public services[,] and communications." *Id.* at 54.

19. *See* NASSIM NICHOLAS TALEB, THE BLACK SWAN: THE IMPACT OF THE HIGHLY IMPROBABLE xxi–xxii (2007) (explaining the theory of black swan).

20. *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFF., GAO-13-187, CYBERSECURITY NATIONAL STRATEGY, ROLES, AND RESPONSIBILITIES NEED TO BE BETTER DEFINED AND MORE EFFECTIVELY IMPLEMENTED (2013) (showing the number of incidents from 2006–2012).

21. *Id.*

22. PWC, *supra* note 16, at 7.

and expectations in the business community found that the number of "security incidents" detected by the business community increased forty-eight percent from 2013 to 2014, up to a total of 42.8 million incidents: "the equivalent of 117,339 incoming attacks per day."[23] The number of institutions reporting cyber attacks costing more than $20 million increased ninety-two percent in the same period.[24] Additionally, there was an eighty-six percent increase "[in] respondents who say they have been compromised by nation-states."[25]

Whether warnings of a cyber Pearl Harbor are warranted[26] or are overly alarmist,[27] there is no questioning the growing awareness of the need to prepare to face such challenges. Not surprisingly, an increasing number of governments have directed their attention to these emerging risks.[28]

In the United States, the Obama administration has sought to devise policies to prepare for both "cyber 9/11" attacks, as well as lower-grade cyber attacks. Echoing Former U.S. Secretary of Defense Leon Panetta's view that "a cyber attack perpetrated by nation states or violent extremists groups could be as a destructive as the terrorist attack on 9/11,"[29] the 2015 Director of National Intelligence's Worldwide Threat Assessment identified cyber threats as the most significant global threat[30] facing the

23. *Id.* at 7.

24. *Id.* at 10.

25. *Id.* at 16.

26. Elisabeth Bumiller & Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, N.Y. TIMES (Oct. 11, 2012), http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=0; Yasmin Tadjdeh, *NSA Chief: China, Russia Capable of Carrying Out 'Cyber Pearl Harbor' Attack*, NAT'L DEFENSE (Feb. 23, 2015), http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?List=7c996cd7-cbb4-4018-baf8-8825eada7aa2&ID=1757 (quoting Admiral Mike Rogers, the Director of the National Security Agency and Commander of Cyber Command).

27. *See, e.g.*, John Arquilla, *Panetta's Wrong About a Cyber "Pearl Harbor"*, FOR. POL'Y (Nov. 20, 2012), http://foreignpolicy.com/2012/11/20/panettas-wrong-about-a-cyber-pearl-harbor/. A 2011 OECD study suggests that, "despite a multiplicity of potential triggering events . . . there are very few single cyber-events with the capacity to provoke a global shock." OECD, *supra* note 5, at 10. *See also* Henry Farrell, *The Hack on the U.S. Government Was Not a 'Cyber Pearl Harbor' (But it Was a Very Big Deal)*, MONKEY CAGE BLOG (June 15, 2015), http://www.washingtonpost.com/blogs/monkey-cage/wp/2015/06/15/the-hack-on-the-u-s-government-was-not-a-cyber-pearl-harbor-but-it-was-a-very-big-deal/.

28. *National Cyber Security Strategies in the World*, EUR. UNION AGENCY FOR NETWORK AND INFO. SECURITY (2013), http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world. *See also* Scott Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305, 340–41 (2015) (suggesting that states are currently "in the midst of reshaping their own cybersecurity policies").

29. Shaun Roberts, *Cyber Wars: Applying Conventional Laws of War to Cyber Warfare and Non-State Actors*, 41 N. KY. L. REV. 535, 536 (2014) (quoting Leon Panetta).

30. James Clapper, U.S. Director of National Intelligence, also views cyber attacks as the most significant threat facing the United States since 2013, when he stated that "cyber attacks and cyber espionage ha[s] supplanted terrorism as the top security threat facing the country." Jupillat, *supra* note 8, at 115.

international community at this time,[31] ranking ahead of counterintelligence, terrorism, weapons of mass destruction, and nuclear proliferation.[32] While the Department of Defense focuses on thwarting and responding to the most serious cyber attacks—those that would have "significant consequences"[33] such as "loss of life, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States"[34]—other agencies and officials realize the need to address "the near-constant, lower-grade attacks that are carried out routinely."[35] In February 2015, the administration announced the creation of the Cyber Threat Intelligence Integration Center (CTIIC), to "analyze and integrate information about cyber threats within the federal government."[36] The CTIIC will not act as an independent investigative force, but will instead analyze data already gathered by various federal agencies. In this way, the CTIIC is intended to operate similarly to the National Counterterrorism Center, providing "a central agency to analyze cyberthreats and coordinate strategy" amongst the preexisting cyber-operations centers in various federal agencies—including Homeland Security, the FBI, and the NSA.[37] Around the same time, a bill was introduced in the U.S. Senate entitled "The Cyber Threat Sharing Act of 2015." The bill sought to allocate $14 billion in fiscal year 2016 to protect federal and private networks from hacking threats,[38] and to "give companies legal liability protections when sharing cyber threat data with [the Department of Homeland Security's National Cybersecurity and Communications Integra-

31. Kristen Eichensehr, *Cybersecurity in the Intelligence Community's 2015 Worldwide Threat Assessment*, JUST SECURITY (Mar. 6, 2015, 12:06 PM), https://www.justsecurity.org/20773/cybersecurity-u-s-intelligence-communitys-2015-worldwide-threat-assessment/.

32. James R. Clapper, Director of National Intelligence, Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee (2015), http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf.

33. Army Sgt. 1st Class Tyrone C. Marshall Jr., *New DoD Cyber Strategy Nears Release, Official Says*, DOD NEWS (Apr. 14, 2015), http://www.defense.gov/News-Article-View/Article/604456 (quoting Assistant Secretary of Defense Eric Rosenbach's testimony before the Senate Armed Services Committee's emerging threats and capabilities subcommittee as saying the "most serious" cyberattacks constitute no more than two percent of all cyberattacks).

34. DEPARTMENT OF DEFENSE, THE DOD CYBER STRATEGY 5 (2015), http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf [hereinafter DOD CYBER STRATEGY].

35. Elias Groll, *U.S. Spy Chief: Get Ready for Everything to be Hacked All the Time*, FOREIGN POL'Y (Sept. 10, 2015, 3:25 PM), http://foreignpolicy.com/2015/09/10/u-s-spy-chief-get-ready-for-everything-to-be-hacked-all-the-time/.

36. Eric Naing, *White House to Create New Cyber Threat Agency*, CQ ROLL CALL, 2015 WL 544274 (Feb. 11, 2015).

37. Ellen Nakashima, *New Agency to Sniff Out Threats in Cyberspace*, WASH. POST (Feb. 10, 2015), https://www.washingtonpost.com/world/national-security/white-house-to-create-national-center-to-counter-cyberspace-intrusions/2015/02/09/a312201e-afd0-11e4-827f-93f454140e2b_story.html.

38. Pamela Parker, Bill Would Increase Sharing of Cyber Threat Data, WESTLAW CORPORATE GOVERNANCE DAILY BRIEFING, 2015 WL 586515 (Feb. 13, 2015).

tion Center]."[39] The effect of this legislation would be to improve domestic cybersecurity safeguards and encourage greater information sharing between private and governmental institutions.[40] After the bill's introduction it was referred to the Committee on Homeland Security and Government Affairs, where it remains a pending issue at the time of this writing.[41]

On April 1, 2015, President Obama issued Executive Order (EO) 13694. The President found that "the increasing prevalence and severity of malicious cyber-enabled activities . . . constitute an unusual and extraordinary threat to . . . national security," leading him to declare that the threat of cyber warfare was a national emergency.[42] EO 13694 identifies the following as perpetrators of cyber attacks:

> [A]ny person . . . responsible for or complicit in . . . cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economy health or financial stability of the United States.[43]

Once an individual or group has been identified as the perpetrator of a cyber attack, the EO "enables the U.S. government to block the property and assets of those involved in such attacks,[44] who have otherwise been difficult to reach."[45] The practical effectiveness of EO 13694 in deterring cyber attacks or holding perpetrators accountable still remains to be seen.[46]

Despite all the attention given to cyber crime, cyber espionage, cyber attacks, and cyber warfare, these terms do not enjoy widely accepted definitions.[47] Generally speaking, there are two major approaches to relating

---

39. Cory Bennett, *Senate Dem Introduces White House Cyber Bill*, THE HILL (Feb. 11, 2015), http://thehill.com/policy/cybersecurity/232534-senate-dem-introduces-white-house-cyber-bill.

40. Many firms are "afraid to share vital cyber intelligence [with the government] due to potential lawsuits or federal enforcement actions." Naing, *supra* note 36 (quoting Cal. Rep. Adam B. Schiff).

41. *See* S. 456, 114th Cong. (2015–2016).

42. Exec. Order No. 13,694, 80 Fed. Reg. 18,077 (Apr. 2, 2015), http://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf.

43. *Id.*

44. "Such attacks" include (i) "Harming, or otherwise significantly compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector," (ii) "significantly compromising the provision of services by one or more entities in a critical infrastructure sector," (iii) "causing a significant disruption to the availability of a computer or network of computers," (iv) "causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain," or (v) engaging in a conspiracy to commit any of the aforementioned offenses. *Id.*

45. Allan Abravanel et al., *President Issues Executive Order to Block Assets of Foreign Cyber Attackers*, 20 CYBERSPACE L. 3 (May 2015).

46. Kristen Eichensehr, *The Cyber Sanctions Executive Order: What Will It Do and Will It Work?*, JUST SECURITY (Apr. 2, 2015, 1:24 PM), https://www.justsecurity.org/21744/cyber-sanctions-executive-order-work/.

