VOLUME 52, NUMBER 2, SUMMER 2011

An e-SOS for Cyberspace

Duncan B. Hollis

TABLE OF CONTENTS

An e-SOS for Cyberspace

Duncan B. Hollis*

Individuals, shadowy criminal organizations, and nation states all currently possess the capacity to harm modern societies through computer attacks. These new and severe cyberthreats put critical information, infrastructure, and lives at risk—and the threat is growing in scale and intensity with every passing day.

The conventional response to such cyberthreats is self-reliance; but when self-reliance comes up short, states have turned to law for a solution. Cybercrime laws proscribe individuals from engaging in unwanted cyberactivities. Other international laws establish what states can (and cannot) do in terms of cyberwarfare. Both sets of rules work by attribution, targeting bad actors—whether criminals or states—to deter cyberthreats.

This Article challenges the sufficiency of existing cyberlaw and security. Law cannot regulate the authors of cyberthreats because anonymity is built into the very structure of the Internet. As a result, existing rules on cybercrime and cyberwar have little deterrent effect. They may even create new problems when attackers and victims assume that different rules apply to the same conduct.

Instead of regulating bad actors, this Article proposes that states adopt a duty to assist victims of the most severe cyberthreats. A duty to assist provides victims with assistance to avoid or mitigate serious harms. At sea, anyone who hears a victim's SOS must offer whatever assistance is reasonable. An e-SOS would work in a similar way. It would require assistance for cyberthreat victims without requiring them to know who, if anyone, was threatening them. An e-SOS system could help avoid harms from existing cyberthreats and deter others. Even when cyberthreats succeed, an e-SOS could make computer systems and networks more resilient against any harm they impose. At the same time, an e-SOS would complement, rather than compete with, self-reliant measures and existing legal proscriptions against cyberthreats.

Introduction

Cyberspace is in trouble.[1] Consider three examples: on January 12, 2010, Google announced a dramatic theft of intellectual property from its computer networks and those of twenty other major U.S. companies. Google traced the thieves to China, where its accusations touched off a furor in diplomatic and business circles.[2] Six months earlier, a malfunction in the

* Associate Dean for Academic Affairs and Associate Professor of Law, Temple University Beasley School of Law. I want to thank Jeff Dunoff, Jack Goldsmith, David Hoffman, Neal Katyal, Orin Kerr, Herb Lin, James Lippard, and David Post for helpful comments along with those received when I presented versions of this idea at Harvard Law School and the U.S. Naval War College. I am particularly indebted to Henry Richardson, who inspired me to explore the SOS analogy in the first place. Finally, I extend special thanks to Sarah Happy, Mathew Lewis, Athas Nikolakakos, Timothy Stengel, David Struwe, and Anthony Uy for invaluable research assistance.

1. By cyberspace, I am referring to *all* computer systems, networks, and wireless devices, not just the Internet. *Accord* Richard A. Clarke & Robert Knake, Cyberwar 70 (2010).

2. John Markoff et al., *In Digital Combat, U.S. Finds No Easy Deterrent*, N.Y. Times, Jan. 26, 2010, at A1; David Drummond, *A New Approach to China*, The Official Google Blog (Jan. 1, 2010, 3:00 PM), http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

Washington D.C. Metro computer system contributed to a crash that killed nine people and injured dozens.[3] In 2007, an entire nation—Estonia—had its computer networks overwhelmed for several weeks, with serious consequences; even emergency phone lines for paramedics and fire fighters were temporarily disabled.[4]

Each of these seemingly disparate incidents illustrates the dangers, or cyberthreats, that have emerged as individuals, corporations, and governments grow more dependent on computer systems and networks. Cyberthreats have myriad causes. Some—like the D.C. Metro tragedy—are internal: *computer errors* resulting from the increasing complexity of information technology and the tasks it performs. Others—like the Google and Estonian cases—have external origins. Dubbed Operation Aurora, Google's loss of property represents an example of *cyberexploitation*: the use of computer code to obtain unauthorized access to information on, or transiting through, a computer system or network. Estonia fell victim to a *cyberattack*: the use of malicious code to alter, disrupt, usurp, or destroy computer systems or networks.[5]

Today's cyberthreats range just as widely in effects as causes. In 2008, data theft from cyberexploitations produced estimated losses of $1 trillion.[6] U.S. officials have discovered cyberattacks on the U.S. power grid, inserting programs that—if not disabled—would allow outsiders to control that system or perhaps destroy it entirely.[7] In what has been described as an "Oppenheimer moment," a 2010 cyberattack apparently disabled two of Iran's uranium enrichment facilities, substantially impeding its nuclear ambitions.[8] Experts fear future cyberattacks may disrupt everything from water

3. The crash was attributed to "a failure of track circuit modules" and inadequate maintenance. Press Release, National Transportation Safety Board, NTSB Cites Track Circuit Failure and WMATA's Lack of a Safety Culture in 2009 Fatal Collision (July 27, 2010), *available at* http://www.ntsb.gov/Pressrel/2010/100727c.html.

4. *See, e.g.*, Mark Landler & John Markoff, *After Computer Siege in Estonia, War Fears Turn to Cyberspace*, N.Y. Times, May 29, 2007, at A1; Steven Lee Myers, *Estonia Computers Blitzed, Possibly by the Russians*, N.Y. Times, May 18, 2007, at A8; *Newly Nasty*, Economist, May 26, 2007, at 63. For an in-depth account, see Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, Wired (Aug. 21, 2007), http://www.wired.com/politics/security/magazine/15-09/ff_estonia.

5. *See* Nat'l Research Council Comm. on Offensive Information Warfare et al., Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities 1–2 (Owens et al. eds., 2009) [hereinafter 2009 NRC Study] (defining cyberexploitation and cyberattack). *Accord* Jack Goldsmith, *The New Vulnerability*, The New Republic (June 24, 2010), http://www.tnr.com/article/books-and-arts/75262/the-new-vulnerability.

6. President Barack Obama, Securing Our Nation's Cyber Infrastructure (May 29, 2009), *available at* http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure [hereinafter President Obama Speech].

7. Jordan Robertson & Eileen Sullivan, *U.S. Power Grid Hacked, Officials Say*, Chi. Trib., April 9, 2009, at C28; *see also* Jeanne Meserve, *Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid*, CNN.com (Sept. 26, 2007), http://www.cnn.com/2007/US/09/26/power.at.risk/index.html (researchers show cyberattack causing electric generator to shake, smoke, and shut down).

8. Ron Rosenbaum, *The Triumph of Hacker Culture*, Slate (Jan. 21, 2001), http://www.slate.com/id/2281938/ (comparing the Stuxnet virus targeting Iran as a similar technological leap to the "way the first nuclear weapon Oppenheimer built at Los Alamos left mere TNT in its wake and shadowed the

supplies to stock exchanges.[9] Researchers have revealed cyberattacks may even kill, for example by using wireless technology to manipulate and disable a pacemaker.[10] The collective dangers of cyberthreats are so great that President Obama labeled them "among the most serious economic and national security risks we face as a nation."[11]

How should law respond to such cyberthreats? For years, Internet users have held fiercely to a self-reliant mentality. They believe they can counter cyberthreats alone, using security systems to monitor, repair, and defend their computers and networks.[12] When those efforts fail, secrecy is often the preferred strategy. Companies and governments rarely admit the existence of a problem, let alone ask for assistance.[13] Government regulation of any kind is unwanted.[14]

Unfortunately, self-help can no longer serve as the only response to electronic threats. Cyberattacks and cyberexploitations have proven more than capable of adjusting to—and regularly overcoming—the latest security innovations.[15] At the same time, sophisticated criminal networks, newly minted military cyberforces, and so-called "hacktivists" all now possess extensive cyberexploitation and cyberattack capacities.[16]

---

world we live in with the threat of cataclysmic extinction"); *see also* William J. Broad et al., *Israel Tests Called Crucial In Iran Nuclear Setback*, N.Y. TIMES, Jan. 16, 2011, at A1; Christopher Williams, *Stuxnet: Cyber attack on Iran 'was carried out by Western Powers and Israel'*, TELEGRAPH (London), Jan. 21, 2011.

9. When stocks inexplicably dropped over 1000 points on May 6, 2010, the White House had to quell fears of a cyber attack. *No Indication Cyberattack Caused Stock Sell-off: U.S.*, REUTERS, May 9, 2010, *available at* http://www.reuters.com/article/idUSTRE64817820100509; *see also* Michael Crawford, *Utility Hack Led to Security Overhaul,* COMPUTERWORLD (Feb. 16, 2006, 12:00 PM), http://www.computerworld.com/s/article/108735/Utility_hack_led_to_security_ overhaul (hacker dumps millions of gallons of sewage into Australian waterways).

10. Daniel Halperin et al., *Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses*, PROCEEDINGS OF THE 2008 IEEE SYMPOSIUM ON SECURITY AND PRIVACY (2008), *available at* http://www.secure-medicine.org/icd-study/icd-study.pdf.

11. President Obama Speech, *supra* note 6.

12. *See, e.g.*, STEWART A. BAKER, SKATING ON STILTS 224 (2010).

13. *See, e.g.*, NAT'L RESEARCH COUNCIL COMM. ON IMPROVING CYBERSECURITY RESEARCH IN THE UNITED STATES, TOWARDS A SAFER AND MORE SECURE CYBERSPACE 184 (Seymour E. Goodman & Herbert Lin eds., 2007) [hereinafter 2007 NRC STUDY].

14. *See, e.g.*, DAVID G. POST, IN SEARCH OF JEFFERSON'S MOOSE: NOTES ON THE STATE OF CYBERSPACE 163–85 (2009) (describing Internet "exceptionalists," who advocate "self-governing communities"); David R. Johnson & David G. Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1375, 1387–88 (1996) (favoring self-regulation over government regulation); David R. Johnson et al., *The Accountable Net: Peer Production of Internet Governance*, 9 VA. J.L. & TECH. 9, 15–16, 21 (2004) (same). *But see* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? (2006) (arguing governments can, and should, regulate cyberspace).

15. *Cyberwar: War in the Fifth Domain*, ECONOMIST, July 1, 2010, at 25, 26–27 (A senior FBI official said that "given enough time, motivation and funding, a determined adversary will always—always—be able to penetrate a targeted system."); Markoff et al., *supra* note 2, at A1 (A senior Pentagon official insisted that "a fortress mentality will not work in cyber" and that "we cannot retreat behind a Maginot Line of firewalls.").

16. STEWART BAKER ET AL., IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 2–12 (Center for Strategic & International Studies, 2010) [hereinafter CSIS REPORT].

To date, policy and scholarly circles have shown remarkable uniformity in their favored regulatory response to this failure of self-help: proscription.[17] This approach regulates actors; it forbids specific acts by specific persons, groups, or governments, and it holds those found to have engaged in proscribed behavior publicly accountable. Thus, under the banner of *cybercrime*, governments—acting unilaterally or by treaty—have banned individuals from engaging in certain cyberattacks.[18] More recently, experts have explored prospects for *cyberwar* and the use of existing international rules on force to proscribe what militaries can do in launching (or defending against) cyberattacks.[19] Forecasts of *cyberterrorism* have generated similar calls for separate rules targeting terrorists.[20]

None of these regulatory models purports to redress all cyberthreats. Rather, each targets a different set of actors who would use cyberspace to cause harm. Each model assumes—and indeed requires—attribution. Categorizing a cyberattack as cybercrime, cyberwar, or even cyberterrorism, requires knowing which type of actor was responsible. A cyberattack by a criminal organization, for example, falls under the mantle of cybercrime.[21] But, if the same attack has military origins, very different rules of international law apply, such as the laws of war.[22] More importantly, by attributing a cyberattack to a particular individual (or military), proscriptions endeavor to remedy past harms and deter future attacks.[23] To date, proponents of rules on cybercrime and cyberwar regularly assume that sufficient attribution of an attack's origins can and will occur.[24]

---

17. Some scholars, like Jonathan Zittrain, continue to resist a regulatory response, favoring instead voluntary mechanisms where those who care about an open Internet develop new ways to "preserve . . . generativity while making necessary progress toward stability." Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974, 2029 (2006).

18. *See, e.g.*, Council of Europe, Convention on Cybercrime, Nov. 23, 2001, Europ. T. S. No. 185 [hereinafter Convention on Cybercrime].

19. *See, e.g.*, CLARKE & KNAKE, *supra* note 1, at 6; Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. INT'L L.J. 179, 185 (2006); Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 890 (1999); Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192, 196–98 (2009); Mike McConnell, *Mike McConnell on How to Win the Cyber-war We're Losing*, WASH. POST, Feb. 28, 2010, at B01.

20. *See, e.g.*, JOHN ROLLINS & CLAY WILSON, CONG. RESEARCH SERV., RL33123, TERRORIST CAPABILITIES FOR CYBERATTACK: OVERVIEW AND POLICY ISSUES 3–4 (2007); Christopher E. Lentz, *A State's Duty to Prevent and Respond to Cyberterrorist Acts*, 10 CHI. J. INT'L L. 799, 816–22 (2010).

21. *See* Susan Brenner, *"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 J. CRIM. L. & CRIMINOLOGY 379, 440 (2007).

22. *See* Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1037, 1049–50 (2007).

23. *See, e.g.*, MARTIN C. LIBICKI, CYBERDETERRENCE AND CYBERWAR 41 (2009); Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1055–56 (2001).

24. *See, e.g.*, *Advance Questions for Lt. Gen. Keith Alexander, USA Nominee for Commander, U.S. Cyber Command Before the S. Armed Serv. Comm.*, 111th Cong. 23 (2010), *available at* http://armed-services.senate.gov/statemnt/2010/04%20April/Alexander%2004-15-10.pdf [hereinafter *Alexander Q&A*] ("The bottom line is, the only way to deter cyber attack is to work to catch perpetrators and take strong and public action when we do so.").

In reality, however, anonymity, not attribution, prevails. Current information technology makes it difficult to identify the actual server from which an attack (or exploit) originates, let alone its perpetrators. And this is not a transient problem—the very architecture of the Internet enables hackers to maintain anonymity if they so desire.[25] Attackers can disguise their efforts to make them appear to originate with some other group or government.[26] In some situations, a victim may not even realize an attack has occurred, attributing the threat to computer error or malfunction.[27]

The absence of attribution has profound implications for the practicality of using law to respond to cyberthreats. It becomes difficult to know which set of proscriptions—crime, war, or terrorism—applies. Dangerous consequences may result if hackers and victims apply different regimes. More critically, anonymity makes it difficult—if not impossible—for rules on either cybercrime or cyberwar to regulate or deter. If cyberattackers assume that they cannot be identified (let alone sanctioned), rules prohibiting cyberattacks and exploits will have little deterrent effect. For the time being, skilled cyberattackers can act with near impunity.

In this Article, I argue that international law needs a new norm for cybersecurity: a duty to assist, or DTA. DTAs are not themselves novel, nor do they require identifying bad actors to operate. They work by requiring assistance for victims facing emergent and serious harm. The most well known example—the SOS—does this by providing a universal maritime distress call and requiring vessels that hear it to "proceed with all speed" to provide whatever assistance they can.[28] Depending on the context, other DTAs vary in terms of *which* victims can call for help, *when* they can do so, *who* must provide help, and *what* help those assisting must give.[29] In all cases, the goal is the same: mitigate or avoid unwanted harm to life or property.

As yet, there is no DTA for the Internet. But an SOS for cyberspace, an e-SOS, could both regulate *and* deter the most severe cyberthreats. Unlike proscriptive approaches, a DTA would not require attribution to function effectively; those facing harm would not need to know if it came from a cyberattack, let alone who launched it. A DTA would seek to redress unwanted harms directly, whatever their cause. It would do so by marshaling sufficient resources to avoid or at least mitigate that harm as much as possible. If it does so effectively, attackers may think twice about whether it is worth the effort to attack at all.

---

25. *See* CSIS REPORT, *supra* note 16, at 6; HOWARD F. LIPSON, CERT COORDINATION CENTER, TRACKING AND TRACING CYBER-ATTACKS: TECHNICAL CHALLENGES AND GLOBAL POLICY ISSUES 18, 56 (2002), *available at* http://www.sei.cmu.edu/library/abstracts/reports/02sr009.cfm.

26. LIBICKI, *supra* note 23, at 44.

27. *See* Goldsmith, *supra* note 5, at 22; Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 212–13 (2002).

28. *See, e.g.*, International Convention for the Safety of Life at Sea, Annex, Ch. V, Reg. 33(1), Nov. 1, 1974, T.I.A.S. No. 9700 [hereinafter SOLAS].

29. *See infra* Part III.C.

An e-SOS might organize and frame nation states' nascent efforts to organize against cyberthreats.[30] I do not expect any resulting duty to remediate all threats nor to operate in all contexts. Nevertheless, the DTA would give law a much needed boost in deterring cyberthreats. It would complement—not compete with—existing approaches. In doing so, the duty would increase the "resilience" of computer networks, providing a concrete way to contain and limit harm when self-reliance fails.