47. *See, e.g.*, THOMAS WINGFIELD, THE LAW OF INFORMATION CONFLICT, NATION SECURITY LAW IN CYBERSPACE 1–2, 13 (2000) (noting that efforts to classify them are still in

to cyber events of the categories noted above: the instrument-based approach or the object-based approach.[48] The instrument-based approach focuses on the mode of assault.[49] The use of computers or related networks to cause damage may amount to cyber crime, cyber attacks, or cyber warfare (provided that certain thresholds are crossed which are not the focus of this paper) regardless of whether the harm caused is done to computers or computer networks.[50] The term "cyber" in "cyber attack" refers to and describes, therefore, the mode of assault and distinguishes it from traditional kinetic attacks. In contradistinction, the object-based approach focuses not on the instrumentalities of attack but on computers or computer networks as the targets of attack conducted through and by any means, digital or kinetic.[51] In this context, "cyber" refers to the object under attack rather than to the mode of attack.[52] The absence of consensus around accepted definitions of "cyber" crime, espionage, attacks, and warfare is further exacerbated by a lack of consensus as to whether norms of international law and the U.N. Charter apply to cyberspace,[53] and spe-

their infancy); WILLIAM YURCIK & DAVID DOSS, INTERNET ATTACKS: A POLICY FRAMEWORK FOR RULES OF ENGAGEMENT 2 (2001) (discussing the development of "information warfare" with a focus on U.S. vulnerabilities); Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 J. CRIM. L. & CRIMINOLOGY 379, 381 (2007) (defining cyber threats as "using computer technology to engage in activity that undermines a society's ability to maintain internal or external order" and defining cyber crime, cyber terrorism, and cyber warfare separately); Roderic Broadhurst, *Developments in the Global Law Enforcement of Cyber-Crime*, 29 POLICING: AN INT'L J. OF POLICE STRATEGIES & MGMT. 408, 413–14 (2006) (defining the broader idea of "computer crime"); Michael Gervais, *Cyber Attacks and the Laws of War*, 30 BERKELEY J. INT'L L. 525, 533 (2012) (referencing the U.S. Army's D.C.S.I.N.T. Handbook No. 1.02 definition of "cyber attack"); Joanna Kulesza, *State Responsibility for Cyber-Attacks on International Peace and Security*, 29 POLISH Y.B. INT'L L. 139, 140 (2009) (defining "Information Warfare"); Scott J. Shackelford, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 GEO. J. INT'L L. 971, 978 (2011) ("'[C]yberwarfare' generally refers to an attack by one hostile nation against the computers or networks of another to cause disruption or damage (as compared to a criminal or terrorist attack involving private parties).").

48. Reese Nguyen, Note, *Navigating Jus Ad Bellum in the Age of Cyber Warfare*, 101 CALIF. L. REV. 1079, 1085 (2013).

49. *Id.* at 1088.

50. *Id.*

51. *Id.* at 1086–87.

52. *Id.* at 1087–88. To be sure, the increasing incorporation of networked computing technology into physical infrastructure, systems, and products means that the target of an attack on a computer network may well be the physical components with which that network is tightly connected rather than the network itself. *Id.*

53. U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 19, U.N. Doc. A/68/98 (June 24, 2013) [hereinafter GEE], http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98 ("International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment."). A new consensus document, however, prepared in 2015 by the Group of Governmental Experts "[e]xcluded . . . another U.S. proposal: One that sought to spell out the implications of a 2013 experts' group agreement that international law generally applies in cyberspace just as it does on land or at sea." *See* Joseph Marks, *U.N. Body Agrees to U.S. Norms in Cyberspace*, POLITICO (July 9, 2015, 12:44 PM), http://www.politico.com/story/2015/

cifically, whether and how the norms pertaining to self-defense under article 51 of the Charter apply to cyber attacks and operations, and the responses thereto.[54]

Both the instrument-based approach and the object-based approach share a common conception of willfully perpetrated cyber crime, cyber attacks, and cyber warfare. Whether criminally or politically motivated, terrorist and state-sponsored attacks are pre-meditated and intentional. Unauthorized access to computer systems or networks, theft of information contained in electronic forms, mail bombing, data diddling, salami attacks, computer viruses and malwares, logic bombs, Trojan horses, Internet time thefts, Web jacking, and key-logging are all deliberate logical attacks.[55] Such attacks may focus on the syntax of the target system, disrupting its operating system; or they may be semantic, compromising the accuracy of the information processed by the system.[56] They may penetrate the system—such as through viruses, worms, and Trojans—or disrupt the system

07/un-body-agrees-to-us-norms-in-cyberspace-119900. The drafters of the Tallinn Manual on the International Law Applicable to Cyber Warfare adopted the position that general principles of international law applied to cyberspace. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 13 (Michael N. Schmitt ed. 2013) [hereinafter TALLINN MANUAL].

54. David E. Sanger, *U.S. and China Seek Arms Deal for Cyberspace*, N.Y. TIMES (Sept. 19, 2015), http://www.nytimes.com/2015/09/20/world/asia/us-and-china-seek-arms-deal-for-cyberspace.html. The agreement concluded between the two countries did not, eventually, include a provision pertaining to attacks on CIS. *See* The White House, Fact Sheet: President Xi Jinping's State Visit to the United States (Sept. 25, 2015), https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states. *See also* Kristen E. Eichensehr, *Cyberwar & International Law Step Zero*, 50 TEX. INT'L L.J. 357, 365–67 (2015).

55. *See* Kamini Dashora, *Cyber Crime in the Society: Problems and Preventions*, 3 J. ALTERNATIVE PERSP. SOC. SCI. 240, 245–52 (2011) (defining each of the different types of cyber attacks as well as classifying them by attacks against individuals, against individual property, against organizations, and against society at large). For a summary of cyber security incidents recorded from the US-CERT Control Systems Center (CSSC), see generally ROBERT J. TURK, CYBER INCIDENTS INVOLVING CONTROL SYSTEMS (2005); Vida M. Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places*, 51 NAVAL L. REV. 132, 138–141 (2005); Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F.L. REV. 121, 134–38 (2009); Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 13–21 (2009) (discussing the effects of different types of cyber-attacks); Benjamin S. Buckland et al., *Democratic Governance Challenges of Cyber Security* 15 (D.C.A.F. Horizon 2015 Working Paper No. 1, 2010), http://www.dcaf.ch/Publications/Democratic-Governance-Challenges-of-Cyber-Security (providing a table of categories of cyber threats).

56. The most common syntactic attack is the (Distributed) Denial-of-Service, flooding a system with bogus requests for service. Nguyen, *supra* note 48, at 1097. It should be noted that DoS or DDoS attacks disrupt the system by diminishing the system's functionality, but the attacks typically do not leave a permanent mark on the system inasmuch as they do not modify or destroy the computer system's resources. *Id. See also* Eric Naing & Ryan Lucas, *DNI: Cyber threat shifting to data manipulation*, CQ ROLL CALL, 2015 WL 5256370 (Sep. 10, 2015) (arguing that the focus of cyber attacks will shift from theft and destruction towards "operations that will change or manipulate electronic information to compromise its integrity . . . its accuracy and its reliability instead of merely deleting it or disrupting access to it").

by diminishing its functionality without penetrating the system or modifying the attacked system's resources, such as in the case of denial of service attacks.[57] In addition, attacks may be kinetically performed against the physical infrastructure underlying ICT through, for example, bombing a server's farm.[58]

Yet, the harm to both computer networks and physical systems interconnected with such networks may be just as catastrophic when the source of damage is not intentional, but rather, the result of human error or conventional threats.[59] There is ample empirical data demonstrating the central role human error plays in cybersecurity incidents.[60] A report by IBM indicates that human error has been a contributing factor in over ninety-five percent of all investigated cyber incidents.[61] Similarly, natural disasters may result in the weakening and overburdening of critical information systems due to higher than normal demand levels,[62] and the lowering of security protocols in order to allow out-of-venue responders to use existing systems for disaster management operations.[63] Such weakening of critical systems may have cascading effects when criminals, terrorists, or other nations seek to engage in cyber attacks against the weakened systems. Conventional disasters may also be followed by secondary—or even tertiary—events that would degrade critical systems even further, compounding once again the potential for a large-magnitude harm.

II. Imposing Legal Responsibility on Directly Affected States

Considering cybersecurity incidents through the prism of natural disasters (rather than through the traditional focus on intentional harms) assists in explaining and justifying the imposition of responsibilities on a

57. *See, e.g.*, Stefan Kirchner, *Distributed Denial-of-Service Attacks: Under Public International Law: State Responsibility in Cyberwar*, 8 IUP J. CYBER L. 10, 10–11 (2009).

58. *See* DEPT. OF DEFENSE OFFICE OF GENERAL COUNSEL, AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 5 (2009).

59. U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-1036, CRITICAL INFRASTRUCTURE PROTECTION: MULTIPLE EFFORTS TO SECURE CONTROL SYSTEMS ARE UNDER WAY, BUT CHALLENGES REMAIN, 2, 12, 13 (2007).

60. *See, e.g.*, Ghi Paul Im & Richard L. Baskerville, *A Longitudinal Study of Information System Threat Categories: The Enduring Problem of Human Error*, 36 DATA BASE FOR ADVANCES IN INFO. SYSTEMS 68, 68–79 (2005).

61. IBM GLOBAL TECH. SERV., IBM SECURITY SERVICES 2014 CYBER SECURITY INTELLIGENCE INDEX 3 (2014), http://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf. The most common errors included: opening an infected attachment or unsafe URL, system misconfiguration, poor patch management, use of default usernames and passwords, lost laptops or mobile devices, and disclosure of information through use of an incorrect email address. *Id. See also* Im, *supra* note 60, at 75 ("[T]he major source of unmanaged risks to information systems continues to be accidental in nature. Most of these accidents result arise at the knowledge base error level.").

62. An example is the overloading of information infrastructures in the aftermath of a disaster. Such overloading may result in the system crashing, preventing flow of critical information in real time that may interfere with timely identification and assessment of the harm as well as inhibit recovery efforts. Im, *supra* note 60, at 69.

63. *Id.*

state that has been exposed to a cyber incident.[64] Such justifications are both inward- and outward-looking. On the one hand, a state owes certain duties to its own nationals as well as to those who find themselves in its territory. Such duties are inherent in human rights law and in international humanitarian law,[65] as well as in the very notion of sovereignty. Conceptions of sovereignty as a contingent value depend on the actions of the state that invokes its subordinate state sovereignty to human rights claims. Justifications for sovereignty no longer rest exclusively on sovereignty's own presumptive legitimacy, but rather expand to incorporate justifications that derive from the individuals whose rights are to be protected, and from their right to a safe framework in which they can enforce their autonomy and pursue their interests.[66] As former U.N. Secretary-General Kofi Annan put it: "[t]he state is now widely understood to be the servant of its people, and not vice versa."[67] In its report to the Secretary-General, entitled *A More Secure World: Our Shared Responsibility*, the United Nations Secretary-General's High-level Panel on Threats, Challenges and Change pursued a similarly holistic view of security, looking both at state security and human security. The Panel adopted a broad conception of the latter to incorporate both negative freedoms (freedom from fear and absence of violent conflict) and positive freedoms (such as freedom from want) in order to subject state security to human security.[68]

To do that, the Panel redefined state sovereignty as a responsibility-based rather than a rights-based concept: "In signing the Charter of the United Nations, States not only benefit from the privileges of sovereignty but also accept its responsibilities," which include both external obliga-

64. DAS responsibilities, measured against a background of cybersecurity incidents that are the result of natural disasters, raise less resistance as seeking to blame the victim. It is because of that broader conception of cybersecurity incidents that is suggested in this Article, for example, as comprising both intentional and non-intentional threats and harms, that I prefer to use the term "Directly Affected State" to describe states who suffer the harmful consequences of cybersecurity incidents, rather than the terms "victim state" or "target state" that may suggest a certain degree of intentionality behind the threat.

65. States have an Article 58 duty to protect civilian populations "to the maximum extent feasible." Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 58, Dec. 12, 1977, 1125 U.N.T.S. 3. Article 58 also requires that the government take "other necessary precautions." Eric Talbot Jensen, *Cyber Warfare and Precautions against the Effects of Attacks Symposium*, 88 TEX. L. REV. 1533, 1552 n.123 (2010). "Precautions" refers to actions taken in advance, not in response to attacks. In the context of cyber attacks, a state cannot take this obligation as a reactionary responsibility. *Id.* at 1554.

66. For recent scholarly work regarding responsibility to protect, see generally Monica Hakimi, *Toward a Legal Theory on the Responsibility to Protect*, 39 YALE J. INT'L L. 247 (2014); Thomas H. Lee, *The Law of War and the Responsibility to Protect Civilians: A Reinterpretation,* 55 HARV. INT'L L.J. 251 (2014); Saira Mohamed, *Taking Stock of the Responsibility to Protect*, 48 STAN. J. INT'L L. 319 (2012).

67. Press Release, U.N. Secretary-General, Secretary-General Presents His Annual Report to General Assembly, U.N. Press Release SG/SM/7136 (Sept. 20, 1999).

68. *See generally* U.N. Secretary-General, A More Secure World: Our Shared Responsibility: Rep. of the High-level Panel on Threats, Challenges and Change, U.N. Doc. A/59/565 (Dec. 2, 2004).

tions to other states and the international community as a whole, and internal obligations to protect the welfare of their own peoples.[69] States are to be protected not because they are, as such, intrinsically good, but because they are "[n]ecessary to achieve the dignity, justice, worth and safety of their citizens."[70] The interconnectedness between computer networks and the physical world means that cybersecurity incidents are increasingly more likely to threaten individuals' enjoyment of some of their basic rights, and even endanger their health and lives.[71] Computers and computer networks are now embedded in every facet of modern life, from cellphones, cars, and traffic lights, to hospitals, dams, airport control, and electricity grids. Failure of a state to give appropriate protection to its computer networks or to remedy and correct damage to such systems expeditiously, adequately, and in a timely manner may impair the ability of citizens to enjoy such fundamental rights as the rights to health, privacy, movement, and association—and indeed the very right to life.

A state's obligations, however, are not merely to its own nationals and to people in its territory. In a digitally interconnected world, the strength of the digital chain may be only as strong as its weakest link.[72] Cybersecurity incidents that compromise the security or the functionality of a network component in one country may have critical spillover impacts on the security or functionality of other parts of the network, or other networks that are connected or otherwise related to it, and that may directly or indirectly affect other states or non-state actors.[73] Attacks on servers in the territory of Country X may result in significant harm to the networks and interests of Country Y—and indeed Countries A, B, and C—as well as to individuals who have otherwise no relationship to Country X. Virus or malware attacks directed at a particular country's computers may not be limited to that country, either because the malware has not been programmed carefully or because of other factors that may cause the malware to spill over to computers in other countries.[74]

---

69. *Id.* at 17.

70. *Id.*

71. "There are significant and growing risks of localised misery and loss as a result of compromise of computer and telecommunications services." OECD, *supra* note 5, at 6.

72. Stephen E. Henderson & Matthew E. Yarbrough, *Suing the Insecure?: A Duty of Care in Cyberspace*, 32 N.M. L. Rev. 11, 11 (2002).

73. OECD, *supra* note 5, at 85.

74. *Id.* Thus, for example, Stuxnet, a computer worm considered to be the world's first digital weapon that attacked Iranian centrifuges and computer system involved in Iran's nuclear program, also infected computer systems outside of Iran. Historic data from the early days of the Stuxnet worm attack shows Iran, Indonesia, and India accounting for 58.85%, 18.22%, and 8.31% respectively of infected machines globally. W32.Stuxnet, Symantec (Feb. 26, 2013) http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99. *See also* Kim Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon 29–31 (2014) (noting that over 300,000 machines were infected by the worm with the majority of those located in Iran, but about forty percent located in other countries such as Indonesia and India).

It is well established that a state may not use, nor permit the use of, its territory in such a manner as to cause injury in or to the territory of another or the properties or persons therein.[75] A state may not "allow knowingly its territory to be used for acts contrary to the rights of other States."[76] Similarly, the International Group of Experts (IGE) that drafted the Tallinn Manual on the International Law of Cyber Warfare, concluded that a "State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States."[77] According to the IGE, this due diligence obligation is imposed on states both with respect to government and private cyber infrastructure on their territory as well as cyber activities emanating from that territory.[78] Furthermore, states may have a duty to prevent illegal attacks that they knew about beforehand.[79] The European Convention on Cybercrime criminalizes cyber attacks and also confirms the duty of states to prevent territories from being used by non-state actors to conduct these cyber attacks.[80] The U.N. General Assembly has also called for the criminalization of cyber attacks,[81] prevention of allowing safe havens to launch cyber attacks,[82] and cooperation in the investigation and prosecution of international cyber attacks.[83] The General Assembly and some states have also labeled cyber attacks as a threat to

75. Trail Smelter Case (U.S. v. Can.), 3 R.I.A.A. 1905, 1965 (Perm. Ct. Arb. 1941) (noting that a state "owes at all times a duty to protect other states against injurious acts by individuals from within their jurisdiction"). *See also* Island of Palmas Case (Neth. v. U.S.), 2 R.I.A.A. 829, 839 (Perm. Ct. Arb. 1928) (noting the duty of every state "to protect within the territory the rights of other states, in particular their right to integrity and inviolability in peace and in war").

76. Corfu Channel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, ¶ 22 (Apr. 9). *See also* Rorbert P. Barnidge, Jr., *The Due Diligence Principle under International Law*, 8 INT'L COMM. L. REV. 81 (2006); Riccardo Pisillo-Mazzeschi, *The Due Diligence Rule and the Nature of the International Responsibility of States*, 35 GERM. Y.B. INT'L L. 9 (1992).

77. TALLINN MANUAL, *supra* note 53, at 26 (Rule 5).

78. *See id*. *See also* Michael N. Schmitt, *In Defense of Due Diligence in Cyberspace*, 125 YALE L.J. FORUM 68, 70 (2015). Rather than recognize due diligence as a legal obligation that is imposed on states in cyberspace, however, the GGE report merely stated that "States should seek to ensure that their territories are not used by non-state actors for unlawful use of ICTs." GGE, *supra* note 53, at 23.

79. This duty includes state obligations to enact stringent criminal laws against the commission of international cyber attacks from within national boundaries; to conduct meaningful, detailed investigations into cyber attacks; to prosecute those who have engaged in these attacks; and to cooperate with the victim states' own investigations and prosecutions of those responsible for the attacks. Sklerov, *supra* note 55, at 62–72. *But see* Schmitt, *supra* note 78, at 70–71 (noting that the IGE did not come to an agreement as to whether the due diligence obligation "applies when a state knows that such [harmful cyber] activities will be launched but they have not yet materialized").

80. Convention on Cybercrime, Council of Europe, Nov. 23, 2001, 41 I.L.M. 282, 2296 U.N.T.S. 167. While primarily a treaty among members of the Council of Europe, this convention has also been ratified by the United States, Australia, Canada, and Japan, along with several other non-Council of Europe nations.

81. G.A. Res. 45/121, ¶ 3 (Dec. 14, 1990) [hereinafter G.A. Res. 45/121].

82. G.A. Res. 55/63, ¶ 1 (Jan. 22, 2001).

83. *Id.*

international peace and security.[84] Similarly, the 2015 report of the U.N. Group of Governmental Experts adopts the U.S.-supported "rules of the road" in cyberspace,[85] which include, among others, the acknowledgment that "[a] State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public."[86] While the duty to prevent applies to the state whose territory has been used to launch a cyber attack, it may be extended, conceptually, to DAS who—by the very weakness and vulnerability of their ICT systems—endanger not only themselves and their nationals but also other states and non-state actors.[87] Notions of "good neighborliness" and *sic utere tuo ut alienum non laedas* may be similarly useful in this context.[88] Going a step further, it may also be appropriate to conceptualize the Internet and ICT networks and systems as matters of a common concern of mankind, much like biodiversity and the world's climate.[89]

States that are directly affected by cybersecurity incidents, therefore, ought to bear some of the burden of meeting the threats and challenges related to such incidents. Their responsibility—which does not in any way reduce the responsibility of the states or non-state actors who have initiated the threat—has several layers to it. Successfully coping with cybersecurity harms requires all states to invest funds, technology, intelligence, and human resources to reduce their vulnerabilities to cybersecurity incidents; invest in and improve their capacities to identify, assess, prioritize, and disrupt threats at as early a stage as possible; and act comprehensively and effectively in coordinating and executing both their short-term responses

84. DEP'T OF HOMELAND SEC., THE NAT'L STRATEGY TO SECURE CYBERSPACE 49–52 (2003), http://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf; G.A. Res. 45/121, *supra* note 81.