Part I of this Article surveys existing cyberthreats. I provide a typology of the effects, causes, and potentially responsible parties. Part II examines cyberspace's attribution problem and its negative implications for existing legal responses. Part III examines various DTAs and explores how to devise one for cyberspace. Part IV asks the normative question of what benefits (and costs) would accompany such a duty. In the end, I argue that governments can—and should—create a DTA to remedy the most serious cyberthreats and that doing so would have systemic benefits for international regulation of cyberspace more generally.

I. Defining the Problem: Cyberthreats & Their Origins

Today, almost every form of human endeavor has a virtual outlet. Computers allow searches, sharing, and storage of almost any type of information. Computer networks offer new pathways of control; everything from automobiles to ovens can now be directed remotely.[31] Banking and securities industries rely on computer networks to manage transactions. Governments and industry depend on so-called "supervisory control and data acquisition" (SCADA) systems to control infrastructure, such as electrical and nuclear power systems, telecommunications, and oil storage facilities.[32]

But the benefits of this migration to cyberspace have come with corresponding costs. Cyberthreats reflect new vulnerabilities that accompany this ever-increasing dependency on information technology. Computer systems, networks, and wireless devices are all at risk. The threats range enormously in terms of severity, causes, and authors. But their potential for indirectly affecting critical infrastructure and human life is the most troubling.

30. The United States, Russia, China, and a dozen other nations are currently preparing to negotiate new rules for cyberthreats. Warwick Ashford, *US Joins UN Cyber Arms Control Collaboration*, ComputerWeekly.com (July 20, 2010, 4:14 PM), http://www.computerweekly.com/Articles/2010/07/20/242045/US-joins-UN-cyber-arms-control-collaboration.htm.

31. Clarke & Knake, *supra* note 1, at 71, 85; Paul Ridden, *Automobile Computer Systems Successfully Hacked*, GizMag (May 20, 2010, 1:27 AM), http://www.gizmag.com/vehicle-computer-systems-hacks/15156/.

32. Clarke & Knake, *supra* note 1, at 96–101.

A. Direct & Indirect Effects: What Can Cyberthreats Do?

Cyberthreats come in all shapes and sizes. Traditionally, they are defined by their potential to produce one (or more) of four impacts on a computer system or network through a loss of:

- *confidentiality* (accessing confidential data without authorization)
- *integrity* (altering data to generate inaccurate information or results)
- *authenticity* (obscuring or forging data's true source to fool recipients)
- *availability* (impacting computer functions by denying or slowing down access to them).[33]

None of these categories, however, differentiate the severity of the harm posed. Unauthorized distribution of a gossipy e-mail is just as much a confidentiality loss as unauthorized access to U.S. war plans for Afghanistan, despite vastly different harms. To identify severe threats, we need different variables. Three—(1) time; (2) scale; and (3) indirect effect—help to assess the dangers, if any, of a particular cyberthreat.

Time defines the impact of a cyberthreat in two ways: immediacy and duration. A cyberthreat can do damage almost immediately once it has access to the targeted system or network. The 2003 "Slammer" worm infected 90% of all susceptible computers worldwide in under 10 minutes.[34] In contrast, logic bombs do nothing right away; instead, they compromise the system's susceptibility to a future triggering date or event.[35] A delayed response is not necessarily a less dramatic one. In 1982, the largest non-nuclear explosion in history destroyed part of the Soviet Union's gas pipeline when the CIA apparently tampered with the computer-control system, forcing it to "go haywire, after a decent interval, to reset pump speeds and valve settings" at intolerable levels.[36] Apart from immediacy, there is a question of duration—how long does the loss last? Some cyberthreats produce singular losses in less than a second, others last for hours, days, or even years.[37]

The *scale* of a cyberthreat depends on its intensity and how much data it affects. A cyberthreat may produce only minor or partial losses to a computer systems' integrity, or it could disrupt that system completely. Whatever its intensity, cyberthreats can also range widely in their distribution. Loss of confidentiality can range from a few kilobytes of data, to the

33. *See* 2009 NRC STUDY, *supra* note 5, at 111–12, 118; Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SEC. L. & POL'Y 63, 68–70 (2010).

34. David Moore et al., *Inside the Slammer Worm*, IEEE SECURITY & PRIVACY, July–Aug. 2003, at 33, *available at* http://cseweb.ucsd.edu/~savage/papers/IEEESP03.pdf.

35. *See infra* note 81 and accompanying text.

36. CLARKE & KNAKE, *supra* note 1, at 92–93; *Cyberwar: War in the Fifth Domain*, *supra* note 15, at 25.

37. *See, e.g.*, CLARKE & KNAKE, *supra* note 1, at 110–11 (describing 1999 cyberexploitation dubbed "Moonlight Maze" involving data ex-filtration from unclassified Defense Department network, which U.S. officials could not stop); Noah Shactman, *Communication with 50 Nuke Missiles Dropped in ICBM Snafu*, WIRED (Oct. 26, 2010, 5:15 PM), http://www.wired.com/dangerroom/2010/10/communications-dropped-to-50-nuke-missiles-in-icbm-snafu/ (hardware failure caused disruption of communications on network that links launch control center for 50 U.S. nuclear missiles for three quarters of an hour).

several terabytes related to the $300 billion Pentagon Joint Strike Fighter project lost in 2009.[38] Compromises in availability can range from a single computer to the 2007 denial of access to three of the thirteen "domain name servers" that direct Internet traffic.[39]

Of all the criteria for assessing a cyberthreat, the most important—and the chief concern of this Article—is the *indirect effect*. Despite the term's connotations, as Herbert Lin notes, indirect effects "are almost always more important" than direct effects on data confidentiality, integrity, authenticity, or availability.[40] Indirect effects arise when direct losses to a computer system or network spill over and impact the functions that the system or network supports. For example, when a breach of authenticity obscures or falsifies the true source of data, it may indirectly lead to identity theft or theft of business services. A confidentiality loss can have a host of follow-on effects, beyond simply compromising otherwise private data; indeed, it may even indirectly put human lives at risk. China has apparently utilized information obtained from compromises in the Dalai Lama's private computer networks to identify—and later detain—his supporters.[41]

Indirect effects encourage some to preach apocalyptic visions of cyberharm. A loss of computer integrity in financial systems could have significant repercussions if it disabled currency exchanges, credit card transactions, or stock market trades, or erased the data that support such transactions.[42] Disruptions in the availability of a SCADA system that controls infrastructure, like the power grid, could mean widescale loss of electricity.[43] Computers controlling mass transit, civil aviation, oil refineries, and even

38. Siobhan Gorman et al., *Computer Spies Breach Fighter-Jet Project*, WALL ST. J., Apr. 21, 2009, at A1.

39. *See* Ted Bridis, *Hackers Attack Key Net Traffic Computers*, USA TODAY, Feb. 7, 2007, *available at* http://www.usatoday.com/tech/news/computersecurity/2007-02-07-hacker-attack_x.htm. The attacks did not affect ordinary users because traffic could be rerouted. A 2002 attack had greater success, taking down seven of the thirteen servers for two hours. *Id.*

40. Lin, *supra* note 33, at 68.

41. BAKER, *supra* note 12, at 208–11. Researchers extensively studied this cyberexploitation, dubbed GhostNet, revealing confidentiality breaches on a thousand-plus computers in 100 countries, including those of foreign affairs ministries, embassies, international organizations, and others. Although China has used information obtained via GhostNet, it remains unclear whether it was responsible for the cyberexploitation directly, or if it purchased or otherwise obtained the information from those responsible. INFORMATION WARFARE MONITOR, TRACKING GHOSTNET: INVESTIGATING A CYBER ESPIONAGE NETWORK 12–13 (2009), *available at* http://www.infowar-monitor.net/research/ [hereinafter GHOSTNET REPORT].

42. *See* CLARKE & KNAKE, *supra* note 1, at 66.

43. SCADA systems are closed networks and should not have access to the Internet or any other open network. In reality, many SCADA systems *are* connected. CSIS REPORT, *supra* note 16, at 19 (in survey of 600 security experts and executives, more than 75% of those responsible for SCADA or related systems reported they were connected to the Internet or an IP network).

military weaponry are all at risk,[44] in ways that are often very difficult to predict.[45]

For others, this parade of potential catastrophes is the stuff of movie scripts, not reality.[46] The notion that cyberthreats may cause infrastructure disruptions or loss of life is labeled as scaremongering because real examples of such impacts are few and far between.[47] As a description of events to date, there is certainly some truth to these charges. A "Digital Pearl Harbor" has yet to occur despite more than a decade of predictions that such an event is imminent. And many—if not most—cyberthreats that have been realized involved temporary and largely pecuniary losses.

Ultimately, however, cyberthreats are dangerous not because of what they have (or have not) done to date, but precisely, because they threaten to generate serious impacts in the future. And, to be clear, cyberthreats have the *capacity* to produce the indirect effects described above. Estonia experienced this first-hand when the unavailability of computer networks used to route telecommunications traffic temporarily halted mobile and emergency phone service there.[48] In April 2009, U.S. officials discovered hackers had accessed the U.S. power grid and left behind programs that—if activated—could have given outsiders control over the system.[49] In 2007, a CIA official revealed that similar cyberattacks had created a blackout in an unidentified foreign country.[50] Most dramatically, in July 2010, experts identified a new

---

44. *Id.* at 14; FED. AVIATION ADMIN., REVIEW OF WEB APPLICATIONS SECURITY AND INTRUSION DETECTION IN AIR TRAFFIC CONTROL SYSTEMS 5 (2009) (it is "a matter of when, not if" cyberthreats will do serious harm to civilian air traffic operations); Shactman, *supra* note 37.

45. 2009 NRC STUDY, *supra* note 5, at 122. For example, recent reports suggest malware infecting SpanAir's computer maintenance system led to the deadly 2008 crash of Flight 5022. Leslie Meredith, *Malware Implicated in Fatal Spanair Plane Crash*, TECHNEWS DAILY (Aug. 20, 2010, 2:08 PM), http://www.technewsdaily.com/malware-implicated-in-fatal-spanair-crash-1078/.

46. *See, e.g.*, LIBICKI, *supra* note 23, at 123; *Cyberwar: War in the Fifth Domain*, *supra* note 15 (security guru Bruce Schneier views apocalyptic cyberattack possibilities as "movie-script stuff"); *see also* John Schwartz, *When Computers Attack*, N.Y. TIMES, June 24, 2007, at WK1; Ryan Singel, *Cyberwar Hype Intended to Destroy the Open Internet*, WIRED (Mar. 1, 2010, 6:56 PM), http://www.wired.com/threatlevel/2010/03/cyber-war-hype/.

47. Charles J. Dunlap, Jr., *Meeting the Challenge of Cyberterrorism: Defining the Military Role in a Democracy*, 76 INT'L L. STUD. 353, 359–62 (2002) (arguing that absence of any catastrophic cyberevents demonstrates that cyberattacks may be more difficult to accomplish than theorists realize); Stephen M. Walt, *Is the Cyber Threat Overblown?*, STEPHEN M. WALT, FOREIGN POLICY (Mar. 30, 2010, 4:14 PM), http://walt.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown (proposing that the potential danger from cyberthreats is not as significant as others suggest).

48. *See Newly Nasty*, *supra* note 4.

49. *See* Siobhan Gorman, *Electricity Grid in U.S. Penetrated by Spies*, WALL ST. J., Apr. 8, 2009; Robertson & Sullivan, *supra* note 7; *see also* OFFICE OF INSPECTOR GEN., U.S. DEP'T. OF HOMELAND SEC., CHALLENGES REMAIN IN DHS' EFFORTS TO SECURE CONTROL SYSTEMS (2009). Researchers have shown similar cyberthreats could impact newer, "Smart Grid" systems, designed to improve the efficiency of the U.S. power grid. *See* Erica Naone, *Hacking the Smart Grid*, M.I.T. TECH. REV. (Aug. 2, 2010), http://www.technologyreview.com/computing/25920/page1/.

50. *See* Ellen Nakashima & Steven Mufson, *Hackers Have Attacked Foreign Utilities, CIA Analyst Says,* WASH. POST, Jan. 19, 2008, at A4 (CIA analyst indicates cyberattackers accessed foreign utility's computer systems, made demands, and in one case, caused power outage affecting multiple cities). Subsequent attempts to identify a Brazilian blackout as this cyberattack have proved controversial. Marcelo

computer worm, dubbed Stuxnet, intended for SCADA systems.[51] News reports suggested Stuxnet was specifically designed to speed up Iran's nuclear centrifuges to intolerable levels while hiding this activity from Iranian engineers. Stuxnet apparently did so successfully, while also infecting other SCADA systems globally, albeit without as much demonstrable harm.[52]

These are not merely anecdotes. In 2009, the Center for Strategic and International Studies published a report, surveying six hundred information officials from critical infrastructure enterprises across seven sectors in fourteen countries spread throughout the world:[53] Nearly two-thirds reported cyberthreats that had affected their operations, with particularly severe effects in the energy and water sectors.[54] Attacks harmed websites, "e-mail connectivity, Internet-based telephone systems and other operationally significant functions" at an estimated cost of more than $6 million per day.[55]

B. How do Cyberthreats Arise?

Cyberthreats result from "vulnerabilities" in computer systems or networks.[56] These systems and networks are increasingly (and extraordinarily) complex, with designers writing millions of lines of code to produce desired functions.[57] Software errors are essentially inevitable. Similar errors may arise with the manufacture and maintenance of computer hardware.[58]

Sometimes vulnerabilities can cause harm without outside help. The D.C. Metro tragedy is one example. Air France Flight 447, which crashed, killing 228 passengers and crew, is another: its on-board computer system provided pilots with incorrect readings of the plane's speed.[59] In 1999, three people died after a gasoline pipeline ruptured and started a fire in Bellingham, Washington. Investigators found that that accident occurred because pipeline company employees were performing database work on their SCADA system at the same time that system was operating the pipeline, causing it

Soares, *Brazilian Blackout Traced to Sooty Insulators, Not Hackers*, WIRED (Nov. 9, 2009, 6:15 PM), http://www.wired.com/threatlevel/2009/11/brazil_blackout/#ixzz0x45wolvM.

51. Elinor Mills, *Details of the First-Ever Control System Malware (FAQ)*, CNET NEWS (Jul. 21, 2010, 4:00 AM), http://news.cnet.com/8301-27080_3-20011159-245.html.

52. Broad et al., *supra* note 8, at A1.

53. CSIS REPORT, *supra* note 16, at 1.

54. *Id.* at 7.

55. *Id.* at 7, 10.

56. *See* LIBICKI, *supra* note 23, at xiii; *see also* CLARKE & KNAKE, *supra* note 1, at 86.

57. *See* CLARKE & KNAKE, *supra* note 1, at 74.

58. *See* LIBICKI, *supra* note 23, at 12; Sally Adee, *The Hunt for the Kill Switch*, IEEE SPECTRUM, May 2008, at 34.

59. Richard Woods & Matthew Campbell, *Air France 447: The Computer Crash*, SUNDAY TIMES (U.K.), June 7, 2009.

to become nonresponsive.[60] Other computer errors have degraded operations of everything from financial markets to water supplies.[61]

In other cases, vulnerabilities cause harm because of outside interference. Attackers—whether engaging in cyberattacks *or* cyberexploitation—must do more than simply identify a vulnerability. They must have both *access* to the vulnerability and a *payload* to produce the desired result.[62] It is not enough to know that a SCADA system can be degraded in ways that will cause power outages. Attackers must also have access to that system and a program allowing them to exfiltrate information or to alter, disrupt, usurp, or destroy the system itself.

To understand cyberthreats, it is important to understand the different paths an attack can take.[63] Five ways exist:

(i) supply chains
(ii) remote access
(iii) denial of access
(iv) proximity
(v) insiders

First, the global supply chain for computer and network hardware and software provides numerous opportunities for the purposeful creation of vulnerabilities. Back door access might be built in at the very moment of production.[64] Alternatively, it might be introduced later by those servicing a computer system or network.[65]

Second, remote access involves hacking; that is, unauthorized accessing of a computer system, its functions, or resident data. Hacking features the novelty of geographic separation between victim and intruder, since the Internet allows attackers to gain access from anywhere on the globe. Attacks can be carried out much more cheaply than with other technologies, such as military aircraft, which cross similar geographic distances.[66] Remote access to one system can also quickly engender remote access to others via mali-

60. Kathy Kowalenko, *The Cyberhacker's Next Victim: Industrial Infrastructure*, INSTITUTE, Apr. 6, 2010, *available at* http://www.theinstitute.ieee.org/portal/site/tionline/menuitem.130a3558587d56e8fb2275875bac26c8/index.jsp?&pName=institute_level1_article&TheCat=2201&article=tionline/legacy/inst2010/apr10/featuretechnology.xml&.

61. *See, e.g.*, Edgar Ortega & Jeff Kearns, *NYSE Computer Error Halts Trading in 242 Stocks*, BLOOMBERG (June 12, 2009, 4:49 PM), http://www.bloomberg.com/apps/news?pid=newsarchive&sid=axW7yiJtSSTo; Julia Werdigier, *Computer Breakdown Halts Trading at London Exchange*, N.Y. TIMES, Sept. 9, 2008, at C5; Peter Bukowski, *Computer Malfunction Floods Yakima River With Sewage in Mabton, City Remains Silent*, KIMA CBS (Apr. 28, 2010, 6:26 PM), http://www.kimatv.com/news/92371909.html.

62. *See* LIBICKI, *supra* note 23, at 16. By "payload," I am referring to the actual data transmitted via the Internet (or other networks); in the context of either a cyberexploitation or a cyberattack, the payload will exploit the vulnerability in the targeted system or network, producing one or more of the direct or indirect effects discussed previously. *See supra* Part I.A.

63. *See* Steven R. Chabinsky, *Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line*, 4 J. NAT'L SEC. L. & POL'Y 27, 32–34 (2010).

64. For example, try this: type "=rand()" into most versions of Microsoft Word and press "Enter" to reveal a harmless backdoor introduced at the design stage. 2009 NRC STUDY, *supra* note 5, at 361 n.2.

65. *See* Chabinsky, *supra* note 63, at 32.

66. 2009 NRC STUDY, *supra* note 5, at 20.

cious software (malware), whether piggy-backing on files passed from user-to-user (viruses) or through self-propagation (worms).[67]

Third, in some cases, a vulnerability is exploited not by gaining access, but by denying it to others. The paradigmatic example is a "Distributed Denial of Service" (DDoS) attack, where data requests flood an Internet server, overwhelming its ability to respond or process requests. Legitimate traffic cannot access the site, and it is effectively disabled.[68] Today, DDoS attacks occur with increasing frequency given the advent of "botnets," networks of thousands of computers culled together to do the bidding of an unauthorized remote user.[69]

Fourth, wireless technology for computers and wireless communications devices provide access by proximity.[70] If you can get physically close enough to a wireless network (even if not inside it), access becomes possible. Attackers can monitor signals, connect to the same network as their targets, or convince unsuspecting targets to make the connection for them.

Finally, outsiders can always use insiders to gain access.[71] As the WikiLeaks controversy reveals, disgruntled employees or contractors may do so willingly.[72] More often, techniques—known as social engineering—have insiders offer up access unwittingly. Google's loss of intellectual property occurred through one such method, known as "spear-phishing." One of its high-level employees received an instant message that actually appeared to come from a trusted friend or colleague.[73] That message linked to a Taiwanese website that someone had rigged to install trap-doors on com-

67. *See* CSIS REPORT, *supra* note 16, at 6 (89% of those surveyed reported viruses or other malware had infected their systems or networks).

68. *Id.* at 5; LIBICKI, *supra* note 23, at 17–18 n.19.

69. *See* CSIS REPORT, *supra* note 16, at 5 (estimating a botnet of 3.5 million computers in the United States alone).

70. Proximity of access also includes cases where attackers target the physical layer (i.e., boxes and wires) of a computer network. LIBICKI, *supra* note 23, at 12; *see also* Chabinsky, *supra* note 63, at 34.

71. *See* Chabinsky, *supra* note 63, at 34. An estimated 25–40% of attacks come via insider access. Scott Hamilton, *The Unknown*, ARMED FORCES J., Nov. 2009, at 33, *available at* http://www.armedforcesjournal.com/2009/11/4268936/.

72. WikiLeaks is a private organization that publicizes otherwise secret, confidential or classified information. In April 2010, it released a controversial video of a 2007 helicopter attack in Baghdad that included civilian casualties. A low-level insider—U.S. army intelligence analyst Bradley Manning—provided WikiLeaks with the video. Manning also provided WikiLeaks with thousands of secret U.S. diplomatic cables, which, when released in the fall of 2010, provoked sustained and substantial controversy. *See, e.g.*, Elisabeth Bumiller, *Army Broadens Inquiry Into WikiLeaks Disclosure*, N.Y. TIMES, July 31, 2010, at A4 (reporting that the U.S. Army charged one of its privates with leaking 150,000 classified documents to WikiLeaks); Scott Shane, *Leaked Cables Offer Raw Look at U.S. Diplomacy*, N.Y. TIMES, Nov. 29, 2010, at A1. These incidents dramatically illustrated the potential scale and impact of cyberexploitation. *Unpluggable: How WikiLeaks Embarrassed and Enraged America, Gripped the Public and Rewrote the Rules of Diplomacy*, ECONOMIST, Dec. 2, 2010, *available at* http://www.economist.com/node/17633606 ("Secrets are as old as states, and so are enemies', critics' and busybodies' efforts to uncover them. But the impact and scale of the latest disclosures by WikiLeaks, a secretive and autocratic outfit that campaigns for openness, are on a new level.").

73. CLARKE & KNAKE, *supra* note 1, at 60; John Markoff & David Barboza, *Inquiry Is Said to Link Attack On Google to Chinese Schools*, N.Y. TIMES, Feb. 19, 2010, at A1.

puters that visited it, using a previously unidentified vulnerability in Microsoft's Internet Explorer program.[74]

After outsiders gain access through any of these methods, they can execute a payload that takes advantage of the designated vulnerability. A payload may be selective or indiscriminate, targeting only certain computers or all computers to which access can be gained.[75] It may even be hidden so users are unaware of its arrival.[76]

Payloads distinguish cyberexploitations from cyberattacks.[77] In a cyberexploitation, the payload seeks to gain access to data resident on a computer or network without otherwise affecting its operations.[78] The payload of a cyberattack is more nefarious, interfering with a computer system or network's normal operations.[79] Data may be altered, or the attacker may usurp control over all or parts of a system. Botnets, for example, partially usurp a computer system, leaving users with sufficient functionality while the attacker has given the system other tasks that users cannot see.[80]

Payloads may also destroy. Logic bombs act as erasers, wiping out all software on a computer.[81] A more sophisticated logic bomb can instruct the targeted computer to disrupt or degrade the system or infrastructure that that computer operates before wiping away all information, including evidence of the logic bomb's existence.[82]

Despite their distinct functions, cyberexploitations and cyberattacks are not mutually exclusive. It is possible for a payload to only execute a cyberexploitation (or only a cyberattack), but access to a vulnerability can also generate multiple payloads. Cyberexploitations and cyberattacks can thus occur simultaneously or sequentially.[83] And since the means of access are the same, users who discover a cyberthreat cannot distinguish if it is a cyberexploitation, a cyberattack, or both. Of course, if the payload is sufficiently disguised, victims may not know of the attack at all.[84] Table 1 summarizes the three primary causes of cyberthreats and the methods by which they arise.

---

74. Goldsmith, *supra* note 5, at 21–28.

75. *See* LIPSON, *supra* note 25, at 9.

76. Viruses, for example, can sit inactive until users run or open the infected file or program. Trojan Horses are programs that appear innocent but contain malware designed to exploit vulnerabilities. Rootkit programs access computer functions while remaining hidden from a user's operating system and antivirus software. 2009 NRC STUDY, *supra* note 5, at 88.

77. Lin, *supra* note 33, at 64 (The "primary technical difference between cyber attack and cyberexploitation is in the nature of the payload to be executed—a cyber attack payload is destructive whereas a cyberexploitation payload acquires information nondestructively.").

78. *Id.* at 63–64.

79. *Id.* at 64.

80. *See* CSIS REPORT, *supra* note 16, at 5.

81. CLARKE & KNAKE, *supra* note 1, at 92.

82. *Id.* (suggesting that a logic bomb might order an electric grid to produce a surge that fries circuits in transformers before erasing everything on the computer system).

83. 2009 NRC STUDY, *supra* note 5, at 152.

84. CLARKE & KNAKE, *supra* note 1, at 122.

TABLE 1: CAUSES OF CYBERTHREATS

	Vulnerability	***Access***	***Payload***
Computer Error	Coding or inter-operability errors that *generate* losses in confidentiality, integrity, authenticity or availability	None needed	None needed
Cyber-exploitation	Coding or inter-operability errors that create *opportunities* for losses in confidentiality, integrity, authenticity, or availability	Supply chain, remote access, denial of service, proximity access, or insider access	Loss of confidentiality over information on computer or network with minimal interference in their operations
Cyber-attack	Coding or inter-operability errors that create *opportunities* for losses in confidentiality, integrity, authenticity or availability	Supply chain, remote access, denial of service, proximity access, or insider access	Computer/network loses integrity, authenticity, or availability with potential indirect effects on controlled systems or devices

C. Who Creates Cyberthreats and Why?

In 1982, Mathew Broderick introduced cyberthreats to U.S. popular culture through his role as a hacker in the film, *War Games*. Hackers—like Broderick's character—formed groups where a member's status often depended on the technical skill displayed in finding or exploiting some vulnerability.[85] This often meant attacking high-profile targets or producing malicious mischief.[86] Today, many hackers have adopted less antagonistic aims. Through events like the annual Black Hat conference, some hackers publicly reveal vulnerabilities they have discovered, giving potential victims an opportunity to boost security.[87]

In recent years, however, others, including criminal organizations and governments, have begun to target and exploit computer vulnerabilities. A new group of hackers—hacktivists—have emerged, seeking to launch cyber-exploitations and attacks to advance a specific country, government, cause, or policy.[88] Hactivists played a role in deluging Estonia with DDoS attacks in 2007, because they considered Estonia's decision to relocate a World War

85. Peter T. Leeson & Christopher J. Coyne, *The Economics of Computer Hacking*, 1 J.L. ECON. & POL'Y 511, 512–15 (2005).

86. Hamilton, *supra* note 71; Leeson & Coyne, *supra* note 85, at 517–21.

87. *See About Black Hat*, BLACK HAT, http://www.blackhat.com/html/about.html (last visited Mar. 6, 2011).

88. In 1998, Amy Harmon noted how the technical skill hackers brought to demonstrating vulnerabilities in the military-industrial complex's computer security apparatus also offered new tools to political activists: "the rapid growth of the Internet has transformed what was once a hacker playground into, among other things, a far-reaching political platform. What's more, the tricks invented by hackers have become easier for activists to learn and adopt because they are now widely published on how-to Web sites. . . . [S]ome members of the famously sophomoric hacker underground are finding motivation in

II war memorial an affront to Russian nationalism.[89] Other hacktivists have participated in attacks opposing (or favoring) various groups or causes, such as the current Iranian government and WikiLeaks.[90] Some hactivists (most notably in China) have apparently passed the results of their cyberexploitations on to their favored government or group.[91]

Beyond hackers and hactivists, cyberthreats often have criminal origins. Criminals with the right skill set can make money online.[92] In the last several years, highly sophisticated cybercriminal organizations have emerged.[93] They have stolen data ranging from drug formulas to designs for weapon systems.[94] Criminal cyberattacks facilitate money laundering and intellectual property crimes involving theft of software and services. They can often extort funds from companies whose operations depend on maintaining an online presence with threats of a DDoS attack.[95] Criminal cyberorganizations have even found ways to profit from hacking technology itself. Certain Russian websites allow you to "rent" a botnet. Other organizations sell hacking tools and, just like a computer security company, provide regular updates to ensure the product continues to function as intended.[96]

At the same time, governments have developed their own capabilities. The United States launched U.S. Cyber Command in October 2009 to defend U.S. defense networks and to conduct offensive cyberoperations.[97] China, Russia, the United Kingdom, France, Israel, Iran, and Australia are all reported to have similar programs.[98]

Almost anything to do with military and intelligence operations in cyberspace is classified. Nonetheless, it is not difficult to hypothesize the utility of cyberexploitations and attacks to militaries or their governments. Military thinkers already laud their ability to "prepare the battlespace" for future

causes other than ego gratification." Amy Harmon, *'Hactivists' of All Persuasions Take Their Struggle to the Web*, N.Y. TIMES, Oct. 31, 1998, at A1.

89. *See* Schwartz, *supra* note 46.

90. *See* John F. Burns & Ravi Somaiya, *Hackers Attack Sites Considered WikiLeaks Foes*, N.Y. TIMES, Dec. 9, 2010, at A1; Benjamin Joffe-Walt, *Hackers Take Iran's Civil War Online,* JERUSALEM POST, Feb. 7, 2010, at 17; Brad Stone & Noam Cohen, *Social Networks Spread Iranian Defiance Online*, N.Y. TIMES, June 16, 2009, at A11; ANONYMOUS IRAN, http://iran.whyweprotest.net (last visited Mar. 6, 2011) (Iranian hacktivist's website that seeks to circumvent Iranian government filters); *supra* note 72.

91. CLARKE & KNAKE, *supra* note 1, at 59.

92. *See* Katherine T. Kleindienst et al., *Computer Crimes*, 46 AM. J. CRIM. L. 315, 316–21 (2009).

93. *See Cyberwar: War in the Fifth Domain*, *supra* note 15; Tyler Moore et al., *The Economics of Online Crime*, 23 J. ECON. PERSP. 3, 4 (2009). *See generally* CLAY WILSON, CRS REPORT FOR CONGRESS: BOTNETS, CYBERCRIME, AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS (2008) [hereinafter CRS REPORT].

94. Goldsmith, *supra* note 5.

95. *See, e.g.*, CSIS REPORT, *supra* note 16, at 8.

96. *See* Spencer Kelly, *Gaining Access to a Hacker's World*, BBC CLICK (Mar. 13, 2009, 9:55 GMT), http://news.bbc.co.uk/2/hi/programmes/click_online/7938201.stm; John Markoff, *Attack of the Zombie Computers Is Growing Threat*, N.Y. TIMES, Jan. 7, 2007, §1, at 1.

97. *See* U.S. CYBER COMMAND, FACT SHEET (May 25, 2010), http://www.defense.gov/home/features/2010/0410_cybersec/docs/CyberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf.

98. CLARKE & KNAKE, *supra* note 1, at 63–64.

conflicts. If logic bombs could replace real bombs (say, by lying in wait to order a generator to self-destruct at the opportune time), militaries will surely prefer them to the costs (and risks) of deploying their forces. At the same time, cyberattacks give militaries a capacity kinetic weapons never afforded. They may now *temporarily* disable a power grid via its SCADA system instead of having to blow it up.[99] A military (or intelligence agency) can employ cyberattacks to alter data, such as logistics plans, causing adversaries unexpected shortages of armor, fuel, or food.[100] Or, it might compromise the authenticity of enemy networks, impersonating enemy officials and issuing phony orders.[101] Cyberexploitation, meanwhile, enables governments to acquire (in secret) information on adversary strategy, tactics, and technology.

Militaries may have already used cyberattacks in their operations. In 2007, Israel bombed a North Korean-designed nuclear facility in Syria, without any resistance from Syrian military forces. Reports suggest Israel managed to disrupt the integrity of Syrian Air Defense networks to make Syrian airspace appear empty just as Israeli planes flew their sorties.[102] Israel (perhaps with U.S. assistance) is also reputedly behind the Stuxnet virus that so dramatically degraded Iranian nuclear facilities.[103] In 2008, DDoS attacks on Georgian websites—including those of its government—preceded Russian boots-on-the-ground. The attacks caused confusion within Georgia and limited the country's ability to publicize its version of events.[104]

At the same time, governments and their militaries clearly recognize that cyberexploitations and cyberattacks work even if they are not followed by actual fighting. Cyberattacks may influence or intimidate foreign governments, industries, or groups into a preferred course of action. Additionally, cyberexploitation greatly facilitates espionage.[105] At much less cost and risk, governments can access an exponentially greater amount of information that may have important consequences for diplomatic relations. For example, the U.S. Department of Defense recently confirmed that a USB device compro-

99. *See id.* at 101.

100. *See Cyberwar: War in the Fifth Domain*, *supra* note 15.

101. A cyberattack might limit an adversary's connectivity, privileges or services online, preventing them from receiving data such as targeting information. 2009 NRC STUDY, *supra* note 5, at 114–16.

102. *See* CLARKE & KNAKE, *supra* note 1, at 3–8; Wesley K. Clarke & Peter L. Levin, *Securing the Information Highway*, FOREIGN AFFAIRS, Nov.–Dec. 2009, at 2.

103. *See supra* notes 8, 51–52 and accompanying text.

104. *See, e.g.*, *Cyberwar: War in the Fifth Domain*, *supra* note 15; Kim Hart, *Longtime Battle Lines are Recast in Russia and Georgia's Cyberwar*, WASH. POST, Aug. 14, 2008, at D1; John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES, Aug. 13, 2008, at A1. Attackers also disrupted Georgia's financial system by having botnets launch DDoS attacks against *international* financial institutions that appeared to come from Georgia, triggering an automatic shut-down of Georgian banks' access to international financial markets. CLARKE & KNAKE, *supra* note 1, at 20.