85. Joseph Marks, *U.S. Makes New Push for Global Rules in Cyberspace*, POLITICO (May 5, 2015), http://www.politico.com/story/2015/05/us-makes-new-push-for-global-rules-in-cyberspace-117632.

86. U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 13(f), U.N. Doc. A/70/174 (July 22, 2015), http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

87. *But see* Schmitt, *supra* note 78, at 71 (noting that the IGE did not agree "on whether a state must take preventive measures to ensure the cyber hygiene of the infrastructure on its territory or whether states should be required to monitor for malicious activity that might be directed at other states"). Schmitt also notes that the IGE failed to reach consensus on whether the obligation of due diligence is imposed on transit states. *Id.* at 72–73. Those who would not extend the obligation to transit states are even less likely to see it applied to and imposed on states that are the targets of harmful cyber activities.

88. U.N. Charter art. 74; United Nations Conference on the Human Environment, *Stockholm Declaration*, princ. 21, U.N. Doc. A/CONF.48/14/Rev.1 (June 5-16, 1972). *See* Elmer E. Smead, Sic Utere Tuo Ut Alienum Non Laedas *A Basis of the State Police Power*, 21 CORNELL L. REV. 276, 276 (1936).

89. *See, e.g.*, U.N. Conference on Environment and Development, *Rio Declaration on Environment and Development*, U.N. Doc. A/CONF.151/26/Rev.1 (Vol. I), annex I (Aug. 12, 1992).

and recovery efforts once threats materialize, as well as long-term adjustments and rehabilitation. In order to minimize the harmful consequences of cybersecurity incidents—in particular when CIS are concerned—DAS will have to invest purposefully in and improve not only their own capabilities but also ensure open, uninterrupted channels of communication with other states and potentially with non-state actors who may be able to assist in mitigation of the harms caused.[90]

Increasing the free flow of information between private institutions and the government, both by encouraging private institutions to disclose incidents to the government (as addressed, for example, by EO 13694) and sharing government information with the relevant non-state actors is key to improving the detection, identification, and eventual punishment of potential cyber attackers. Lisa Monaco, the Homeland Security Advisor to President Obama, recognizes that "[g]etting the private sector to share data about cyber threats is a key part of bolstering . . . cyber defenses."[91] Exchange of information between state and non-state actors would "crowdsource solutions to cyber threats by allowing private industry and the government to share malware . . . and create solutions to defend against it."[92] Facilitating and encouraging the free flow of information between the private and public sectors—both inter-nationally and intra-nationally—would allow states to build stronger safeguards against cyber threats, reducing the likelihood and frequency of cyber incidents. The United States Secretary of Defense, Ash Carter, similarly touted the need for close partnership between the private sector and government.[93] Noting that "American businesses own, operate, and see approximately ninety percent of our national networks,"[94] Secretary Carter emphasized that

> the private sector must be a key partner. The U.S. government has a unique suite of cyber tools and capabilities, but we need the private sector to take its own steps to protect its data and networks. We want to help where we can, but if companies themselves don't invest, our country's collective cyber pos-

90. Carter, *supra* note 13. Secretary Carter stated:

> As a military, we have to embrace openness. Today dozens of militaries are developing cyber forces, and because stability depends on avoiding miscalculation that could lead to escalation, militaries must talk to each other and understand each other's abilities. And DoD must do its part to shed more light on cyber capabilities that have previously been developed in the shadows.

91. Naing, *supra* note 36 (citing Cal. Rep. Adam B. Schiff). *See also* Carter, *supra* note 13 ("One way we're responding . . . is by being more transparent, to raise awareness in both the public and the private sector. Indeed, shining a bright light on such intrusions can eventually benefit us all—businesses and governments alike.").

92. Ranking Member Adam Schiff, Opening Statement in House Permanent Select Committee on Intelligence on Worldwide Cyber Threats (Sept.10, 2015), http://webcache.googleusercontent.com/search?q=cache:FrE4TS5v7EAJ:https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/NunesOpeningnum209102015.pdf+&cd=1&hl=en&ct=clnk&gl=us.

93. Carter, *supra* note 13 (" . . . we know that working together in the cyber domain is essential. And that's why one of the primary aspects of our strategy is working with partners—in the private sector, across our government, and around the world.").

94. *Id.*

ture is weakened and our ability to augment that protection is limited.[95]

Furthermore, as this Article discusses below, DAS may be under an obligation not only to communicate with other states—and perhaps even non-state actors—about cybersecurity incidents, but also to receive external assistance in meeting those threats and harms. Finally, it should be noted that global interconnectivity and interdependence of information and telecommunication technologies and computer networks mean that, to varying degrees, each and every country may find itself the direct object of cybersecurity incidents. Thus, whatever obligations DAS may have are shared among the nations of the world.

In looking for sources for state legal responsibility in this area it may also be instructive to note the argument that companies that fall victim to cybersecurity breaches and cyber attacks bear responsibility for protecting themselves against such attacks and their harmful consequences.[96] Yang and Hoffstadt argue that the victim-company would be forced to absorb losses and might incur additional losses if it were sued for failing to secure its intellectual property and computer systems.[97] Such lawsuits may seek tort relief for breach of the duty of care to maintain a secure network or a breach of fiduciary duty to keep data secure.[98] Recently, the Third Circuit upheld a suit brought by the Federal Trade Commission against the Wyndham hotel chain in which the FTC argued that Wyndham's failure to undertake adequate cybersecurity measures—failure that resulted in hackers carrying out three cybersecurity attacks against the hotel chain and stealing personal information stored by Wyndham about its guests[99]—constituted an "unfair business practice." Judge Ambro, writing for the court, rejected Wyndham's three arguments against finding of unfairness. First, the court held that unfair conduct need not necessarily be unscrupulous or unethical.[100] Second, the court ruled that even if one were to accept Wyndham's argument equating "unfair" with "not equitable," a company "does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business."[101] Finally, the court rejected Wyndham's con-

95. *Id.*

96. Debra Wong Yang & Brian M. Hoffstadt, *Countering the Cyber-Crime Threat*, 43 AM. CRIM. L. REV. 201, 207–08 (2006).

97. *See id.* at 207. *See, e.g.*, Complaint at 4, Parke v. Cardsystems Sols., Inc., No. CGC-05-442624 (Cal. Super. Ct., June 27, 2005); Class Action Complaint, Goldberg v. ChoicePoint, Inc., No. BC329115 (Cal. Super. Ct., Feb. 18, 2005).

98. Yang & Hoffstadt, *supra* note 96, at 208. This will, arguably, incentivize companies to take measures to prevent cyber attacks. Hardware and software manufacturers are generally shielded from liability because they condition the use of their product on the acceptance of a licensing agreement that absolves them of most forms of liability for design defects that result in future vulnerabilities to users' computers. *Id.* at 208–09.

99. Fed. Trade Comm'n v. Wyndham Worldwide Corp. et al, 799 F.3d 236, 241–42 (2015).

100. *Id.* at 244–45.

101. *Id.* at 245.

tention that a business "does not treat its customers in an 'unfair' manner when the business *itself* is victimized by criminals."[102] Thus, the court concluded, Wyndham's alleged conduct fell within the plain meaning of unfair and was subject to regulation under Section 45(a) of the Federal Trade Commission Act of 1914.[103]

Some scholars have advocated the implementation of a "cybersecurity negligence" standard, as "a means of determining liability for companies who suffer damage from lax cybersecurity."[104] Applying this formula to DAS, however, allows weaker states to implement weaker standards, which is problematic given the interconnected nature of cyberspace, and the ability of cyber threats to penetrate networks through weak links in the interconnected chain. Other scholars support a heightened degree of *mens rea* before imposing obligations or liability upon an institution for failing to prevent a cyber attack. Yet others caution against implementing anything less than an actual knowledge or willful blindness standard. While some may support a "constructive knowledge" standard for holding institutions accountable, Michael Schmitt argues that

> [a]s the means of cyber identification and attribution are typically classified . . . states will be reticent to reveal their capabilities[, making] it highly problematic to determine with some certainty whether a particular state's technical capabilities are at a level at which the offending cyber operations should . . . have been identified and attributed.[105]

The issue of the liability of private corporations and non-state actors for damage caused to them and others as a result of their failure to undertake appropriate cybersecurity measures and put in place robust defenses against harmful cyber incidents, whether man-made or not, is of particular relevance to this discussion. On the one hand, non-state actors often find themselves on the "cyber frontline."[106] Cyber defense does not occur in a

---

102. *Id.* at 246.

103. *Id.* at 247. *See also* David Fagan, John Grabert, Kurt Wimmer and Caleb Skeath, *5 Things Every GC Should Know about Wyndham*, CORP. COUNSEL (Oct. 16, 2015), http://www.corpcounsel.com/id=1202740035068/5-Things-Every-GC-Should-Know-about-Wyndham?slreturn=20150919093615 (noting that the court's ruling "reaffirms the FTC's authority to bring unfairness actions on the basis of 'likely' substantial injury to consumers, even if no such injuries have actually occurred . . . the actions of hackers and other intervening criminal actors may not immunize companies from FTC data security enforcement actions"); Paul Rosenzweig, *The FTC Takes Charge–FTC v. Wyndham*, LAWFARE BLOG (Aug. 26, 2015), https://www.lawfareblog.com/ftc-takes-charge-ftc-v-wyndham ("The FTC now owns cybersecurity in the private sector . . . we've converted a consumer protection mandate into a cybersecurity obligation and assigned that role to an independent agency."); Sheppard Mullin Richter & Hampton LLP, *FTC v. Wyndham: The Third Circuit Recognizes FTC Authority to Regulate Commercial Cyber Security Practices*, NAT'L L. REV. (Sept. 29, 2015), http://www.natlawreview.com/article/ftc-v-wyndham-third-circuit-recognizes-ftc-authority-to-regulate-commercial-cyber ("All web-facing companies which collect personally identifiable information are on notice that they routinely must maintain the integrity and security of such consumer data.").