105. *See, e.g.*, *Cyberwar: War in the Fifth Domain*, *supra* note 15 (spies used to be able to take out a few books' worth of materials, but can now take the whole library).

mised its classified computer network in 2008, establishing a "digital beachhead" for delivering operational plans to unknown sources.[106]

Finally, global terror organizations may launch cyberattacks as well. To date, as far as we know, they have only used their online presence for propaganda and recruitment.[107] Some experts believe this is as far as they will go.[108] Others, including the FBI, believe Al-Qaeda may try some form of catastrophic cyberthreat.[109] If they do, cyberterrorists may look a lot like "ordinary" hactivists. Any dividing line between the two groups is likely to be one of degree, where cyberterrorism involves "politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage."[110]

Table 2 surveys the actors that may be responsible for a cyberexploitation or cyberattack and the various rationales they may have for perpetrating one. I have not included those who may bear responsibility for computer error since, by definition, they do so negligently.[111]

The foregoing reveals the enormity of the cyberthreat problem. Anyone from a teenager to the largest military on earth can cause modern society vast harms. Motives vary: showing off a skill, making money, patriotism, nationalism, or influencing (or even terrorizing) foreign governments and their populations. The cyberexploitations and attacks through which these actors perpetuate a threat can exploit hardware or software vulnerabilities through multiple payloads delivered via any one of five access paths. In terms of effects, cyberthreats can be merely annoying or apocalyptic. One may do no more than deprive a single user of access to a word processing program for a few minutes. Another might deprive a nation of electric power for weeks. In the worst case, cyberthreats could indirectly generate large losses of life or permanent loss of critical infrastructure.

---

106. William J. Lynn, *Defending a New Domain: The Pentagon's Cyberstrategy*, FOREIGN AFFAIRS, Sept.–Oct. 2010, at 97.

107. *See* CRS REPORT, *supra* note 93, at 2, 9, 16, 30.

108. CLARKE & KNAKE, *supra* note 1, at 135 (viewing cyberterrorism as a "red herring").

109. *See Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace: Hearing Before the Subcomm. on Terrorism and Homeland Sec. of the S. Judiciary Comm.*, 111th Cong. 2 (statement of Steven R. Chabinsky, Dep. Asst. Dir., Cyber Division, FBI), *available at* http://judiciary.senate.gov/pdf/11-17-09%20New%20Chabinsky%20Testimony.pdf; Walter Gary Sharp, Sr., *The Past, Present and Future of Cybersecurity*, 4 J. NAT'L SEC. L. & POL'Y 13, 14 (2010) ("It is only a matter of time before terrorists attempt to use the Internet to cause acts of terrorism"); Goldsmith, *supra* note 5 (suggesting experts like Richard Clarke underestimate possibilities of cyberterrorism).

110. Dorothy Denning, *Activism, Hactivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, *in* NETWORKS AND NETWARS 241 (John Arquilla & David Ronfeldt eds., 2001).

111. Programmers or their companies, may, however, bear some liability for negligent coding or maintenance if their efforts fall short of the applicable duty of care. *See, e.g.*, Stephen E. Henderson & Matthew E. Yarbrough, *Suing the Insecure?: A Duty of Care in Cyberspace*, 32 N.M. L. Rev. 11, 15–17 (2002).

TABLE 2: WHO PRODUCES CYBERTHREATS AND WHY

Actor	*Reason for engaging in Cyberexploitation*	*Cyberattack*
Hackers	To demonstrate technical skill	To demonstrate technical skill; to prove concepts of what can be done
Hacktivists	To exfiltrate data for the benefit of a government or useful to advance a policy or cause	To advance the interests of a particular country, government, policy or cause
Criminals/Criminal Organizations	To steal identities, data, and intellectual property for financial gain	To steal software or services; to extort; to profit from markets in hacking technology
Governments/Militaries	To obtain information on adversary intentions, strategy, tactics, and technology; industrial espionage	To prepare the battlespace to support kinetic military operations; to influence foreign decision-making (overtly or covertly)
Terrorists	To steal identities and data to support other terrorist acts	To cause grave harm such as loss of life, property loss, or severe economic damage

II. THE INADEQUACY OF EXISTING LEGAL RESPONSES

To date, domestic and international law have approached cyberthreats almost exclusively through proscription. Generally, proscription seeks deterrence through attribution.[112] Governments look to discourage unwanted cyberthreats by identifying and holding publicly accountable violators among those regulated. But those who want to remain unidentified online can almost always do so. That fact has serious consequences few scholars recognize: cyberspace's attribution problem ensures current proscriptions are insufficient deterrents to the very cyberthreats that cause the most harm. More importantly, having different proscriptions for individuals and states may actually increase the danger cyberthreats pose.

A. The Existing Rules on Cybercrime and Cyberwar and their Attribution Assumptions

The United States and other nations initially dealt with cyberthreats through their own domestic criminal statutes.[113] In 1984, the U.S. Congress passed the Computer Fraud and Abuse Act (CFAA), prohibiting persons

112. I do not mean to suggest either criminal or international laws *only* serve deterrent functions. Criminal law may also have punitive, remedial, safety, or compensatory goals. *See* United States v. Brown, 381 U.S. 437, 458 (1965). And the laws of war, for example, were sought by President Lincoln to establish internal norms for Union forces. *See* General Orders No. 100, *in* LIEBER'S CODE AND THE LAW OF WAR 45–71 (R. Hartigan ed., 1983). Still, deterrence is a primary goal for both sets of rules, and clearly applies to the problem—cyberthreats—under consideration.

113. *See, e.g.*, Mark D. Goodman & Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace*, 10 INT'L J.L. & INFO. TECH. 139, 202–05 (2002) (surveying cybercrime laws of fifty different

from engaging in computer-specific offenses relating to unauthorized access.[114] Two years later, Congress amended that law to prohibit individuals from engaging in data theft and the intentional alteration, damage, or destruction of data belonging to others.[115] U.S. law thus prohibits individuals from engaging in specific acts of cyberexploitation and cyberattack. Today, these and dozens of other U.S. federal (and state) criminal laws proscribe individuals from using computers, networks, and wireless devices as vehicles for criminal activity or as its target.[116]

No single nation's criminal laws, however, could redress cyberthreats given their ability to originate from (and reach) anywhere in the world.[117] In 2001, the ILoveYou virus caused more than $11 billion in global losses, but when authorities located its author in the Philippines, local law did not proscribe his conduct, and he could not be prosecuted.[118] The United States and other states responded by campaigning for nations to harmonize their cybercrime laws and dedicate more law enforcement resources to the threat.[119] Today, dozens of states, including China and Russia, have legislated cybercrime proscriptions, although far from all have done so.[120]

In 2001, Western nations negotiated a treaty—the Convention on Cybercrime—that endorsed the proscriptive response to cyberthreats.[121] The Convention requires parties to adjust their domestic criminal law to proscribe certain commonly defined offenses such as illegal access and data interference.[122] It also requires a certain amount of cooperation in investigating and prosecuting such crimes through preservation and production of digital evidence, extradition, and mutual legal assistance.[123] Twenty-nine European

---

nation states); Salil K. Mehra, *Law & Cybercrime in the United States Today*, 58 AM. J. COMP. L. 659, 661 (2010) (surveying federal cybercrime laws).

114. Pub. L. No. 98–473 (1984) (amended 1986).

115. Pub. L. No. 99–474 (codified as amended at 18 U.S.C. § 1030 (2010)).

116. *See, e.g.*, 18 U.S.C. §§ 2510–22 (prohibiting unauthorized persons from intercepting wire and electronic communications); 18 U.S.C. §§ 2701–12 (prohibiting persons from intentional and unauthorized obtention or alteration of an electronic communication in electronic storage); Katyal, *supra* note 23, at 1016–19 (2001 survey of then-federal and state laws proscribing cybercrime). *See generally* Mehra, *supra* note 113 (surveying federal cybercrime law).

117. *See generally* Richard W. Downing, *Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime*, 43 COLUM. J. TRANSNAT'L L. 705 (2005).

118. *See* Katyal, *supra* note 23, at 1004.

119. Goodman & Brenner, *supra* note 113, at 165–74 (surveying international efforts to cooperate in drafting, investigating, and prosecuting cybercrimes); Mehra, *supra* note 113, at 682.

120. *See* Goodman & Brenner, *supra* note 113, at 202–05 (2002 study of fifty nations worldwide found twenty-seven proscribed hacking or other forms of unauthorized access; twenty-four prohibited unauthorized destruction, modification, copying or other manipulation of data; twenty-two prohibited computer sabotage through viruses, worms, denial of service, etc.; and twenty-five proscribed privacy breaches of personal data or interceptions of communications).

121. *See* Convention on Cybercrime, *supra* note 18. In the interest of full disclosure, in 2001 I served as part of the U.S. delegation that negotiated the final clauses of this treaty.

122. *Id.* arts. 2–13.

123. *Id.* arts. 14–35.

states and the United States have since joined the Convention on Cybercrime.[124] And, so far, it is the *only* cyber-specific treaty.[125]

Both the Convention on Cybercrime and domestic criminal laws focus on identifying and deterring particular perpetrators without regard to motives, so long as they are private actors.[126] But if a cyberattack or exploit comes from a military or intelligence agency, neither domestic nor international rules regulating cybercrime apply.[127] The Convention on Cybercrime, for instance, requires states to criminalize intentional access to a computer system "without right."[128] The accompanying Explanatory Memorandum clarifies that this "without right" caveat "leaves unaffected conduct undertaken pursuant to lawful governmental authority" including acts to "protect national security or investigate criminal offenses."[129] In other words, negotiators intended to exclude state attacks.

What rules apply when a state engages in (or defends against) a cyberattack or cyberexploitation? Unlike cybercrime, states have yet to devise cyber-specific rules for their own actions, leaving existing international law to apply by analogy.[130] How this law applies is not always clear, but there are at least three general proscriptions applicable to state conduct in cyberspace.

First, states must not launch (or threaten) a cyberattack that qualifies as a use of force absent U.N. Security Council authorization or pursuant to a state's inherent right to self-defense in response to an armed attack.[131] This prohibition is vague in its particulars.[132] Estonia, for example, accused Rus-

124. *Convention on Cybercrime: CETS No.: 185*, COUNCIL OF EUROPE, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (last visited Apr. 7, 2011). In particular, although it could have joined the treaty, Russia has declined to do so. *Id.*

125. Other treaties, most notably those relating to terrorism, may require states to treat certain cyberthreats as crimes. *See, e.g.*, Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation art. 1, Sept. 23, 1971, 24 U.S.T. 564, 974 U.N.T.S. 178.

126. Explanatory Report, Convention on Cybercrime, ¶ 38 (Nov. 8, 2001), http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

127. *See, e.g.*, 18 U.S.C. § 1030(f) (excluding lawfully authorized intelligence and law enforcement activity).

128. Convention on Cybercrime, *supra* note 18, at art. 2. The same "without right" language is included in the Convention's other criminalization provisions. *See id.* arts. 3–9.

129. Explanatory Report, *supra* note 126, ¶ 38.

130. *See* OFFICE OF GEN. COUNSEL, DEP'T OF DEF., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS (Nov. 1999), *reprinted in* 76 INT'L L. STUD. 459, 475, 520 (2002) [hereinafter DOD GC MEMO] (suggesting laws of war apply to cyberattacks by extrapolation); Hollis, *supra* note 22, at 1035–37. I have previously questioned the desirability of a law-by-analogy approach to government cyberoperations. *Id.* at 1029.

131. U.N. Charter arts. 2(4), 42, 51.

132. Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. (forthcoming 2011) (noting difficulties in line drawing over permissible and impermissible cyberattacks). The "instrumentality" theory views cyberattacks that interrupt communications (e.g., DDoS attacks) as not constituting a use of force under the Charter. *See* U.N. Charter art. 41; Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, 37 HARV. INT'L L.J. 272, 288–89 (1996). A "target-based" approach suggests cyberattacks are uses of force or armed attacks whenever they penetrate "critical national infrastructure" systems. Jensen, *supra* note 27, at 208 n.2; *see also* WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 129–32 (1999). Third, Michael

sia of violating this prohibition via the 2007 DDoS attacks that Estonia claimed constituted an "act of war," but for which Russia denied responsibility, and NATO ultimately could not agree on its qualification as an armed attack.[133] Nonetheless, there is little doubt that a catastrophic cyberattack severely disrupting a state's critical infrastructure would qualify.[134] Furthermore, any state victimized by such an attack would have a right to defend itself in cyberspace or beyond.

Second, states must not deploy cyberattacks within armed conflicts that violate the laws of war.[135] Thus, states must avoid cyberattacks that target civilian objects, cause indiscriminate harm, or violate the rights of neutral states.[136] Translating these proscriptions into cyberspace is not easy, but the laws of war require that states do so, just as they have for other novel developments in warfare such as airpower or nuclear, chemical, and biological weapons.[137]

Third, states must respect the sovereignty of other states in responding to any cyberattacks that do not constitute a use of force or arise within an armed conflict. Thus, states are proscribed from responding to such cyberattacks directly if it would interfere with the sovereignty of another state.[138]

Schmitt has suggested cyberattacks qualify as uses of force if their effects equate to those of a kinetic use of force. Michael Schmitt, *Wired Warfare*: *Computer Network Attack and* jus in bello, 84 INT'L REV. RED CROSS 365, 368, 396–97 (2002). This approach appears to have found favor with the U.S. Defense Department. DOD GC MEMO, *supra* note 130, at 483. For my critique of all three theories, see Hollis, *supra* note 22, at 1040–42.

133. *See* Hollis, *supra* note 22, at 1026–28.

134. Indeed, only the instrumentality theory might preclude cyberattacks as uses of force, but that reading was developed when cyberattacks did little to affect infrastructure or human life. *See, e.g.*, Charles J. Dunlap, Jr., *Towards a Cyberspace Legal Regime in the Twenty-First Century: Considerations for American Cyber-Warriors*, 87 NEB. L. REV. 712, 714 (2008) (some cyberattacks now warrant national security—as opposed to law enforcement—responses).

135. *Alexander Q&A*, *supra* note 24, at 15 (laws of war govern Defense Department activities, even in cyberspace). Most of these rules apply only to international armed conflicts between nation states, but some of their proscriptions undoubtedly also reach states engaged in non-international armed conflicts (such as civil wars). Hollis, *supra* note 22, at 1048.

136. *See, e.g.*, Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Armed Conflict (Protocol I) art. 48, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I] (conflicting states "shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives"); *id.* art. 51(4)–(5) (prohibiting states from using indiscriminate weapons and requiring them to employ proportionality); KNUT DÖRMANN, APPLICABILITY OF THE ADDITIONAL PROTOCOLS TO COMPUTER NETWORK ATTACKS 6 (2004), *available at* www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf.; Schmitt, *supra* note 132, at 389–90; George K. Walker, *Neutrality and Information Warfare*, 76 INT'L L. STUD. 233 (2002).

137. AP I, *supra* note 136, art. 36 (states have affirmative duty after they develop or acquire "a new weapon, means or method of warfare . . . to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable"). Although not a party, the United States considers most of AP I's provisions declaratory of customary international law. *See* Michael J. Matheson, *The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions*, 2 AM. U. J. INT'L L. & POL'Y. 419, 420, 423–29 (1987).

138. *See, e.g.*, Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 106 (June 27) ("principle of non-intervention involves the right of every sovereign state to conduct its affairs without outside interference . . . it is part and parcel of customary international law").

Instead, victim states must request that the state from which an attack is believed to have originated stop it.[139] Beyond these three proscriptions, at least a half-dozen other sets of rules prohibit states from cyberattacks that misuse satellites, telecommunications, or the high seas.[140]

State cyberexploitation is a grey area. Most states recognize that activity as simply a new method of espionage, and international law does not directly ban spying.[141] States do criminalize spying under domestic laws, applying it to any individual spies they catch. But for cyberexploitation, of course, the chances of apprehension are remote, since states can conduct it without putting their agents physically inside a foreign nation.[142]

What about terrorists in cyberspace? As individuals, their acts are likely cybercrimes under one or more national laws. But after the September 11 attacks, the United States and other nations began to re-label terrorist acts as uses of force, thereby justifying responsive acts of self-defense and application of the laws of war.[143] Today, there is no consensus on whether terrorism qualifies as only crime, only war, both, or neither.[144] If terrorists succeed in launching a severe cyberattack, that debate is likely to extend into cyberspace.

Whether through rules on cybercrime or through those implicating state-sponsored cyberoperations, governments have assumed that their proscriptions will deter unwanted behavior. But deterrence requires attribution. By attribution, I mean the ability to identify those engaged in the unwanted behavior.[145] Cybercrime rules rest on the theory that if states identify and prosecute enough hackers, hactivists, and criminal organizations for cyberthreats, other individuals will refrain from engaging in that conduct.[146] Rules on the use of force and the laws of war rest on similar grounds. If

---

139. *See* DOD GC MEMO, *supra* note 130, at 487–88; Yoram Dinstein, *Computer Network Attacks and Self-Defense*, 76 INT'L L. STUD. 99, 103 (2002). Only if the requested state is unable or unwilling to stop a cyberattack can the aggrieved state take counter-measures (or perhaps engage in self-defense). *See* Draft Articles on Responsibility of States for Internationally Wrongful Acts, G.A. Res. 56/83, Annex art. 49, U.N. Doc. A/RES/56/83 (Dec. 12, 2001); DOD GC MEMO, *supra* note 130, at 488.

140. *See* Hollis, *supra* note 22, at 1051–52.

141. *See* DOD GC MEMO, *supra* note 130, at 516; Simon Chesterman, *The Spy Who Came in from the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L L. 1071, 1072 (2006); Lin, *supra* note 33, at 72.

142. CLARKE & KNAKE, *supra* note 1, at 228; GHOSTNET REPORT, *supra* note 41, at 5; LIBICKI, *supra* note 23, at 23–25.

143. *See, e.g.*, Hollis, *supra* note 22, at 1026–28.

144. In contrast to the U.S. position, for example, the International Court of Justice has suggested self-defense is not an available option in responding to non-state actors; law enforcement of criminal laws is the only option. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136 (July 9); *accord* Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 116, 210–11 (Dec. 19).

145. The attribution assumption does not accompany all deterrence theories. But it is central to a proscriptive regime, unlike theories of nuclear deterrence. *Cf.* HERMAN KAHN, ON THERMONUCLEAR WAR (1960); HERMAN KAHN, THINKING ABOUT THE UNTHINKABLE (1962).

146. *See, e.g.*, Katyal, *supra* note 23, at 1012 (focusing on deterrence goals of cybercrime laws); Graham H. Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 A.F. L. Rev. 65, 79 (2009) (same).

enough states challenge a warring state for violating the rules, other states will refrain from engaging in such bad acts.[147]

Thus, deterrence through attribution serves as the law's primary response to cyberthreats. For many, it is the only response.[148] The current head of U.S. Cyber Command, Major General Keith Alexander, put it starkly: "The bottom line is, the only way to deter cyber attack is to work to catch perpetrators and take strong and public action when we do."[149] In looking at cyberthreats, scholars often ignore attribution entirely. Instead, they focus on assessing the nature and parameters of existing cybercrime or cyberwar proscriptions, and how to improve them.[150] Where scholars do address the importance of attribution, they tend to propose adjustments to existing proscriptions to ensure attribution occurs. To accommodate cybercrime attribution issues, scholars have suggested harsher sanctions or civilian enforcement.[151] For cyberwar, scholars have favored imputing attribution to states if cyberthreats originate in their territory.[152]

In sum, proscription dominates existing legal responses to cyberthreats on both the domestic and international planes. Cybercrime laws target individual hackers, hactivists, and criminal organizations engaged in cyberthreats.

147. The prospect of a state being labeled in breach of its international obligations carries reputational consequences that *can* deter unwanted state behavior. *See, e.g.*, ANDREW T. GUZMAN, HOW INTERNATIONAL LAW WORKS: A RATIONAL CHOICE THEORY 43 (2008); Rachel Brewster, *Unpacking the State's Reputation*, 50 HARV. INT'L L.J. 231 (2009).

148. Some states, notably China, also regulate the technology by which cyberthreats arise. These states require architectural controls—design requirements—on computer systems and networks to make it harder for outsiders to author a cyberthreat *and* easier for the government to detect and repel any attacks. *See* CLARKE & KNAKE, *supra* note 1, at 56–57.

149. *Alexander Q&A*, *supra* note 24, at 23.

150. *See, e.g.*, Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 VAND. J. TRANSNAT'L L. 57, 65–66 (2010) (arguing that the most feasible way to deter cybercrime is to prosecute cyber criminals under the international law principle of universal jurisdiction); Lentz, *supra* note 20, at 810 (presuming perpetrators of cyberterrorism or states that harbor them can be identified and caught); Jonathan A. Ophardt, *Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield*, 2010 DUKE L. & TECH. REV. 3, 52–53 (2010) (assuming cyberattackers can be caught and prosecuted under international criminal law); Schmitt, *supra* note 19 (attribution assumed in otherwise definitive exploration of international use of force rules for cyberattacks); Sharon R. Stevens, *Internet War Crimes Tribunals and Security in an Interconnected World*, 18 TRANSNAT'L L. & CONTEMP. PROBS. 657, 711 (2009) (seeking further proscriptions against cyberthreats via international criminal law); Sean Watts, *Combatant Status and Computer Network Attacks*, 50 VA. J. INT'L L. 391, 411–27 (2010) (attribution assumed in reviewing how laws of war regulate who conducts cyberattacks). My own earlier work had this focus as well. *See* Hollis, *supra* note 22, at 1029.

151. *See, e.g.*, Brenner, *supra* note 21, at 465–74 (advocating a redistribution of responsibility for the identification of cyber criminals to civilians to improve cybercrime investigations); Katyal, *supra* note 23, at 1075 (detailing problems with attribution but suggesting heightened penalties can preserve the law's deterrent functions); Peter Swire, *No Cop on the Beat: Underenforcement in E-Commerce and Cybercrime*, 7 J. TELECOMM. & HIGH TECH. L. 107, 126 (2009) (arguing for a more federal or federated approach to catch and prosecute cybercriminals).

152. *See, e.g.*, David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SEC. L. & POL'Y 87, 92–93 (2010) (seeking to impute responsibility to states for attacks originating from that state's territory); Lentz, *supra* note 20, at 810 (same); Shackelford, *supra* note 19, at 231–34 (same); *see also* Matthew Hoisington, *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, 32 B.C. INT'L & COMP. L. REV. 439, 451 (2009).

Rules proscribing cyberwar and other cyberattacks—but not cyberexploitation—seek to constrain and deter a state from unauthorized acts that cause severe harm or interfere with other states' rights. In issuing these proscriptions, all involved—governments and scholars alike—have assumed attribution will occur (either under existing proscriptions or through some adjustments to them). Unfortunately, that is a mistaken, and perhaps dangerous, assumption, given the current construction of cyberspace.

B. The Attribution Problem

On July 4, 2009, a DDoS attack took down dozens of U.S. and South Korean government and commercial websites. The affected sites included the U.S. Secret Service and its Treasury and Transportation Departments, along with South Korea's presidential Blue House, Defense Ministry, and National Assembly.[153] No one knows for sure who did it. The South Korean government blamed North Korea.[154] Others thought it was China.[155] U.S. experts suggested that the attack was unsophisticated and could have come from anyone.[156] Investigators later traced the attacks to Brighton, England—of all places—and then lost the scent.[157]

The July 4 incident is symptomatic of the difficulty in attributing responsibility online.[158] Those with sufficient technical skill can remain anonymous at will. They can even leave behind a "false flag," implicating an otherwise innocent individual, group, or government. The most sophisticated cyberexploitations may never be discovered. A high-level attack might be attributed to mere computer error. This situation is unlikely to change anytime soon; it is a systemic aspect of the Internet, not a simple problem to be fixed.

1. *Architectural Anonymity in Cyberspace.*

The Internet—literally, a network of networks—was originally designed with one particular type of security in mind—to ensure communication in the face of an external attack on U.S. infrastructure.[159] The resulting "packet-switched" network did so, dividing data up into lots of smaller pieces, attaching address information, then moving those pieces *separately* along any number of paths to a final destination where the data was reassem-

153. Choe Sang-Hun & John Markoff, *Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea*, N.Y. TIMES, July 9, 2009, at A4.

154. *Id.* (South Korean Intelligence Service saw this as "not a simple attack by an individual hacker" but one "thoroughly planned and executed by a specific organization or on a state level."); *see also* CLARKE & KNAKE, *supra* note 1, at 24–28 (noting "sophisticated" attacks had possible North Korean origins).

155. Hamilton, *supra* note 71.

156. Sang-Hun & Markoff, *supra* note 153.

157. CLARKE & KNAKE, *supra* note 1, at 25.

158. Thus, the true origins of the 2007 Estonian attacks remain unknown. *See, e.g.*, Landler & Markoff, *supra* note 4 (detailing accusations and denials regarding origin of Estonian cyberattacks).

159. LIPSON, *supra* note 25, at 5.

bled into its original form.[160] The shared rules for formatting and transmitting data, known as the Transmission Control Protocol/Internet Protocol (TCP/IP), made the system work, and remain the foundation for today's Internet.[161]

The complexity of the TCP/IP task was accomplished by layering the rest of the communications process. At the bottom, a "Data Link" layer includes the hardware used to access the Internet. The TCP/IP takes up the next two levels with (i) a "Transport" layer that breaks up and reassembles data; and (ii) a "Network" layer that routes data to its destination. At the top of the stack lies an "Applications" layer that converts data into useful things like web-pages or files. Each layer performs its function without regard to what the other layers do. Internet Explorer works on the Applications layer, for example, regardless of the connection—broadband, WiFi, satellite—used at the Data Link layer.[162]

Together, these aspects—packet-switching and network layering—provide attackers numerous opportunities to hide their identities or assume another. Consider the Network layer. Given the tremendous amount of packets it routes to millions of destinations, simplicity is key. In lieu of personal identification, the Network layer uses an Internet Protocol (IP) address to identify the origin (or destination) of routed data.[163] To uncover the source of a cyberexploitation or attack requires associating the IP address with a particular individual, group, or state.

But it is all too easy to mask your IP address. Imagine Twitter falls victim to a cyberattack.[164] Twitter's systems keep a record (or log) of every IP address visiting its site, which allows it to identify the attacker's IP address. It can then use the IANA (Internet Assigned Numbers Authority) database to identify which internet service provider (ISP) was assigned that IP address.[165] If that ISP keeps good records, it could tell Twitter to which computer's modem it had assigned that address.

Notice that the only way Twitter can trace the request is through the ISP's record-keeping. ISPs regularly empty out their logs, due to current Internet data volumes.[166] Thus, sourcing requests have to happen quickly;

160. *Id.* at 7.

161. *Id.* at 5.

162. Others have explained this better than I, using two, three, and more layers. *See, e.g.*, POST, *supra* note 14, at 80–90; Tim Wu, *Application-Centered Internet Analysis*, 85 VA. L. REV. 1163, 1189–94 (1999). The current system, known as the OSI Model, is divided into seven layers by parsing more closely the Applications Layer. *See The OSI Model's Seven Layers Defined and Functions Explained*, MICROSOFT SUPPORT (Feb. 27, 2002), http://support.microsoft.com/kb/103884.

163. MAC addresses provide a way to identify physical objects at the Data Link level.

164. Nor is this entirely hypothetical. *See* Elinor Mills, *Twitter, Facebook Attack Targeted One User*, CNET NEWS (Aug. 6, 2009, 4:32 PM), http://news.cnet.com/8301-27080_3-10305200-245.html (DDoS attack against Georgian blogger "Cyxymu" blocks access to Twitter and Facebook sites).

165. LIPSON, *supra* note 25, at 33; IANA, http://www.iana.org.

166. David Chaikin, *Network Investigations of Cyber Attacks: The Limits of Digital Evidence*, 46 CRIME L. SOC. CHANGE 239, 244 (2006).

otherwise, any evidence to identify perpetrators is gone.[167] Even where there are records, the IP address might go with a corporate account, numbering thousands of users. Or, the trail might end sooner if it goes to a coffee house that gives users free access, no questions asked.

Assuming Twitter can actually trace the IP address back to a single user, it might find that the computer had been captured. These are botnets that attack at the command of a remote, malicious attacker.[168] In all likelihood, that attacker will install several "stepping stones" between the attacking computer and the system used to control and command it.[169] In effect, attackers can "launder" the packets so that the attack's true origins will be difficult, if not impossible, to find.[170]

All of this assumes IP addresses can be trusted. But, as Howard Lipson has argued, this assumption is faulty. Attackers can forge the address of an IP packet.[171] In other words, high-level attackers can make another individual, group, or government appear as the responsible party by using their IP address.[172]

And these are just the opportunities for anonymity on the Network layer. The Data Link layer has its own opportunities, such as the use of pre-paid, wireless, and internet-accessible devices that grant Internet access without any record of the user's identity.[173] At the Applications layer, social engineering gives attackers access that affords additional opportunities to hide. Attackers routinely destroy or modify system logs so victims lack information (or receive misinformation) on what happened.[174]

This is not to suggest that all attackers remain anonymous. Attribution can occur, but usually does so via secondary intelligence, dumb mistakes, or some admission of responsibility in lieu of tracing attacks back to their original source.[175] The controllers of the large "Mariposa" botnet, for example,

---

167. *Id.* at 244–45.

168. Kelly Jackson Higgins, *How to Trace a DDoS Attack*, DARKREADING, Oct. 3, 2007.

169. CLARKE & KNAKE, *supra* note 1, at 214–15. Indeed, attackers can change the nature of packets transmitted between stepping stones, making it even more difficult to trace the source. LIPSON, *supra* note 25, at 5.

170. Chaikin, *supra* note 166, at 245–46.

171. *Id.* at 254–55.

172. An additional problem of dynamic IP addresses may soon go away. For the last few years, the number of available IP addresses has dwindled, making them a scarce resource. Organizations pooled addresses, which meant connected users were randomly assigned an IP address that changed with each new connection. The latest Internet Protocol—IPv6—provides billions of new IP addresses. This means everyone can be assigned a static IP address. That fix will not, however, remove the attribution problem. Although tracking packets will become easier, the other problems described—record-keeping, stepping stones, botnets—all remain. Moreover, during the IPv6 conversion, there is likely to be an increase in internal errors and hacking where attackers take advantage of a "noisier" environment in which to attack and exploit victims. *See, e.g.*, Carolyn Duffy Marsan, *Invisible IPv6 traffic poses serious network threat*, NETWORK WORLD (July 13, 2009), http://www.networkworld.com/news/2009/071309-rogue-ipv6.html.

173. LIBICKI, *supra* note 23, at 43–44; LIPSON, *supra* note 25, at 56.

174. LIPSON, *supra* note 25, at 18.

175. John Markoff, *Web's Anonymity Makes Cyberattack Hard to Trace*, N.Y. TIMES, July 17, 2009, at A5. In 2000, a Canadian high school student committed several high-profile DDoS attacks against Ya-

were only arrested after a botnet controller mistakenly used his real name on a computer involved in that botnet.[176] To date, however, "[n]o one has come close to solving the problem of technical attribution."[177]

2. *Difficulties with Using Presumptions for Attribution.*

In February 1998, a cyberexploitation called "Solar Sunrise" took hold of the U.S. Defense Department's unclassified computer network. U.S. government officials viewed it as "the most organized and sophisticated attack" the U.S. government had yet encountered.[178] Given a United States crisis with Iraq over the admissions of weapons inspectors, Defense officials presumed the attacks had links to a foreign government. In reality, the attacks came from three teenagers—one from Israel and two from California.[179]

The incident reveals the dangers of making presumptions about attribution. Scholars have proposed attributing responsibility for an attack based on various characteristics—including (i) the type of attack used, (ii) its target, or (iii) the country of origin.[180] In reality, none of these are reliable indicators for sourcing. The fact that an attack has occurred reveals little about its authors or their motivations.[181] As Martin Libicki aptly notes, "[t]here are no vulnerabilities that a state could discover that an individual cannot discover and exploit."[182] Simply put, if an attack or exploitation is possible, it is possible for anyone to perform it—hackers, hacktivists, criminals, terrorists, or states.

The target of an attack is also a poor proxy for identifying attackers. For example, Richard Clarke and Stewart Baker have each suggested that only a

---

hoo! and others, but was only identified after he bragged about doing so online. *Id.* Israeli and U.S. complicity in the Stuxnet virus has come via off-the-record leaks by U.S. officials. *See, e.g.*, Broad et al., *supra* note 8 (assigning responsibility for Stuxnet to U.S. and Israeli government programs).

176. Jeremy Kirk, *Alleged Mariposa Botnet Hacker Arrested in Slovenia*, PC WORLD (July 28, 2010), http://www.pcworld.com/article/202065/alleged_mariposa_botnet_hacker_arrested_in_slovenia.html; *see also* Charles Arthur, *Alleged controllers of 'Mariposa' botnet arrested in Spain*, THE GUARDIAN (March 3, 2010), http://www.guardian.co.uk/technology/2010/mar/03/mariposa-botnet-spain.

177. Lin, *supra* note 33, at 77.

178. Kim Zetter, *Israeli Hacker 'The Analyst' Indicted in New York—Update*, WIRED (Oct. 29, 2008), http://www.wired.com/threatlevel/2008/10/israeli-hacker/. Experts later challenged the sophistication of the attack, noting it took advantage of a known vulnerability; just one that had not been patched within Defense Department networks. *Id.*

179. CLARKE & KNAKE, *supra* note 1, at 110.

180. *See, e.g.*, *id.* at 199 (suggesting that the only motivation for hacking into the power grid is initiation of a cyberwar); Sean M. Condron, *Getting It Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 403, 413–16 (2007) (suggesting that when a state's critical infrastructure is attacked a state can act in self-defense without attribution); Graham, *supra* note 152, at 92–93 (seeking to impute responsibility to states for attacks originating from a state's territory). Analysts have also suggested that the sophistication of the Stuxnet virus required government authorship. Glenn Kessler, *Stuxnet Worm Possibly Made to Cripple Iran Centrifuges*, WASH. POST, Nov. 16, 2010, at A10.