104. Shackelford et. al., *supra* note 28, at 313.

105. Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?*, 25 STAN. L. & POL'Y REV. 269, 278 (2014).

106. Carter, *supra* note 13. Secretary Carter explained:

"neutral space" but inside organizational networks.[107] It depends on the organization—its use of technologies, and its will and ability to protect, cooperate, and collaborate with other organizations and the state—to be successful. At the same time, the gamut of non-state actors whose actions or omissions affect states are not limited to the territory of any one particular state.

Before turning to examine briefly the possible sources and scope of DAS responsibility, I should note that while there are significant developments taking place towards the recognition of the duties discussed in the remainder of this Article as a matter of positive, existing international law, many such duties belong to the realm of *lex ferenda* rather than form obligations *de lege lata*.

III. Responsibility of DAS Before, During, and After Cybersecurity Incidents

A. Responsibility of DAS Before Cybersecurity Incidents

States have sovereign authority over infrastructure and activities within their territory.[108] Although no state can claim sovereignty over cyberspace as such, states may exercise sovereign prerogatives over cyber infrastructure that is physically located, and activities that take place, in their territory.[109] No state, however, is able or expected, regardless of its level of technological sophistication and commitment of human resources and funds, to foolproof its systems against cybersecurity incidents.[110] ICT and their related systems and infrastructures are interconnected globally, which means that prevention cannot be fully accomplished on a local, national level. Inter-state cooperation is needed. Not only is such cooperation lacking on the state level at present,[111] but even if it were attained, non-state actors could still be able to carry out cyber attacks[112] and natu-

> While we in DoD are an attractive target, the cyber threat is one we all face . . . as institutions, and as individuals. Networks nationwide are scanned millions of times a day. And as we've seen cyber attackers bombard the public websites of banks, make off with customer data from retailers, try to access critical infrastructure networks, and steal research and intellectual property from universities and businesses alike . . . so too have individual citizens been compelled to guard against identity theft.

107. I thank Amit Ashkenazi for raising this point when commenting on an earlier draft of this Article.

108. TALLINN MANUAL, *supra* note 53, at 15–23.

109. *Id.*

110. Zoë Baird, *Foreword*, *in* CYBER SECURITY: TURNING NATIONAL SOLUTIONS INTO INTERNATIONAL COOPERATION vii, vii (James A. Lewis ed., 2003).

111. *See* James A. Lewis, *Introduction*, *in* CYBER SECURITY: TURNING NATIONAL SOLUTIONS INTO INTERNATIONAL COOPERATION xi, xi–xii (James A. Lewis ed., 2003). *See also* Michael Vatis, *International Cyber-Security Cooperation, Informal Bilateral Models*, *in* CYBER SECURITY: TURNING NATIONAL SOLUTIONS INTO INTERNATIONAL COOPERATION 1, 1–4 (James A. Lewis ed., 2003).

112. The U.S. Department of Defense's Cyber Strategy clearly points out:

> In addition to state-based threats, non-state actors like the Islamic State in Iraq and the Levant (ISIL) use cyberspace to recruit fighters and disseminate propaganda and have declared their intent to acquire disruptive and destructive cyber

ral disasters would still pose problems of catastrophic proportions. Furthermore, cybersecurity incidents may happen very quickly, even automatically, impacting a large number of victims at the same time.[113] Attacks can be carried out cheaply[114]—or cost nothing in the case of a natural disaster—while establishing robust defenses against cybersecurity incidents is costly and complex, limiting the capacity and willingness of many countries around the world to undertake such measures.[115]

States may be expected to exercise due diligence[116] and establish feasible, primarily passive defenses against cybersecurity incidents.[117] Passive defenses include system access controls that prevent unauthorized users from getting into a system and force authorized users to be security-conscious,[118] data access controls that are aimed at the data and programs

---

> capabilities. Criminal actors pose a considerable threat in cyberspace, particularly to financial institutions, and ideological groups often use hackers to further their political objectives. State and non-state threats often also blend together; patriotic entities often act as cyber surrogates for states, and non-state entities can provide cover for state-based operators. This behavior can make attribution more difficult and increases the chance of miscalculation.

DOD CYBER STRATEGY, *supra* note 34, at 9.

113. Gregory C. Wilshusen & David A. Powner, U.S. GOV'T ACCOUNTABILITY OFF., GAO 10-230T, CONTINUED EFFORTS ARE NEEDED TO PROTECT INFORMATION SYSTEMS FROM EVOLVING THREATS 5 (2009).

114. Stephen E. Henderson & Matthew E. Yarbrough, *Suing the Insecure?: A Duty of Care in Cyberspace*, 32 N.M. L. REV. 11, 22 (2002); William J. Lynn, *Defending a New Domain: The Pentagon's Cyberstrategy*, 89 FOREIGN AFF. 97, 98 (2010).

115. Most developing countries do not have a telecommunications sector capable of supporting ICT. The digital divide is most extreme in Asia, with some countries having seventy percent of households connected to the Internet (like South Korea, Japan, Hong Kong, and Singapore) and less than one percent in others (like Laos, Cambodia, Mongolia, and Myanmar). *See, e.g.*, Roderic Broadhurst, *Developments in the Global Law Enforcement of Cyber-Crime*, 29 POLICING: AN INT'L J. OF POLICE STRATEGIES & MGMT. 408, 410–11 (2006). The 2013 Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security called on member states to engage in capacity building efforts to assist developing countries to build the required skills to protect their networks and citizens. U.N. Doc. A/68/98, *supra* note 53.

116. For a recent discussion of the concept of due diligence in the context of "a state's legal responsibilities when cyber infrastructure located on its territory is used by another state—or by non-state actors, such as hacker groups, individual hacktivists, organized armed groups, or terrorists—to mount the operations," see Schmitt, *supra* note 78, at 68.

117. For an overview of proactive mechanisms, reactive mechanisms, and design and analysis principles, see Alvaro A. Cárdenas et al., *Secure Control: Towards Survivable Cyber-Physical Systems*, 28TH INT'L CONF. ON DISTRIBUTED COMPUTING SYS. WORKSOPS 495, 496–98 (2008). *See also* Andrea Atzeni & Antonio Lioy, *Why to Adopt a Security Metric? A Brief Survey*, *in* QUALITY OF PROTECTION 6–9 (2006); Dennis Edwards et al., *Prevention, Detection and Recovery from Cyber-Attacks Using a Multilevel Agent Architecture*, *in* SYSTEM OF SYSTEMS ENGINEERING 1 (2007) (providing a technical description of how intelligent software agents could improve cyber-security); Barbara Endicott-Popovsky & Deb Fincke, ADDING THE FOURTH "R": A SYSTEMS APPROACH TO SOLVING THE HACKER'S ARMS RACE 8 (2006).

118. Examples of system access controls include a username and password, electronic keys, tokens, badges, and smart cards, as well as biometric or behavioral pass codes including fingerprints, handprints, retina patterns, iris patterns, voice, signatures, or keystroke patterns. Other systems use transmission encryption, challenge response pro-

inside the system instead of access controls,[119] security administration (security policies, training, and audits to ensure protection),[120] and security system design that uses hardware and software to protect the system.[121] They may also include mechanisms that would facilitate timely warnings against cyber threats and security incidents. It is worth noting that employment by states or private companies[122] of more active self-help measures—such as "hackbacks"—that are designed to disable, counterattack, or even destroy the attacker's own system in response to cyber attacks raises serious legal challenges both as a matter of domestic law[123] and of the international law of armed conflict.[124]

States ought also to engage in a robust resilience planning[125] that involves, among other things, building up redundant systems,[126] offline backups, and parallel networks,[127] as well as enhancing system interoperability to improve sharing of critical information, and developing of alter-

---

cedures, and password controls. 2 RICK LEHTINEN ET AL., COMPUTER SECURITY BASICS 49–62 (2006).

119. *Id.* at 50.

120. *Id.* at 96–98.

121. Examples include anti-virus, encryption, firewalls, and intrusion detection programs. *Id.* at 50, 92–93, 189–91. *See also* TIMOTHY SHIMEALL & JONATHAN SPRING, INTRODUCTION TO INFORMATION SECURITY: A STRATEGIC-BASED APPROACH (2013) (organizing cyber defense measures around four defensive strategies: deception, frustration, resistance, and recognition and recovery).

122. *See generally* Jan E. Messerschmidt, *Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm*, 52 COLUM. J. TRANSNAT'L L. 275 (2013); Zach West, *Young Fella, If You're Looking for Trouble I'll Accommodate You: Deputizing Private Companies for the Use of Hackback*, 63 SYRACUSE L. REV. 119 (2012).

123. Remarks by Assistant Attorney General Leslie R. Caldwell at the Georgetown Cybersecurity Law Institute (May 20, 2015), http://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-georgetown-cybersecurity (discussing "the use of ostensibly defensive measures, such as 'hacking back' into an attacker's system either to punish an attacker or to retrieve or delete stolen data," and concluding that not only are such measures prohibited under the Computer Fraud and Abuse Act but that "sound policy also militates against use of hackback tactics"). According to Caldwell, such "sound policy" arguments include the significant risk to innocent third parties, interference with ongoing government investigations, and detrimental effect on U.S. foreign relations, as well as the "low likelihood of being beneficial." *See generally* Yang, *supra* note 96 (examining the legality of hackbacks under U.S. domestic law).

124. Jensen, *supra* note 65, at 1566 n.205. *See generally* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429 (2012) (examining tactics such as hackbacks under the law of armed conflict); Sklerov, *supra* note 55 (same).

125. *See generally* JUDITH RODIN, THE RESILIENCE DIVIDEND: MANAGING DISRUPTION, AVOIDING DISASTER, AND GROWING STRONGER IN AN UNPREDICTABLE WORLD (2014).