181. *See, e.g.*, GHOSTNET REPORT, *supra* note 41, at 48–49; LIBICKI, *supra* note 23, at 75–78. To be clear—I am not suggesting states, cybercriminals, and hackers all have the same capabilities. But whatever may be the relative *median* capacity of each group, individual cases will vary sufficiently to make it an unreliable guide for attribution.

182. LIBICKI, *supra* note 23, at 34; *accord* Chabinsky, *supra* note 63, at 31–32.

nation state could have any interest in exploiting or attacking a SCADA system controlling the power grid.[183] But individuals and criminals could easily see benefits in targeting such systems.[184] Similarly, criminals might be responsible for "thefts" of intellectual property, or a state might be engaged in industrial espionage, or an individual might be trying to establish his reputation as someone living by the hacker's credo that "information needs to be free."[185] Indeed, although Google accused China of stealing its intellectual property through Operation Aurora, some experts have since suggested that the exploitation came from "inexperienced attackers."[186]

Recently, several scholars have claimed that states should bear responsibility for cyberattacks that originate within their territory.[187] But determining the territorial origins of an attack can be very difficult given the architecture of cyberspace. Looking again at Operation Aurora, it is still not certain that the attacks actually originated in China.[188] Moreover, presuming attribution by country of origin will surely motivate more "false-flag" operations where attackers seek to frame someone else as the responsible party.[189] This approach might also produce some unexpected costs for the very states seeking to combat cyberthreats. For example, does such a presumed attribution really mean the United Kingdom bears responsibility for the July 4, 2009 attack?[190] Given that the United States is viewed as the number one source of cyberthreats (China is second), what responsibility should the United States bear if an investigative trail ends at a computer in U.S. territory?[191]

3. *And Vested Interests Will Keep It This Way.*

If cyberspace architecture makes it so difficult to do attribution and attribution presumptions are unreliable, why not change things? The architecture of cyberspace presents opportunities for regulation that are unavailable in real space given the laws of physics. Whether or not "[c]ode is law" as

183. CLARKE & KNAKE, *supra* note 1, at 199 ("The only reason to hack into a power grid's controls . . . is if you are planning a cyber war."); Stewart Baker, *Proof that Other Countries are Planning Cyberattacks on the Power Grid?*, THE VOLOKH CONSPIRACY (July 18, 2010), http://volokh.com/2010/07/18/proof-that-other-countries-are-planning-cyberattacks-on-the-power-grid/.

184. *See supra* note 50 and accompanying text (extortion reportedly behind attack on SCADA system in foreign country).

185. ZULEY CLARKE ET AL., A BRIEF HISTORY OF HACKING (2003), *available at* http://steel.lcc.gatech.edu/~mcordell/lcc6316/Hacker%20Group%20Project%20FINAL.pdf.

186. Dan Goodin, *'Aurora' Code Circulated for Years on English Sites: Where's the China Connection*, THE REGISTER (Jan. 26, 2010, 11:02 AM GMT), http://www.theregister.co.uk/2010/01/26/aurora_attack_origins/; Jaikumar Vijayan, *Update: Attacks on Google May Have Been Work of Amateurs*, COMPUTER WORLD (Mar. 3, 2010), http://www.computerworld.com/s/article/print/9165518/Update_Attacks_on_Google_may_have_been_work_of_amateurs_?taxonomyId=17&taxonomyName=Security.

187. *See supra* note 152 and accompanying texts.

188. *See* Markoff & Barboza, *supra* note 73.

189. *See, e.g.*, LIBICKI, *supra* note 23, at 44.

190. *See supra* notes 153–57 and accompanying text.

191. CSIS REPORT, *supra* note 16, at 30 (United States listed as number one most likely source of cyberattacks by those surveyed); Goldsmith, *supra* note 5, at 27.

Lawrence Lessig dubbed it, code can be drafted to govern what computer systems and networks can (or cannot) do.[192] Some have proposed re-coding the Network layer to give data packets sourcing stamps that cannot be forged or disguised behind stepping stones.[193] But such wholesale changes to cyberspace architecture appear unlikely. Substantial vested interests oppose changing the Internet to render it less anonymous.

For starters, there is the coordination problem of adjusting the technology. The Internet is amazingly complicated, and re-coding it for better (if not perfect) attribution would not be trivial.[194] The latest version of TCP/IP, known as IPv6, for example, seeks to make tracing easier.[195] But, if anything, IPv6 has so far created more vulnerabilities for cyberattacks and exploits.[196] Redesigning other layers of the Internet would pose similar challenges.

Even if technological difficulties could be overcome in a coordinated manner, shifting to an identity-based Internet would be *very* expensive. Transitioning to any new system would be costly in terms of time and capital. Ongoing resistance to IPv6, which requires replacing or upgrading existing routers and other equipment, suggests many users would opt for maintaining the status quo even if socially sub-optimal.[197]

Putting aside the technological and economic difficulties, there is also a question of authority—who should have the capacity to identify sources of Internet traffic? Internet Service Providers (ISPs), for example, already require customers to agree that the ISP can investigate attribution and disclose the results of any investigation to government officials as necessary.[198] Governments also clearly want that power. Some—notably China—have taken steps to re-jigger their corner of the Internet to do just that.[199] In the United States, substantial constitutional and statutory rules dictate when

192. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 6, 89 (1999) (emphasis omitted); Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679, 681 (2003).

193. *See, e.g.*, McConnell, *supra* note 19.

194. *See* Bruce Schneier, *3 Reasons to Kill the Internet Kill Switch Idea*, AOL NEWS (July 9, 2010, 5:37 AM), http://www.aolnews.com/2010/07/09/opinion-3-reasons-to-kill-the-internet-kill-switch-idea/.

195. Jody R. Westby, *Countering Terrorism with Cyber Security*, 47 JURIMETRICS J. 297, 300 (2007).

196. *See supra* text accompanying note 172.

197. CLARKE & KNAKE, *supra* note 1, at 161; David Meyer, *Cerf: UK Government Should Offer IPv6 Upgrade Tax Credit*, ZDNET UK (Nov. 12, 2010, 3:12 PM), http://www.zdnet.co.uk/news/networking/2010/11/12/cerf-uk-government-should-offer-ipv6-upgrade-tax-credit-40090850/ (discussing need for IPv6 because all IPv4 addresses will be exhausted within two years); James Niccolai, *IPv6 Adoption Sluggish: Study*, COMPUTERWORLD (Aug. 25, 2008), http://computerworld.co.nz/news.nsf/tech/8CF2F74925C98009CC2574AC00750583.

198. *See, e.g.*, *Comcast XFINITY Customer Privacy Notice*, COMCAST, http://www.comcast.com/customerprivacy/ (last visited Apr. 4, 2011) ("Cable Act requires us to disclose personally identifiable information and individually identifiable CPNI about subscribers to high-speed Internet and phone services to a government entity in response to a subpoena, court order, or search warrant . . . .").

199. *See* Molly Buetz Land, *Google, China, and Search*, 14 ASIL INSIGHT (Aug. 5, 2010), http://www.asil.org/insights100805.cfm (discussing China's attempts to use "a combination of technological, legal, and social levers to maintain control of online content," including licensing and regulating Internet service and content providers).

and how the government can investigate domestic private conduct.[200] For example, the U.S. agency most versed in information technology—the National Security Agency—must operate under a host of rules in monitoring or investigating cyberthreats.[201] Any adoption of attribution technology by the U.S. government, therefore, must overcome the limits of existing law, or if possible, require changes to it.

Attribution, moreover, would operate in tension with a very important Internet value: speed. For the Internet to work, traffic must move from end-to-end at acceptable speeds for user communities.[202] What is "acceptable" can change over time. Today, increasing bandwidth demands from video and wireless devices have generated widespread concerns about degraded Internet service (or discrimination in favor of those who would pay for speedier access).[203] Attribution will thus likely trade off with the need for speed. To fix identities in cyberspace will place additional burdens on Network and Control layers already strained for bandwidth.

Finally, there is the issue of online norms. For many citizens, non-attribution is a value to be *celebrated*; it facilitates freedom of expression and protects individual privacy.[204] These are deeply held values in the United States generally, and its Internet community in particular.[205] Globally, Internet anonymity has allowed dissidents to speak (and act) out against authoritarian regimes that would otherwise crush them. Protesters in Egypt revealed just how much Internet technology and on-line social networking can facilitate political change, allowing coordination of resistance to President Mubarak and a redoubling of those efforts after the Egyptian government targeted an activist Google executive.[206] Thus, even as it decries cybercrime and cyberterrorism, the United States has actively celebrated non-attribu-

200. *See, e.g.*, U.S. CONST. amend. IV; Federal Wiretap Act, 18 U.S.C. §§2510–2520 (2008); Stored Communications Act, 18 U.S.C. §§2701–2712 (2006); 18 U.S.C. §3121–3127 (2006) (Pen Registers and Trap and Trace Devices); Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2009); *see also* Mehra, *supra* note 113, at 671–75 (surveying limits on federal law enforcement powers in cyberspace).

201. *See* John N. Greer, *Square Pegs in Round Cyber Holes: The NSA, Lawfulness, and the Protection of Privacy Rights and Civil Liberties in Cyberspace*, 4 J. NAT'L SEC. L. & POL'Y 139, 143–47 (2010) (reviewing NSA's constitutional and statutory authorities).

202. *See* CLARKE & KNAKE, *supra* note 1, at 161.

203. *See, e.g.*, DAVID A. WHEELER & GREGORY N. LARSEN, TECHNIQUES FOR CYBER ATTACK ATTRIBUTION, INSTITUTE FOR DEFENSE ANALYSES 20, 28 (2003); Bill D. Herman, *Opening Bottlenecks: On Behalf of Mandated Network Neutrality*, 59 FED. COMM. L.J. 103, 106 (2006); Tim Wu, *The Broadband Debate, A User's Guide*, 3 J. ON TELECOMM. & HIGH TECH. L. 69, 88–90 (2004).

204. *See, e.g.*, Jeffrey Hunker et al., *Attribution of Cyber Attacks on Process Control Systems*, *in* CRITICAL INFRASTRUCTURE PROTECTION II 87, 88 (M. Papa & S. Shenoi eds., 2009); Katyal, *supra* note 23, at 1113.

205. *See, e.g.*, LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 7–8 (2001); Zittrain, *supra* note 17, at 1978.

206. *See, e.g.*, Ari Melber, *Can Egypt's Internet Movement Be Exported?*, THE NATION (Feb. 18, 2011), http://www.thenation.com/print/article/158717/can-egypts-internet-movement-be-exported.

tion in several high-profile incidents, such as those who use it to resist the government in Iran.[207]

Any attempt to "fix' attribution, therefore, will encounter charges that doing so will "harm" privacy, limit freedom of expression, or other existing values.[208] Indeed, federal efforts to develop a system just to defend U.S. government computers (the "EINSTEIN program") have already raised a host of privacy objections.[209] When one combines these objections with existing law, the financial costs, and technological difficulty of the project, the prospects for more regular attribution in cyberspace appear dim.

C. The Consequences of the Attribution Problem

1. *The Existing Laws are Insufficient.*

Cyberthreats of all kinds are rampant and growing. In 1995, the Defense Department faced 250,000 attempted attacks or exploits on its computer systems; by 2006 the number stood at 6 million; by 2008 it had risen to *300 million*.[210] Meanwhile, large-scale DDoS and SCADA system attacks pose increasing threats to critical infrastructure industries.[211] Cybercrime has risen exponentially as well. From 1988 to 2003, the Computer Emergency Response Team (CERT)—set up to monitor and assist in repelling U.S. cyberthreats—watched reported incidents rise from 6 to 137,529. In 2004, CERT stopped watching because "attacks against Internet-connected systems have become so commonplace that counts of the number of incidents reported provide little information with regard to assessing the scope and impact of attacks."[212] CERT believed that 80% of cyberthreats actually went unreported because companies feared the reputational consequences of conceding cyber losses.[213]

At the same time, legal accountability for cyberthreats is exceedingly rare. At most, five percent of cybercriminals are arrested or convicted.[214] No state has ever formally admitted its complicity in a cyberattack or cyberexploita-

---

207. *See* Sec'y of State Hillary Rodham Clinton, Remarks on Internet Freedom at the Newseum (Jan. 21, 2010), transcript *available at* http://www.state.gov/secretary/rm/2010/01/135519.htm.

208. *See, e.g.*, Brian Naylor, *New U.S. Cyber Command Raises Privacy Concerns*, NPR (June 26, 2009), http://www.npr.org/templates/story/story.php?storyId =105962021; Ryan Singel, *Cyberwar Hype Intended to Destroy the Open Internet*, WIRED (Mar. 1, 2010), http://www.wired.com/threatlevel/2010/03/cyber-war-hype/.

209. *See, e.g.*, Gregory T. Nojeim, *Cybersecurity and Freedom on the Internet*, 4 J. NAT'L SEC. L. & POL'Y 119, 122 (2010); Jessylyn Radack, *Cyber Overkill; A Project to Safeguard Governmental Computers, Run by the NSA, is Too Big a Threat to Americans' Privacy*, L.A. TIMES, July 14, 2009, at A19.

210. UNITED STATES GENERAL ACCOUNTING OFFICE, INFORMATION SECURITY: COMPUTER ATTACKS AT DEPARTMENT OF DEFENSE POSE INCREASING RISKS 18 (1996), *available at* http://www.gao.gov/archive/1996/ai96084.pdf; Hamilton, *supra* note 71.

211. CSIS REPORT, *supra* note 16, at 5–10.

212. *CERT Statistics*, CERT, http://www.cert.org/stats/ (last visited Apr. 4, 2011) (last updated Feb. 12, 2009) (CERT now tracks and reports on vulnerabilities instead).

213. CRS REPORT, *supra* note 93, at 29.

214. *Id.*

tion; nor is there any consensus on any state having done so in violation of international law.[215] We still do not know who authored the 2007 Estonia attacks, the 2008 Georgian attacks, the July 4, 2009 attacks, or the implanting of logic bombs in the U.S. power grid. Nor do we have any certainty on who exfiltrated valuable data from the Joint Strike Fighter program or Google. We do not even know if various accidents involving computer error really were negligence or, instead, the result of subtle planning.

Attribution problems are not unique to cyberspace. It is a problem for criminal and international laws generally.[216] Elsewhere, scholars such as Gary Becker have suggested the law ought to use harsher penalties to increase deterrence for crimes that have low conviction rates.[217] The Defense Department has explicitly referenced this theory in suggesting that "the US should take swift and effective action in every case in which it can attribute an offensive action to a particular adversary."[218]

It is not clear, however, that this Beckerian approach to proscriptions actually works, especially when translated into cyberspace. The limited extant evidence suggests that the size of any prospective penalty may not greatly deter criminals.[219] The fact that these cyberthreats can originate in a country other than that of the victim(s) creates a jurisdictional barrier to accountability that allows perpetrators to further discount the chances of getting sanctioned.

2. *The Existing Laws are Dangerous.*

The law's response to cyberthreats may be more than insufficient; it may be dangerously misguided. If you do not know who authored an attack, how can you know whether to treat it as a crime or an act of war? Attribution problems create serious risks of mistakes and miscalculations over *which* set of rules applies to a cyberattack or exploit.[220] Those mistakes may generate unintended responses, including the use of military force.

---

215. LIBICKI, *supra* note 23, at 66.

216. *See, e.g.*, *Alexander Q&A*, *supra* note 24, at 23. Even where attribution occurs, it can take months or years, as was the case with those responsible for the 1988 Lockerbie bombings of Pan Am Flight 103. LIBICKI, *supra* note 23, at 96.

217. *See, e.g.*, Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169, 176 (1968); Katyal, *supra* note 23, at 1006. Katyal offers another solution—increasing the cost to cybercriminals of engaging in the unwanted behavior. Like the sanctions model for deterrence, increasing costs could deter, particularly for low-impact cyberthreats. *See* Katyal, *supra* note 23, at 1040–41. The prospects for nation states doing this—such as by regulating information technology—are unclear. *See infra* notes 228–233 and accompanying text.

218. *Alexander Q&A*, *supra* note 24, at 23.

219. *See, e.g.*, Paul H. Robinson & John M. Darley, *The Role of Deterrence in the Formulation of Criminal Law Rules: At Its Worst When Doing Its Best*, 91 GEO. L.J. 949, 953, 956 (2003).

220. Brenner, *supra* note 21, at 433–40; *Cyberwar: It is time for countries to start talking about arms control on the Internet*, ECONOMIST, July 3, 2010, at 11.