126. DOD CYBER STRATEGY, *supra* note 34, at 11 ("Because the Defense Department's capabilities cannot necessarily guarantee that every cyberattack will be denied successfully, the Defense Department must invest in resilient and redundant systems so that it may continue its operations in the face of disruptive or destructive cyberattacks on DoD networks.").

127. *See* Robert Westervelt, *Kaspersky: Redundancy, Offline Backup Critical for Cyberdefense*, CRN (Feb. 8, 2013), http://www.crn.com/news/security/240148219/kaspersky-redundancy-offline-backup-critical-for-cyberdefense.htm.

native capabilities to protect against disruptions in the primary systems.[128] In a similar vein, the International Law Commission's (ILC) work on draft articles on the Protection of Persons in the Event of Disasters has recently adopted the idea of disaster risk reduction and seeks to impose on all states the obligation to reduce the risk of disasters by taking the necessary and appropriate measures, including through legislation and regulations, to prevent, mitigate, and prepare for disasters.[129] Such disaster risk reduction measures would include the "conduct of risk assessments, the collection and dissemination of risk and past loss information, and the installation and operation of early warning systems."[130] As the ILC explains, the obligation to reduce the risk of disasters covers not only the response phase of a disaster, but also the "pre-disaster duties of States."[131] Quoting from the 2005 Hyogo Declaration,[132] the ILC's commentary on draft article 11 notes that

> a culture of disaster prevention and resilience, and associated pre-disaster strategies, which are sound investments, must be fostered at all levels, ranging from the individual to the international levels . . . . Disaster risks, hazards and their impacts pose a threat, but appropriate response to this can and should lead to actions to reduce risks and vulnerabilities in the future.[133]

Resiliency[134] relates to the ability to adapt and respond rapidly to disruptions and maintain continuity of operations.[135] It requires preparing for potential threats to the continued functioning of computer networks and delivery of critical services.[136] As Secretary Carter suggested, "[w]e have to . . . conduct exercises in resiliency . . . so that if a cyberattack degrades our usual capabilities, we can still mobilize, deploy, and operate our forces in other domains—air, land, and sea—despite the attack."[137] For its part, redundancy is a critical component in resiliency planning.

128. *See Presidential Policy Directive*, *supra* note 5.

129. *See* Rep. of the Int'l Law Comm'n, 66th Sess., May 5–June 6, July 7–Aug. 8, 2014, U.N. Doc. A/69/10, Ch. V [hereinafter ILC Report].

130. *Id.* at 88.

131. *Id.* at 111.

132. World Conference on Disaster Reduction, *Hyogo Declaration*, ¶ 3, U.N. Doc. A/CONF.206/6 (Jan. 18–22, 2005).

133. ILC Report, *supra* note 129, at 112. Similarly, the ILC quotes the concluding summary by the Chair of the fourth session of the Global Platform for Disaster Risk Reduction (2013) noting the "growing recognition that the prevention and reduction of disaster risk is a legal obligation, encompassing risks assessments, the establishment of early warning systems, and the right to access risk information." *Id.*

134. Other terms have been used to express similar ideas such as robustness, reconstitution, recovery, resourcefulness, adaptability, reliability, and mission assurance. *See generally* Nicholas J. Multary & Christopher S. Oehmen, *Building the Theory of Resilience*, PAC. NW. NAT'L LABORATORY, http://cybersecurity.pnnl.gov/documents/Theory_of_Resilience-V15.pdf.

135. Hugh Boyes, *Resilience and Cyber Security of Technology in the Built Environment*, INST. OF ENGINEERING & TECH. (2013), http://www.cpni.gov.uk/documents/publications/2013/2013063-resilience_cyber_security_technology_built_environment.pdf?epslanguage=EN-gb.

136. *Id.*

137. Carter, *supra* note 13.

Redundancy is crucial to achieving safety of ICT systems and ensuring that critical infrastructures that depend on ICT systems continue to function during a cybersecurity incident, as redundancy mitigates possible attacks against, or breakdowns of, a single point of failure.[138]

Implementing defenses and measures as noted above may not be easy. Existing poor cyber hygiene[139] is exacerbated by the fact that new vulnerabilities are easily discovered and exploited.[140] This is especially true in the context of commercial-off-the-shelf (COTS) and public domain products, whose structure is widely available and can be readily analyzed by attackers.[141] Continuous monitoring of potential threats is expensive both in financial terms and in terms of the necessary human resources. Such continuous monitoring may be extremely difficult or even impossible to perform for many states around the world who lack the financial wherewithal and the required technological capacities.[142]

In addition to technological mechanisms to prevent or minimize harm resulting from cybersecurity incidents, DAS may also be expected to ensure that the proper legal measures are put in place. For example, state practice of treating cyber attacks as criminal offenses under domestic law seems to reflect recognition of the duty to prevent cyber attacks.[143] Improving a nation's cyber detection, attribution, and punishment capabilities may, in turn, "make cyber espionage [and attacks] so costly that [they] no longer

138. *See, e.g.*, Arquilla, *supra* note 27. *See also* Shane Harris, *Exclusive: Meet the Fed's First Line of Defense Against Cyber Attacks*, FOREIGN POL'Y (Apr. 29, 2014), http://www.foreignpolicy.com/articles/2014/04/28/exclusivemeet_the_secret_fed_cyber_security_unit_keeping_trillions_of_dollars_s.

139. Gen. Keith B. Alexander, *Building a New Command in Cyberspace*, STRATEGIC STUD. Q. 3, 6 (2011), http://www.au.af.mil/au/ssq/2011/summer/summer11.pdf. Poor hygiene may result from poor systems administration (for example, failure to install security and safety updates, failure to maintain proper firewalls and update virus definitions). See Shackelford, *supra* note 47, at 982, as well as from the fact that implementation of defenses against cybersecurity incidents may get in the way of developing new systems and responding to user requests. *See also* Sara Kraemer & Pascale Carayon, *Human Errors and Violations in Computer and Information Security: The Viewpoint of Network Administrators and Security Specialists*, 38 APPLIED ERGONOMICS 143, 143–44 (2007).

140. Matthew Miller et al., *Why Your Intuition About Cyber Warfare Is Probably Wrong*, SMALL WARS J. 4 (2012), http://smallwarsjournal.com/jrnl/art/why-your-intuition-about-cyber-warfare-is-probably-wrong.

141. YURCIK & DOSS, *supra* note 47, at 5. Production of COTS is often rushed to the market with multiple, existing system vulnerabilities, referred to as "technical debt." Shackelford, *supra* note 47, at 982. Furthermore, most softwares are tested by the penetrate-and-patch approach, whereby someone finds an exploitable security "hole" and the software manufacturer issues a patch. This leaves many vulnerabilities in the software. YURCIK & DOSS, *supra* note 47, at 5.

142. For discussion of the links between the legal obligation of due diligence and states' capabilities, see, e.g., Schmitt, *supra* note 78, at 74–76. *See also* Oren Gross, *The New Way of War: Is There a Duty to Use Drones?*, 67 FLA. L. REV. 1, 62–68 (2015) (discussing the possibility of applying differential rules to the law of armed conflict; in other words, imposing different normative obligations on different states based on each nation's capabilities).

143. CARR, *supra* note 11, at 64.

pay to execute."[144] If there is a high probability that cyber attackers are detected, identified, and effectively punished by "sanctions, civil litigation, or otherwise," there is far smaller incentive to carry through with an attack.[145] Indeed, the implementation of robust criminal justice penalties for cyber attacks is supported by the World Economic Forum.[146] Yet, whether existing state practice amounts to a norm of customary international law is a matter of some contention,[147] especially in light of failure by many states to enforce the law on the books.[148]

The duty to warn of an impending disaster is not a new concept, "[especially after] man-made disasters, such as the Chernobyl meltdown and the Sandoz spill."[149] Indeed, it has been suggested that the International Court of Justice's decision in the *Corfu Channel Case* provides the basis for a general duty to warn other states of potential or impending harm.[150] In the context of cybersecurity threats, however, such a duty to warn is further complicated by two factors. First, DAS may not actually realize that they have fallen victim to an attack or a cybersecurity incident[151] and may also not be able to recognize threats to their ICT systems in a timely and meaningful manner. Second, the scope of the warning that is due (for example, how much information to disclose) may be problematic insofar as much of the pertinent information may be closely linked to the DAS' own national security interests and concerns.[152] In either case, the identity of the source of the cyber attack may well remain unknown.[153]

B. Responsibility of DAS During Cybersecurity Incidents

When prevention has not been successful and a state faces a cybersecurity incident, it bears the responsibility—both to its own citizens and to other states, and perhaps even non-state actors—to identify expeditiously and effectively the nature of the security risk, assess the harm, pri-

144. Melanie Teplinsky, *Cybersecurity and the Cyberthreat Deterrence Trend*, THOMSON REUTERS/ASPATORE, 2015 WL 4512303 at 4 (June 2015).

145. *Id. See also* DOD CYBER STRATEGY, *supra* note 34, at 10–12 (detailing the need and the guidelines for a comprehensive cyber deterrence strategy to deter key state and non-state actors from conducting cyber attacks against U.S. interests).

146. RISK AND RESPONSIBILITY, *supra* note 16, at 9 (advocating for an "end-to-end criminal justice system [giving] law enforcement . . . the capability and resources to investigate cybercrimes and to have an appropriate, comprehensive and agile legal code to support its investigate and prosecutorial activities").

147. *See id.* at 65.

148. *See* Sklerov, *supra* note 55, at 9–10.

149. Tyra Ruth Saechao, Note, *Natural Disasters and the Responsibility to Protect: From Chaos to Clarity*, 32 BROOKLYN J. INT'L L. 663, 681 (2007). In both of these examples, however, neither the Soviet Union nor Switzerland, respectively, faced international legal consequences for their failure to notify adversely affected neighboring states. Devereaux F. McClatchey, *Chernobyl and Sandoz One Decade Later: The Evolution of State Responsibility for International Disasters, 1986-1996,* 25 GA. J. INT'L & COMP. L. 659, 664–65 (1996).

150. *Id. See also* The Corfu Channel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4 (Apr. 9).

151. Buckland, *supra* note 55.

152. *Id.* at 27.

153. *Id.* at 23–24.

oritize plans of action to overcome the danger, manage remedial plans as they are put into action, mitigate damage that has been caused as a result of the incident, and engage in short-term recovery.

DAS may face certain limitations, both technological and legal, in responding to a cybersecurity incident. Even the best detection and monitoring programs are unable to detect all cyber incidents. Indeed, a DAS may not even realize that it has been the object of a cybersecurity incident or, alternatively, may face challenges in differentiating between legitimate operations, intrusive marketing, hacker mischief, competitor attacks, criminal activity, and cyber terrorism.[154] Assessing the harm and damage wrought by the security incident in order to prioritize plans of action to overcome the danger and manage remedial plans, as well as to put in place measures to mitigate the harm, may be similarly difficult.[155]

Identifying the source of the security incident may be nearly impossible in some cases—mostly when the cause of the incident is malicious.[156] "Sophisticated attacks by knowledgeable operators, whether private or state-sponsored, are almost impossible to trace using modern practices."[157] Ascertaining conclusively the identity of an attacker requires an intensive, time-consuming investigation and the help of the state of origin of the cyber attack.[158] The difficulties inherent in identifying the source of a cyber attack and, where relevant, attributing the attack to the appropriate

154. Stephen Hinde, *Cyber-terrorism in Context*, 22 COMPUTERS & SECURITY 188, 188 (2003).

155. *See id.* at 192.

156. Messerschmidt, *supra* note 122, at 285 ("The current packet architecture of the core TCP/IP protocols does not provide an authentication mechanism for individual packets, making it nearly impossible to verify a sender's identity."). The inability to attribute a cyber attack to a particular state has, of course, critical ramifications as far as the jus ad bellum is concerned, for even if the particular attack could be regarded as amounting to an armed attack for purposes of article 51 of the Charter of the United Nations, if it cannot be attributed satisfactorily, then the victim state may not be able to exercise its right to self-defense. *See, e.g.*, Michael Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 892, 928–29 (1999); Michael N. Schmitt, *Cyber Operations and the* Jus ad Bellum *Revisited*, 56 VILL. L. REV. 569, 586–87 (2011).

157. Shackelford, *supra* note 47, at 981. *See also* Howard F. Lipson, *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*, CERT COORDINATION CTR. 13–15 (2002), http://www.dtic.mil/dtic/tr/fulltext/u2/a408853.pdf (discussing the inherent weaknesses in the design of the Internet); TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 252 (William A. Owens et al. eds., 2009). The Committee on Offensive Information Warfare notes:

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

Id. See also Brenner, *supra* note 47 (detailing attribution of attacks and attackers).

158. *See* Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. INT'L L. & POL. 57, 97–99 (2001).

state or non-state actors, emphasize yet again the need for close partnership between governments and the private sector. As Secretary Carter noted recently:

> We like to deter malicious action before it happens, and we like to be able to defend against incoming attacks—as well as pinpoint where an attack came from. We've gotten better at that because of strong partnerships across the government, and because of private-sector security researchers like FireEye, Crowdstrike, HP—when they out a group of malicious cyber attackers, we take notice and share that information.[159]

The challenges and limitations of dealing with cybersecurity incidents alone, and the impact that such incidents may have on DAS' own populations, other countries, and non-state actors, suggest that any discussion of legal duties of DAS will be founded on notions of cooperation.[160] Such notions, which focus on conduct rather than on outcome,[161] and which ought to be balanced against sovereign prerogatives of states,[162] have found their way into numerous international treaties.[163] Yet, at present they have not attained the status of customary international legal norms. Generally, the duty to cooperate "must be understood as encompassing a great variety of coordinating, technical, scientific and logistical activities."[164] Thus, for example, in the area of responding to natural disasters, international agreements have referred to coordinating communications and information sharing,[165] addressing regulatory barriers to entry of foreign personnel and relief equipment,[166] and extending scientific and technical expertise.[167]

The challenges and limitations of dealing with cybersecurity incidents, especially when one considers that an incident may impact a DAS' own population as well as other countries and non-state actors, suggest that at a minimum DAS ought to report the incident and share relevant information with other relevant actors. Indeed, "coordination of communication and exchange of information is [sic] essential to effective disaster response."[168] Thus, some writers propose "cyber incident thresholds"

159. Carter, *supra* note 13.

160. Pierre-Marie Dupuy & Jorge E. Viñuales, International Environmental Law 64–66 (2015).

161. Eduardo Valencia-Ospina (Special Rapporteur on the Protection of Persons in the Event of Disasters), *Fifth Rep. on the Protection of Persons in the Event of Disasters*, 22–24, U.N. Doc. A/CN.4/652 (Apr. 9, 2012) [hereinafter Valencia-Ospina V].

162. *Compare* U.N. Charter art. 1, ¶ 3, *with* U.N. Charter art. 2, ¶ 1.

163. *See, e.g.*, U.N. Charter art. 1, ¶ 3; United Nations Convention on the Law of the Sea art. 303, Dec. 10, 1982, 1833 U.N.T.S. 397; Convention on the Rights of the Child, Sept. 2, 1990, 1577 U.N.T.S. 3; Convention on Cybercrime, Nov. 23, 2001, 13174 T.I.A.S. 1; G.A. Res. 2625 (XXV), Friendly Relations Declaration, U.N. Doc. A/RES/25/2625 (Oct. 24, 1970); United Nations Conference on the Human Environment, *Stockholm Declaration*, U.N. Doc. A/CONF.48/14/Rev.1 (June 5–16, 1972) (emphasizing the importance of international cooperation).

164. Valencia-Ospina V, *supra* note 161, at para. 93.

165. *Id.* at paras. 101–03.

166. *Id.* at paras. 106–13.

167. *Id.* at paras. 104–05.

168. *Id.* at para. 101.

that, when crossed, mandate reporting.[169] It is also worth noting that in those cases when cyber attacks are involved that would constitute not only an impermissible use of force, but amount to an armed attack for purposes of article 51 of the U.N. Charter,[170] a DAS who wishes to exercise its right of self-defense would have to notify the Security Council of the armed attack.[171] President Obama's Policy Directive on Critical Infrastructure Security and Resilience recognizes the critical role of information sharing in preparing for, and responding to, cybersecurity incidents.[172] The Directive, looking only at the domestic scene, emphasizes that "a secure, functioning, and resilient critical infrastructure requires the efficient exchange of information, including intelligence, between all levels of governments and critical infrastructure owners and operators."[173] Such information sharing "must facilitate the timely exchange of threat and vulnerability information as well as information that allows for the development of a situational awareness capability during incidents."[174] Information sharing is no less critical on the international level.

The content and scope of reporting and notification are less clear. First, it is not entirely clear who may be the recipient of such reports and notifications—other states, or also non-state actors such as private companies, international organizations, and even individuals. Non-state actors may be affected by the incident and may also be able to supply much required assistance to overcome the cybersecurity incident and mitigate its harmful consequences. Second, the substantive content of the report and notification are similarly unclear.[175] A laconic statement—"we have been the object of a cybersecurity incident"—neither offers much guidance to others who may be potentially harmed by the incident, nor directs them towards meaningful ways to assist the DAS. On the other hand, cybersecurity incidents may involve significant national security interests of the DAS, which it will be reluctant to expose publicly.[176] The close interconnectedness of the civilian and military cyber infrastructures means inevitably that much information about the incidents may be withheld for

169. *See* Buckland, *supra* note 55, at 27. This, however, would not apply to large groups of low-level events that together, have a large impact. *Cf. id.* at 27.

170. As is the case with definitions of the basic terms, there is no consensus with respect to the question: "when does a cyber incident rise to the level of an armed attack for purposes of article 51 of the UN Charter?" *See, e.g.*, ANTONIA CHAYES, BORDERLESS WARS: CIVIL MILITARY DISORDER AND LEGAL UNCERTAINTY 130–71 (2015); Antonia Chayes, *Rethinking Warfare: The Ambiguity of Cyber Attacks*, 6 HARV. NAT'L SECURITY J. 474 (2015); Priyanka R. Dev, *"Use of Force" and "Armed Attacks" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response,* 50 TEX. INT'L L.J. 381 (2015); Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817 (2012); Nguyen, *supra* note 48; Roberts, *supra* note 29.

171. U.N. Charter art. 51.

172. *See Presidential Policy Directive*, *supra* note 5.

173. *Id.* at 6.

174. *Id.*

175. *See* Valencia-Ospina V, *supra* note 161, at paras. 102–03.

176. *See* Buckland, *supra* note 55, at 27.

national security reasons.[177] Revealing the very existence of the incident may also entail significant embarrassment to DAS—who failed to prevent the threat from materializing. Information sharing also raises weighty issues of privacy and concerns for infringement on civil rights and liberties, especially when such information is shared with foreign entities. Thus, limitations and restrictions on the content, structure, and type of information shared, as well as the timeliness of such act of sharing, may undermine the ability to gain and acquire real-time situational awareness.

Another set of thorny questions arises in the context of external intervention in the aftermath of a cybersecurity incident. While extension of such concepts as the responsibility to protect to cybersecurity incidents may seem, at present, unwarranted,[178] other bases may be relevant in examining external interventions in instances of cybersecurity incidents. States have been helping each other in the wake of natural disasters—earthquakes, floods, tsunamis, typhoons, hurricanes, volcanoes, and droughts—for centuries, yet confusion and lack of coordination define the current system of natural disaster response.[179] Some of the questions that come up in the context of responding to natural disasters are also relevant to cybersecurity incidents for the reasons elaborated above. In the context of the responsibilities of DAS in particular, the following questions ought to be addressed: does a DAS have an obligation to seek assistance in order to deal with such incidents? Does it have an obligation to accept offers of assistance and help if, and when, those are made by other states or non-state actors?[180] Should other states—and perhaps even non-state actors—be entitled, or perhaps, even have a duty to intervene in the DAS, when the latter is technologically unable or politically unwilling to address the security incident and its ramifications in a timely, effective, and comprehensive manner?[181]

---

177. *See id.*; Jeffrey T.G. Kelsey, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, 106 MICH. L. REV. 1427, 1432 (2008).