The U.S. Defense Department, for example, has indicated that international law does not require "that we know who is responsible before we take defensive action."[221] Thus, if a cyberattack disabled critical infrastructure or killed enough people, the United States *could* treat it as an act of war—and respond with force by invoking the right of self defense—without knowing for sure who launched the attack.[222] Indeed, existing proposals would impute responsibility to the state to whose territory the attack was traced.[223] But what if the attack only *looked* like it came from that state, when in fact it had not?[224] Or, even if the cyberattack did originate in that state, what if its government knew nothing since the authors were hackers, criminals, terrorists, or even foreign agents?[225] That state may believe that the rules on cybercrime govern, and that the U.S. response was unlawful. If sufficiently threatened, that state might even respond with its own acts of self-defense, suddenly escalating the situation into an armed conflict.

If this last possibility seems remote, consider it in reverse. Many, if not most cyber attacks originate in or transit U.S. territory.[226] Assume another state attacks the United States in self-defense for a cyberattack it believes originated here. Would the United States accept responsibility for such an attack if its forces did not perpetuate it? That cyberattacks may have instantaneous impacts or cascading, indirect effects beyond their intended target only compounds the possibility that mistakes will be made about the appropriate set of legal rules and responses to apply.

3. *Alternative Legal Responses to Cyberthreats.*

If proscriptive rules do not work, what can law do to deter?[227] There are two other regulatory approaches possible, namely regulating the instrument (here, the technology) that delivers cyberthreats, or regulating victims so they avoid threats in the first place. Both types of proposals already exist, although each faces an uphill battle to become law.

---

221. *Alexander Q&A*, *supra* note 24, at 12.

222. Ongoing coordination questions over the exact division of responsibilities between U.S. Cybercommand, NSA, and the Department of Homeland Security for responding to cyberattacks is a further issue that may impact the question of when, and how, the U.S. military responds to a cyberattack. *See* Brenner, *supra* note 21, at 440; *infra* note 297 and accompanying text.

223. *See supra* note 152 and accompanying text.

224. CLARKE & KNAKE, *supra* note 1, at 212 ("the greatest potential for accidental cyberwar is likely to come in the form of retaliating against the wrong nation because we were misled as to who attacked us").

225. There are reports, for example, that North Korean cyberforces operate out of China because North Korea has so few Internet links. *Id.* at 27–28.

226. *See* Jack Goldsmith, *Can We Stop the Cyber Arms Race?*, WASH. POST, Feb. 1, 2010, at A17.

227. I am limiting my analysis in this paper to alternative legal deterrents to cyberthreats in lieu of proscription. *Cf.* McConnell, *supra* note 19 (proposing a nuclear deterrence model for cyberthreats). Cyberthreats, however, do not analogize well to nuclear threats. *See* CLARKE & KNAKE, *supra* note 1, at 189–95; LIBICKI, *supra* note 23, at xiv, 27–32.

In 1998, the Russian Federation proposed that U.N. Member States agree by treaty to ban cyberweapons.[228] It received a chilly response, with states emphasizing enhanced computer security measures instead.[229] Today, even as it stands accused of cyberattacks on Estonia and Georgia, Russia still lobbies for international rules in cyberspace paralleling those that exist for nuclear, chemical, and biological weapons.[230]

The United States, China, and a dozen other states have agreed to new negotiations on cyberthreats but have yet to endorse Russia's proposed legal framework.[231] The banning of hacking codes raises very different issues than limiting the distribution of nuclear technology. Unlike nuclear weapons, hacking skills are distributed among populations worldwide and can be developed and deployed with material that is inexpensive and easy to obtain. Moreover, difficulties in distinguishing cyberattack and cyberexploitation capacities pose a significant dilemma, since many states (including the United States and China) will resist banning cyberespionage that international law currently tolerates.[232] And anonymity, of course, creates serious problems with any proposed verification of "disarmament," which served as the central tenent for arms control agreements.[233]

If hacking technology cannot—or will not—be banned, perhaps the last legal remedy lies in targeting victims. The most obvious approach involves new laws (domestic or international) that focus on cybersecurity.[234] Many companies and users invest only in the security that they feel is necessary, without regard to how their defenses implicate the United States as a whole. Users often have little incentive to spend the time or money necessary to

228. *See* U.N. GAOR, Letter dated September 23, 1998 from the Permanent Representative of the Russian Federation to the United Nations to the Secretary General concerning Agenda Item 63, U.N. Doc. A/C.1/53/3 (Sept. 30, 1998). Although I focus on proposals to create international law rules regulating hacking technology, Neal Katyal has made a similar proposal for purposes of U.S. law. Katyal, *supra* note 23, at 1076.

229. Of nine states submitting views, only Cuba and Belarus favored negotiations to restrict information warfare. U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of Information Security*, U.N. Doc. A/54/213 (Aug. 10, 1999). Ultimately, the U.N. General Assembly passed Resolution 53/70, calling on Member States simply to promote consideration of existing and potential threats to information security. G.A. Res. 53/70, U.N. GAOR, 53rd Sess., U.N. Doc. A/RES/53/70 (Jan. 4, 1999).

230. *See* John Markoff & Andrew E. Kramer, *In Reversal, U.S. Talks to Russia on Web Security*, N.Y. TIMES, Dec. 13, 2009, at A1.

231. *See* Siobhan Gorman, *U.S. Backs Talks on Cyber Warfare*, WALL ST. J., June 4, 2010, at A3.

232. *See* CLARKE & KNAKE, *supra* note 1, at 228.

233. Even if regulations could overcome these technological differences, larger concerns may still stymie this option. Russia's proposals, for example, seek to restrict "politically destabilizing" speech in cyberspace, but the United States often views such speech positively and defends it as freedom of expression. Markoff & Kramer, *supra* note 230.

234. Katyal, *supra* note 23, at 1077 (discussing government mandated victim precautions against cybercrime); *Alexander Q&A*, *supra* note 24, at 23 ("First and foremost, the most effective way to deter adversaries is to increase the security of our own networks . . . better security solutions must be encouraged for all U.S. public and private networks.").

protect their systems from a botnet infection that they will not even realize they have.[235]

To correct for this problem, governments could require and oversee minimum defenses for the Internet and its users. The Department of Defense, for example, is considering minimum cybersecurity commitments from its vendors in the safeguarding of unclassified information.[236] Several U.S. Senators have sponsored a bill that would give the U.S. federal government authority to mandate security updates for private companies as well as the creation of a "kill switch" the U.S. government could use to cut off a particularly devastating cyberattack.[237] But like proposals to better attribution, privacy and civil liberties objections to these ideas abound.[238] In the United States, at least, there is deep skepticism about government regulation of private security networks.[239]

None of this should suggest that restricting information technology that can do real harm or imposing minimum security requirements are bad ideas. If attribution saps proscriptions of their deterrent force, either approach could provide an alternative path to deterrence. So long as these proposals meet stiff resistance, however, there is a need to consider additional ways for the law to deter. One idea that has yet to receive any real policy or scholarly attention is my proposal: a duty to assist those facing severe cyberthreats.

III. A Duty to Assist Victims of Cyberthreats

On December 7, 2009, the Norwegian vessel *MT Nordik Spirit* found itself under attack by machine gun fire from pirates off Somalia's coast. The ship's captain took evasive maneuvers and sent out a distress call. An Indian Navy ship responded, sending helicopters full of marine commandos. When the pirates saw this show of force, they abandoned the attack and fled. The vessel and its crew escaped unharmed.[240]

The Indian warship helped because international law required it to do so: any and all vessels must provide whatever assistance they can on receiving a

235. Goldsmith, *supra* note 5.

236. Defense Acquisition Regulation Supplement: Safeguarding Unclassified Information, 75 Fed. Reg. 9563 (March 3, 2010).

237. S. 3480, 111th Cong. (2010); *see also* Joe Lieberman et al., *Arming the United States for CyberWar*, AOL News (July 9, 2010, 5:38 AM), http://www.aolnews.com/opinion/article/opinion-arming-the-us-for-cyber-war/19547156.

238. *See* Schneier, *supra* note 194. Those objections exist even if the only victim with minimum security requirements is the U.S. government. *See* Radack, *supra* note 209.

239. *See* Goldsmith, *supra* note 5. Thus, some have labeled the idea of a "Perfect Citizen" National Security Agency program that would monitor and protect U.S. critical infrastructure an Orwellian enterprise. *See, e.g.*, Siobhan Gorman, *U.S. Plans Cyber Shield for Utilities, Companies*, Wall St. J., July 8, 2010, at A3.

240. *Navy Foils Pirate Attack on Tanker in Gulf of Aden*, The Times of India (Dec. 8, 2009, 2:42 AM IST), http://timesofindia.indiatimes.com/india/Navy-foils-pirate-attack-on-tanker-in-Gulf-of-Aden/articleshow/5312407.cms.

distress call, or SOS. The SOS triggers a duty to assist ("DTA") that marshals available resources to help victims avoid or recover from harm. Other DTAs exist in both domestic and international contexts, such as a nuclear accident or a pilot's Mayday call.[241]

Although victims of cyberthreats sometimes get help today, there is currently no cognizable DTA for the Internet. The conditions under which many severe cyberthreats arise, however, parallel those for which the SOS exists. To the extent that some cyberthreats do differ from those on the high seas, other DTAs offer alternative formulations that could apply in cyberspace. In other words, states *can* create a DTA for cyberthreats. They have options, moreover, in terms of both the content of such a duty and the process by which they impose it. International law offers great flexibility to states in deciding the precise contours and requirements of any e-SOS.

A. The SOS and the DTA at Sea

For almost a century, SOS signals have served as the primary vehicle for dealing with emergent threats to life and property in the maritime environment.[242] Regardless of the cause—pirates, weather, equipment failure, even whales—the SOS affords those in distress a universal cry for help.[243] Today, both customary international law[244] and major multilateral maritime treaties—such as the U.N. Convention on the Law of the Sea—require ships receiving an SOS signal to provide whatever assistance they can offer.[245]

Regulations promulgated by the International Maritime Organization pursuant to the Safety of Life at Sea Convention (SOLAS) further elaborate this obligation in two key respects.[246] First, the ship in distress has "the

241. *See infra* Part III.C.

242. SOS is not an acronym, but a specific Morse Code, represented as ". . .---. . ." It was adopted as the standard distress signal in 1912 by the London International Telegraph Convention. G.E. WEDLAKE, SOS: THE STORY OF RADIO-COMMUNICATION 50 (David & Charles 1973).

243. *See, e.g.*, *British Couple's Yacht Sunk by Whale in Caribbean*, TELEGRAPH (U.K) (June 10, 2009, 7:24 PM BST), http://www.telegraph.co.uk/news/worldnews/centralamericaandthecaribbean/5496679/British-couples-yacht-sunk-by-whale-in-Caribbean.html (couple rescued by another yacht after sending out distress signal when a whale struck their vessel, sinking it).

244. In 1956, the U.N. International Law Commission indicated a maritime DTA "states the existing international law." Rep. of the Int'l Law Comm'n, 8th Sess., Apr. 23–July 4, 1956, art. 36, U.N. Doc. A/3159; U.N. GAOR, 11th Sess., Supp. No. 9 (1956), *reprinted in* [1956] 2 Y.B. Int'l L. Comm'n 253, 281 (1956). In 1985, the International Maritime Organization echoed that view. *See* C.54/17(d), IMO Council, 1985; *see also* Mark Pallis, *Obligations of States Towards Asylum Seekers at Sea*, 14 INT'L J. REFUGEE L. 329, 333–34 (2002) (concluding DTA is customary international law "binding on all states").

245. *See, e.g.*, United Nations Convention on the Law of the Sea art. 98, Dec. 10, 1982, 1833 U.N.T.S. 397 [hereinafter UNCLOS] ("Every State shall require the master of a ship flying its flag, in so far as he can do so without serious danger to the ship, the crew or the passengers . . . to proceed with all possible speed to the rescue of persons in distress, if informed of their need of assistance, in so far as such action may reasonably be expected of him . . . ."); United Nations Convention on the High Seas art. 12, Apr. 29, 1958, 13 U.S.T. 2312 (same); *see also* International Convention on Salvage art. 10, Apr. 28, 1989, 1953 U.N.T.S. 193; International Convention on Maritime Search and Rescue, Apr. 27, 1979, T.I.A.S. No. 11,093, Annex 2.1.9–2.1.10 [hereinafter SAR].

246. SOLAS, *supra* note 28, at reg. 33(1).

right to requisition" one or more ships offering assistance. Once requisitioned, the assisting vessel has an obligation to assist until released from its duty by the vessel in distress or the rescue service concerned.[247] Second, if a ship receiving a distress signal is "unable or, in the special circumstances of the case, considers it unreasonable or unnecessary to proceed" to assist, it has to produce a written record of its reasons.[248]

Anyone in distress at sea, "even though an enemy," can utilize the DTA.[249] Distress itself is widely understood to cover cases where the vessel is at risk or lives are otherwise in danger.[250] Both examples suggest distress involves a combination of at least three conditions: an *incapacity* (a situation the vessel cannot remedy on its own) that is *severe* (absent help the vessel or lives aboard may be lost); and *urgent* (help is needed now, postponing assistance is inadvisable). Remove any one of these elements and it becomes hard to characterize a situation as one of distress. A problem to a ship's sails that the crew can repair does not incapacitate it any more than a broken air conditioner the crew cannot repair poses a severe risk to their lives or the vessel.

Ultimately, the SOS empowers victims to decide for themselves when they are in enough distress to call for help. To ensure victims only do so in cases of real need, SOLAS regulations prohibit the misuse or abuse of distress signals.[251] The U.S. law implementing these obligations criminalizes false and fraudulent signals as well.[252]

Assuming a victim in distress issues an SOS, the DTA requires *any* vessel receiving it to respond speedily, whether a Navy destroyer or a pleasure vessel.[253] The victim also has the power to sort through assistance offers and decide which can best counter the threat at hand.[254] The rules do not provide guidance on how a victim should select among offers (nor what types of assistance others must offer). Presumably, this is because distress situations come in endless combinations of weather, the nature of the distress, and the

247. *Id.* at reg. 33(2)–(4). The DTA otherwise ends when a vessel learns it has not been requisitioned. *Id.* SOLAS obligates governments to cooperate to ensure assisting vessels are released from their obligations with as little deviation from intended voyages as possible, as long as doing so does not further endanger the safety of life at sea. *Id.* at ¶ 1.1.

248. *Id.*

249. International Convention for Unification of Certain Rules of Law with Respect to Assistance and Salvage at Sea art. 11, Sept. 23, 1910, 37 Stat. 1658 (DTA covers "assistance to everybody, even though an enemy, found at sea in danger of being lost"); SAR, *supra* note 245, Annex 2.1 (assistance is due "regardless of the nationality or status of such a person or the circumstances in which that person is found").

250. *See, e.g.*, Pallis, *supra* note 244, at 338.

251. *See* SOLAS, *supra* note 28, at reg. 35.

252. 47 U.S.C. § 325 (1996) (stating "No person within the jurisdiction of the United States shall knowingly utter or transmit, or cause to be uttered or transmitted, any false or fraudulent signal of distress, or communication relating thereto"); *see also Three Plead Guilty to Making False Distress Calls to Coast Guard*, WRAL (Mar. 13, 2010), http://www.wral.com/news/news_briefs/story/7227661/.

253. *See* SOLAS, *supra* note 28, at reg. 33(1).

254. *Id.* This power also extends to any government search and rescue operation that receives and responds to a victim's distress signal. *Id.*

conditions of vessels involved (such as their relative size, available equipment, and persons on board).[255]

Vessels in a position to assist can decline to do so if they can show that they cannot help, there is no need for their help, or it would be unreasonable to require their help.[256] With pirates, for example, a pleasure yacht might decline to assist a vessel under attack because it had no weapons (or other skills) to repel them, or because it might be unreasonable to ask private actors to risk their vessel and lives in that effort. In other words, the DTA distills down to a duty of *reasonable* effort.[257]

Most countries—including the United States—have incorporated the SOS and its DTA into their domestic law.[258] It applies to all maritime environments at all times.[259] The laws of war even have a modified DTA among adversaries at sea.[260]

States look to the SOS to serve a specific objective—to avoid unwanted loss of lives and the vessels that support them. And it has done so.[261] States provide whatever assistance they can to meet the need, regardless of who called for help. In September of 2009, for example, a South Korean helicopter responded to a distress call from a North Korean ship under attack by pirates and dispersed them.[262] Six months later, North Korea would torpedo a South Korean warship.[263]

Obviously, the SOS and the DTA cannot preclude every ship from sinking or every person from drowning or suffering harm at sea.[264] But the system works because all involved value the effort. The DTA tries to respond to threats—like hurricanes and icebergs—that generally lie beyond the ability

255. Frederick J. Kenny & Vasilios Tasikas, *The Tampa Incident: IMO Perspectives and Responses on the Treatment of Persons Rescued at Sea*, 12 Pac. Rim. L. & Pol'y 143, 150 (2003).

256. *Id.* (quoting SOLAS, *supra* note 28, at reg. 33).