178. *See* U.N. Secretary-General, *Implementing the Responsibility to Protect*, ¶ 10(b), U.N. Doc. A/63/677 (Jan. 12, 2009) (limiting the application of R2P ideas to four specific crimes: genocide, war crimes, ethnic cleansing, and crimes against humanity).

179. *See* David P. Fidler, *Disaster Relief and Governance After the Indian Ocean Tsunami: What Role for International Law?*, 6 MELB. J. INT'L L. 458, 459 (2005); Alejandra de Urioste, *When Will Help Be on the Way? The Status of International Disaster Response Law*, 15 TUL. J. INT'L & COMP. L. 181, 183–85, 194 (2006); Saechao, *supra* note 149, at 665–66.

180. *See also* Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARV. INT'L L. J. 374, 408–25 (2011) (discussing a "duty to assist" network for victims of the most severe cyber threats). A concomitant issue, outside the scope of this Article, is if other states and non-state actors should have the right to intervene even in the absence of DAS' consent to overcome an incident that may affect their own interests, such as when a DAS is technologically unable or politically unwilling to address effectively and comprehensively the risk that is presented by the incident.

181. *See, e.g.*, Council Regulation 1257/96,1996 O.J. (L 163) 1 (EU) (stating that, "people in distress, victims of natural disasters, wars and outbreaks of fighting, *or other comparable exceptional circumstances* have a right to international humanitarian assistance where their own authorities prove unable to provide effective relief") (emphasis added).

Instructive parallels may be drawn from the International Law Commission's work on protecting persons in the event of a disaster. A significant part of its efforts has been directed at establishing the legal duties of states affected by such disasters.[182] The ILC's draft article 12 of the draft articles on the Protection of Persons in the Event of Disasters establishes an effected state's duty to ensure both the protection of persons and to ensure the provision of disaster relief and assistance on its territory.[183] Draft article 13 deals with a duty of the affected state to seek external assistance and provides that, "[t]o the extent that a disaster exceeds its national response capacity, the affected State has the duty to seek assistance from among other States, the United Nations, other competent intergovernmental organizations and relevant non-governmental organizations, as appropriate."[184] In the context of natural disasters, a duty to seek assistance may derive primarily from international human rights law. In the case of cybersecurity incidents, this duty can also be based on the notion of a duty to cooperate[185] and duty to prevent trans-boundary harm to other states.[186]

Imposing duties on DAS to seek and accept assistance is, to a certain degree, in tension with traditional notions of sovereign rights and prerogatives. It is thus not surprising that even in the context of catastrophic natural disaster, some states are weary of couching obligations in legal terms, preferring instead to use hortatory formulations such as "should seek assistance."[187] Indeed, even those who accept as desirable a legal duty on DAS to seek and accept assistance recognize the ability of affected states to impose certain conditions on the provision of external assistance.[188]

One important condition that the ILC raises in the context of natural disasters and whose significance and challenges are likely to be amplified

182. *See generally* ILC Report, *supra* note 129.

183. *Id.* at 117–19.

184. *Id.* at 119–23. The duty of the affected state to accept external assistance is qualified by draft articles 14 and 15 that provide, respectively, that the provision of external assistance requires the consent of the affected State (which shall not be withheld arbitrarily), and that the affected state may place conditions on the provision of external assistance. *Id.* at 123–26, 127–29.

185. DUPUY & VIÑUALES, *supra* note 160, at 64–66. *See also* Int'l Law Comm'n Rep. on the Work of Its Sixty-Second Session, U.N. Doc. A/65/10, at 327–30 (2010) (discussing the duty to cooperate in the context of protecting persons in the event of disasters).

186. See discussion *supra* notes 75–89 and the accompanying text. *See also* Int'l Law Comm'n Rep. on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10, at 372 (2001); Eduardo Valencia-Ospina (Special Rapporteur on the Protection of Persons in the Event of Disasters), *Sixth Rep. on the Protection of Persons in the Event of Disasters*, 5–25, U.N. Doc. A/CN.4/662 (May 3, 2013) (analyzing the principle of prevention in human rights law and international environmental law); DUPUY & VIÑUALES, *supra* note 160, at 55–61 (discussing the principles of "no harm" and prevention in the context of international environmental law); XUE HANQIN, TRANSBOUNDARY DAMAGE IN INTERNATIONAL LAW (2009).

187. *See* Valencia-Ospina V, *supra* note 161, at para 28.

188. *See id.* at paras. 117–81. In his report, the Special Rapporteur states that "any condition imposed by the affected State must be reasonable and must not undermine the duty to ensure protection of persons on its territory." *Id.* at para. 119. He also emphasizes that the affected state "has a corresponding duty to facilitate the prompt and effective delivery of assistance." *Id.*

in the context of cybersecurity incidents pertains to identifying needs and quality control.[189] In the context of natural disasters the ILC emphasizes the discretionary power of the affected state to choose the assistance that is "most appropriate to its specific needs"—taking into consideration the gravity of the emergency to frame appropriate response policies.[190] Yet in the context of cybersecurity incidents, the principle of needs-based allocation of assistance is likely to be much harder to implement because the DAS may not actually know that it has been attacked. It may also be extremely difficult—if not downright impossible—to assess the scope of the dangers, the risks involved, and the likely harms that may entail to the DAS itself, its citizens, and to other countries and non-state actors. Similarly, quality control is likely to pose major challenges when viewed in the context of assistance to overcome cybersecurity incidents and mitigation of harms that follow from such incidents.

It is worth noting that in its work on protection of persons in the event of disasters, the ILC has recognized the right of "States, the United Nations, and other competent intergovernmental organizations . . . to offer assistance to the affected State" responding to a disaster.[191] Furthermore, the ILC's draft articles provide that "[r]elevant non-governmental organizations may also offer assistance to the affected State."[192] Concomitantly, the draft articles provide that, for its part, the affected State "shall take the necessary measures, within its national law, to facilitate the prompt and effective provision of external assistance . . . ."[193]

C. Responsibility of DAS After Cybersecurity Incidents

In the aftermath of a cybersecurity incident, DAS ought to have the responsibility not only to implement recovery measures[194] but also to engage in long-term adjustment plans and rehabilitation efforts.

One major challenge with cybersecurity incidents is that, "[w]ith the globalization of communications networks, public safety is increasingly dependent on effective law enforcement cooperation with foreign governments. That cooperation may not be possible, however, if a country does not have substantive laws in place to prosecute or extradite a perpetrator."[195] International cooperation depends on states enacting relevant

189. *Id.* at paras. 146–60.

190. *Id.* at para. 146 (quoting Int'l Law Comm'n Rep. on the Work of Its Sixty-Third Session, U.N. Doc. A/66/10, at 249 (2011)).

191. ILC Report, *supra* note 129, at 129.

192. *Id.*

193. *Id.* at 131.

194. G.A. Res. 41/128, annex, Declaration on the Right to Development, art. 1, (Dec. 4, 1986) ("[A]n inalienable human right by virtue of which every human person and all peoples are entitled to participate in, contribute to, and enjoy economic, social, cultural and political development, in which all human rights and fundamental freedoms can be fully realized."). *See also* INT'L COMM'N ON INTERVENTION AND STATE SOVEREIGNTY, INT'L DEV. RESEARCH CTR, THE RESPONSIBILITY TO PROTECT xi (2001), http://responsibilitytoprotect.org/ICISS%20Report.pdf.

195. Miriam F. Miquelon-Weismann, *The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?*, 23

domestic legislation, both penal and civil, and enforcing such legislation. In a similar vein, U.N. Security Council Resolution 1373 states that "all States shall . . . [a]fford one another *the greatest measure of assistance* in connection with criminal investigations or criminal proceedings relating to or financing or support of terrorist acts, including assistance in obtaining evidence in their possession necessary for the proceedings."[196]

Conclusion

Cybersecurity incidents may result in significant harm regardless of whether the cause of such harm is a premeditated syntactic or semantic attack orchestrated by states or hacktivists, or a natural disaster that results in partial or complete destruction of digital infrastructure or networks. Preventing, overcoming, and recovering from such incidents require concerted actions by a variety of actors, both state and non-state, both domestically and internationally. There is a multiplicity of stakeholders in ICT networks and CIS structures. Domestically, federal (where relevant), state and local government, civil society, organizations and corporations, individuals, owners, and operators of critical infrastructure all have an essential stake in the issues discussed in this Article.[197] Internationally, foreign governments, as well as non-governmental organizations and international organizations, may be both part of the problem and of the solution.[198] The diversity of stakeholders raises concerns of fragmentation, transparency, oversight, accountability, cost, and network complexity.[199] At the same time, the growing challenges of cybersecurity incidents require streamlined processes for collaboration and exchange of information. They also require recognition and acknowledgement that every state, whether a source state for such incident or a state directly affected by the incident, must bear some responsibility to prevent, mitigate, manage, and ultimately recover from such incidents. Such responsibilities are owed, ultimately, both to the state's own citizens and to the global community of states and non-state actors.

J. MARSHALL J. COMPUTER & INFO. L. 329, 335–36 (2005) (citing U.S. Dept. of Just., Comments of the United States Government on the European Commission Communication on Combating Computer Crime).

196. Christopher E. Lentz, *A State's Duty to Prevent and Respond to Cyberterrorist Acts*, 10 CHI. J. INT'L L. 799, 820 (2010) (citing S.C. Res. 1373, ¶ 2(f) (Sept. 28, 2001)) (emphasis added).

197. A GAO report found that thirty-one out of thirty-four of the United States Department of Defense's most critical assets were dependent upon the public power grid, which is eighty-five percent privately owned and, under current U.S. law, cannot be ordered to comply with hardening its networks against cyber attacks. U.S. GOV'T ACCOUNTABILITY OFF., GAO-10-147, DEFENSE CRITICAL INFRASTRUCTURE: ACTIONS NEEDED TO IMPROVE THE IDENTIFICATION AND MANAGEMENT OF ELECTRICAL POWER RISKS AND VULNERABILITIES TO DOD CRITICAL ASSETS 10, 22, 36 (2009).

198. Buckland, *supra* note 55, at 17.

199. *Id.*