257. In this respect, the DTA contrasts with a related duty—the duty to rescue at sea—that requires coastal states to have "adequate and effective" search and rescue facilities. UNCLOS, *supra* note 245, art. 98(2); *see also* SOLAS, *supra* note 28, at reg. 7; SAR, *supra* note 245, as amended, Annex, ch. 1, ¶ 1.3.2 (defining "rescue" as "an operation to retrieve persons in distress, provide for their initial medical or other needs, and deliver them to a place of safety"). The structure of this duty to rescue might provide an alternative basis for cyberdeterrence besides the e-SOS.

258. *See, e.g.*, 46 U.S.C. § 2304 (2006).

259. *Id.*; *see also* SOLAS, *supra* note 28, at 7(1).

260. Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea art. 18, Aug. 12, 1949, 6 U.S.T. 3217 (after each engagement, parties have to collect and protect shipwrecked, wounded, and sick persons).

261. *See, e.g.*, Nick Allen & Gary Cleland, *Sinking Antarctic Cruise Ship Evacuated*, Telegraph (U.K.) (Nov. 23, 2007, 1:47 GMT), http://www.telegraph.co.uk/news/uknews/1570295/Sinking-Antarctic-cruise-ship-evacuated.html (detailing SOS-related rescue of 154 passengers and crew).

262. Int'l Maritime Bureau, Piracy and Armed Robbery Against Ships, Annual Report 35, 80 (2010) [hereinafter IMB Report]; Anne Barrowclough, *South Koreans Defend North Korean Ship as Pirates Attack Near Aden*, Times (U.K.), May 5, 2009, http://www.timesonline.co.uk/tol/news/world/africa/article6222591.ece.

263. Choe Sang-Hun, *South Korea Publicly Blames the North for Ship's Sinking*, N.Y. Times, May 19, 2010, http://www.nytimes.com/2010/05/20/world/asia/20korea.html?_r=1.

264. *See, e.g.*, IMB Report, *supra* note 262, at 13, 25 (reporting 47 hijackings of vessels by Somali pirates in 2009, plus 4 deaths, 10 injuries, and 867 hostages).

of governments to control. It also tries to forestall harms that humans—like pirates—can impose.[265] Today, a fifty-nation effort exists off Somalia's coasts to deter piracy and assist its victims. Those efforts have paid off as the pirates' success rate has gone from 63% in 2007, to 34% in 2008, to 25% in 2009.[266]

B. A Sea of Cyberthreats: Similarities to the Ocean Environment

Packet-switching is not sailing, any more than cyberspace is real space.[267] And yet, the threat conditions of both environments contain striking parallels. As discussed, cyberspace faces threats that range widely in terms of their direct and indirect effects, causes, and authors.[268] So does the sea. Weather conditions can make sailing uncomfortable or deadly; equipment problems can inconvenience or destroy. And when the ship sinks, the loss is not just felt by the vessel itself, but indirectly impacts whatever crew and cargo it carried. Depending on the cargo—say, oil—additional economic and environmental losses may occur as well.

Like cyberspace, threats at sea can have internal (equipment failure) or external (weather, collisions, pirates) causes. And like many cyberthreats, sometimes their causes will be entirely unclear; a vessel may not know why it is sinking or why its cargo fell overboard, just that it did so.[269] Even when a vessel can identify the cause of the threat, such as pirates, it may not be able to identify them for accountability purposes. Pirates generally do not fly a state's flag, and if they do, it may not be their own.[270] Nation states may be able to identify, track, or even capture pirate ships, but those capacities do not necessarily translate into full attribution. Even when captured, attribution may still be difficult because the pirate's identity, age, or role may not be fully discernable.[271] Like cyberspace, piracy proscriptions have

265. UNCLOS, *supra* note 245, art. 101 (defining piracy and requiring states to combat it).

266. *See, e.g.*, Jacquelyn S. Porth, *Int'l Navies Coordinate to Deter Pirates*, AMERICA.GOV (Feb. 19, 2010), http://www.america.gov/st/peacesec-english/2010/February/20100219174011SJhtroP0.8000299.html#. Deterring Somali pirates entirely is a harder proposition given the geopolitical landscape, but attacks did decline in early 2010. *Pirates Face New Resistance as Navies Strike Back*, INT'L CHAMBER OF COMMERCE (July 15, 2010), http://www.iccwbo.org/index.html?id=38030. More recent news reports suggest, however, that 2011 piracy levels may not be continuing to decline. *See* Brad Knickerbocker, *Somali Pirate Gets Stiff Sentence in US Court. Will it Deter Piracy?*, CHRISTIAN SCI. MONITOR (Feb. 16, 2011), http://www.csmonitor.com/USA/Justice/2011/0216/Somali-pirate-gets-stiff-sentence-in-US-court.-Will-it-deter-piracy.

267. *See* POST, *supra* note 14, ch. 1.

268. *See supra* Part I.

269. Sharon Carty, *When Cargo Gets Lost at Sea, Firms Can See Big Losses and Shortages*, USA TODAY, Aug. 4, 2006, at 3B (2000 to 10,000 containers fall off ships each year).

270. If a pirate ship had previously flown under the flag of a state, a state's laws determine whether to treat the ship as one of its own. UNCLOS, *supra* note 245, art. 104.

271. The age of the one Somali pirate prosecuted in U.S. court, for example, remains disputed. Knickerbocker, *supra* note 266.

not fared well in the face of anonymity and the jurisdictional challenges posed by where pirates act.[272]

Strikingly, the three elements giving rise to the SOS at sea—incapacity, severity, and urgency—characterize cyberthreats as well. As at sea, the timing and scale of some cyberthreats (large-scale DDoS attacks, spear phishing) can overwhelm the most sophisticated individuals, groups, and even states. The evidence suggests, moreover, that incidents of such incapacity are on the rise. Estonia felt so helpless in the face of DDoS attacks on its networks it asked NATO for military assistance.[273] Even the mighty Google had to concede a need for help with Operation Aurora, contracting with the NSA for assistance.[274]

In terms of severity, notably, most losses from cyberthreats involve risks of only economic loss. Traditionally, the law of the sea handles such losses under different rules, known as salvage.[275] Salvors provide assistance in recovering property lost at sea, but are paid to do so.[276] Does this mean that economic losses from exploits like Operation Aurora or the attacks on Estonia are not severe (at least for purposes of mandating assistance)? It might. Losses of life versus those of money may simply be different categories, warranting different treatment. I would argue, however, that the potential systemic effects and scale of economic losses from some cyberthreats are sufficiently different from losses at sea to suggest reconsidering that conclusion.

When something goes wrong at sea, its severity is judged by the problem's potential impact on a *single* vessel or its crew. From that perspective, potential economic losses are relatively limited. To be sure, the loss of a single vessel or its contents may cost the owners (or, more likely, insurance carriers) millions of dollars. But, the direct and indirect impacts of the loss run only to that vessel and its cargo.

In contrast, some cyberthreats have the potential for *systemic* consequences. As a result, focusing on individual economic losses may be an inappropriate measure of the threat's severity. For example, a cyberthreat targeting the

---

272. *See* Eugene Kontorovich, *A "Guantanamo on the Sea": The Difficulties of Prosecuting Pirates and Terrorists*, 98 CAL. L. REV. 243, 262, 272–73 (2010).

273. *See Newly Nasty*, *supra* note 4, at 51. Estonia later concluded an agreement with NATO on cyberdefense. *NATO and Estonia Conclude Agreement on Cyber Defence*, NATO (Apr. 23, 2010), http://www.nato.int/cps/en/natolive/news_62894.htm.

274. John Markoff, *Google Asks Spy Agency to Look into Cyberattacks*, N.Y. TIMES, Feb. 5, 2010, at A6. There are, of course, alternative possible motivations that might explain both Estonia's and Google's requests for help. Estonia might have wanted to solidify its relationship with NATO; Google might have been seeking to reorient its market position in China.

275. The DTA does, however, apply to pirates even if the losses imposed are largely economic. *See* James Kraska & Brian Wilson, *The Pirates of the Gulf of Aden: The Coalition is the Strategy*, 45 STAN. J. INT'L L. 243, 255 (2010).

276. International salvage law regulates how property lost at sea (whether a vessel or its cargo) can be recovered and how much those who do so may charge for rescuing it. *See generally* International Convention on Salvage, *supra* note 245; Jason Parent, *No Duty to Save Lives, No Reward for Rescue: Is that Truly the State of International Salvage Law?*, 12 ANN. SURV. INT'L & COMP. L. 87 (2006).

Internet's very architecture could produce losses system-wide, which is rarely, if ever, the case with threats at sea. Similarly, attacking a stock exchange or financial system would not just impact individual traders or bank accounts, but the ability of the system itself to function. Cyberthreats often succeed by *aggregation*; individual losses are kept at minimal or moderate levels, but, taken together, impose a heavy toll, such as the $1 trillion in data theft losses in 2008 alone.[277] Given their aggregate impact, it might make sense to adopt a broader DTA with severity defined in terms of both threats to life *and* systemic economic losses.

Where a cyberthreat is severe and beyond a victim's capacity to handle, urgency does not seem like it would be much of an issue. Cyberthreats can arise literally at the speed of light, having immediate impacts on computer systems or networks.[278] As with severity, however, the urgency criterion may require further thinking. For example, what to do with logic bombs in a SCADA system or a cyberexploitation from a major company like Google? The logic bomb is not causing any immediate harm and the systemic impact of the data theft is debatable (as is any impact on human life). As far as the potential victim is concerned, however, a logic bomb could go off at any time, or Google might discover what started out as data theft has suddenly affected the integrity of its core operations (with arguably systemic effects beyond Google's bottom line). Thus, unlike at sea, where urgency is a function of present threats, urgency in cyberspace might need to encompass both present threats, and those threats that have a capacity to become present threats at any time.

C. Other DTAs as Examples for Cyberspace

Despite strong similarities, deriving a DTA for cyberspace does not depend solely on comparisons with the law of the sea. The concept has wider and deeper roots. Vattel—on whose theories much of the present international legal order rests—posited as his *first general law* the idea that states owe other states a duty of mutual assistance, so long as doing so does not cause injury to the assisting state.[279] From that general principle, states have agreed to specific DTAs that vary in terms of (a) *what* threats are covered, (b) *which* victims can invoke the duty, (c) *who* has to provide assistance, and (d) *what* kinds of assistance they must give.

First, in terms of threats, most existing international DTAs involve serious risks to human life or the environment, such as those created by land mines, nuclear accidents, or the use of chemical weapons.[280] Like vessels

277. President Obama Speech, *supra* note 6, at 2.

278. *See* Moore et al., *supra* note 34, at 38 (discussing the speed of the Slammer worm).

279. EMERICH DE VATTEL, THE LAW OF NATIONS §§ 12–14 (J. Chitty ed., 1854) (1758).

280. *See, e.g.*, The Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on Their Destruction art. 5, Sept. 18, 1997, 36 I.L.M. 1507 [hereinafter Landmines Convention]; Convention on the Prohibition of the Development, Production, Stockpiling

under the DTA at sea, states have agreed to assistance for aircraft in distress.[281] In at least one case involving space objects, the DTA extends to recovering property and returning it to its owners.[282] There is also a preexisting DTA involving cyberspace. Under the Convention on Cybercrime, the commission of cybercrimes can mandate requests for investigation and other forms of law enforcement assistance from one party to another.[283]

Second, in terms of which victims can invoke the duty, the DTA at sea is exceptional in permitting private parties to ask for help themselves. Usually, only states can ask for help under international law.[284] That is the case with cybercrime investigations, nuclear accidents, chemical weapons, and demining landmines.[285]

Third, when it comes to providing assistance, international law again has tended to focus on imposing the duty primarily on states. Other than the law of the sea, only combatants have DTAs under international law, and then only in fairly narrow circumstances.[286] Otherwise, the assistance requirement falls on states. Sometimes the duty applies to any state in a position to help, as in the case of astronauts, landmines, and chemical weapons.[287] Where the threat arises in a specific territory—like a plane crash—the duty only applies to the state on whose territory the incident occurred.[288] In several cases, international organizations also must assist or facilitate assistance, most notably in the case of chemical weapons and nuclear accidents.[289]

---

and Use of Chemical Weapons and on Their Destruction art. X, Sept. 3, 1992, 1974 U.N.T.S. 45 [hereinafter CWC]; Convention on Assistance in the Case of a Nuclear or Radiological Emergency art. 2, Sept. 26, 1986, 25 I.L.M. 1369 [hereinafter Nuclear Assistance Convention].

281. *See, e.g.*, Convention on International Civil Aviation art. 25, Dec. 7, 1944, 61 Stat. 1180 [hereinafter ICAO] ("Each contracting State undertakes to provide such measures of assistance to aircraft in distress in its territory as it may find practicable . . . .").

282. Agreement on the Rescue of Astronauts, the Return of Astronauts, and the Return of Objects Launched into Outer Space art. 5, Apr. 22, 1968, 19 U.S.T. 7570, T.I.A.S. No. 6599 [hereinafter Space Objects Treaty]. This treaty and the Outer Space Treaty that preceded it also provide a DTA to astronauts in distress. *Id.*; Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies art. V, Jan. 27, 1967, 18 U.S.T. 2410, T.I.A.S. No. 6347.

283. Convention on Cybercrime, *supra* note 18, art. 25.

284. This stands in contrast, of course, with domestic jurisdictions, where individuals are allowed to request help, whether by calling 911, or sending out another signal, like a stranded hiker's six flashes of light. *See* Public Safety and Homeland Security Bureau, *9-1-1 Service*, FED. COMMC'N COMM'N, http://www.fcc.gov/pshs/services/911-services/ (last visited Feb. 15, 2011).When a hiker sends out a distress signal, the response is typically undertaken by governmental authorities or government-authorized volunteer response units. *See, e.g.*, MOUNTAIN RESCUE ASS'N, http://www.mra.org (last visited Feb. 16, 2011).

285. *See, e.g.*, Convention on Cybercrime, *supra* note 18, art. 25; CWC, *supra* note 280, art. X(8).

286. *See* Geneva Convention Relative to the Protection of Civilian Persons in Time of War arts. 16, 27, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 135.

287. CWC, *supra* note 280, art. X(8); Space Objects Treaty, *supra* note 282, art. 2; Landmines Convention, *supra* note 280, art. 5.

288. ICAO, *supra* note 281, art. 25; *see also* Space Objects Treaty, *supra* note 282, art. 5.

289. CWC, *supra* note 280, art. X(8) (regarding Organization for the Prohibition of Chemical Weapons); Nuclear Assistance Convention, *supra* note 280, art. 2 (regarding International Atomic Energy

In several areas, moreover, international law has gone beyond a DTA, imposing on states a duty to rescue, assist, or warn whether or not they have received a call for help.[290] The duty applies when the state learns of the risk. Thus, states aware of risks in areas where they are responsible have a duty to warn other states of such risks.[291] States have to help civilian aircraft in distress whether they ask for it or not.[292] And once a state knows that an astronaut is in distress or a space object has landed back on earth, it has to notify the launching state of the situation and help the astronaut, or recover and return the object.[293]

Within their own territories, states vary in extending the DTA to private parties. This policy choice has domestic roots; though civil law countries generally impose such a duty,[294] common law countries do not.[295] The proper scope of a domestic DTA is a controversial topic. Opponents find such assistance unnecessary since help *is otherwise available* from domestic law enforcement, firefighters, etc.[296] That assumption does not translate as easily into cyberspace. Governments can exercise some control over the Internet through their own territorial jurisdiction. The global nature of these threats, however, creates substantial collective action problems among governments that preclude effective assistance or rescue from any single domestic government's services (especially when the impact of a cyberthreat is immediate). At the same time, many states—including the United States—are still

---

Agency). Although it is not bound to assist, the World Health Organization (WHO) can assist states facing a pandemic. If the WHO asks for state parties to help in this effort, they should do so. *See* WHO, *Revision of the International Health Regulations*, Doc. WHA58.3 (May 23, 2009), *reprinted in* WHO, INTERNATIONAL HEALTH REGULATIONS (2d ed. 2005).

290. This duty exists at sea in concert with that imposed by receipt of an SOS. *See, e.g.*, UNCLOS, *supra* note 245, art. 98 (imposing a DTA independent of any SOS if vessel finds persons in danger of being lost at sea; or a vessel collides with another vessel and causes harm).

291. *See* Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4 (Apr. 9) (holding Albania had duty to warn foreign vessels of danger of mines in the Corfu Strait).

292. ICAO, *supra* note 281, art. 25; *see also* Landmines Convention, *supra* note 280, art. 5; Space Objects Treaty, *supra* note 282, arts. 2, 5.

293. Space Objects Treaty, *supra* note 282, arts. 2, 5.

294. *See* John T. Pardun, *Good Samaritan Laws: A Global Perspective*, 20 LOY. L.A. INT'L & COMP. L.J. 591, 592 (1997); Dinah Shelton, *The Duty to Assist Famine Victims*, 70 IOWA L. REV. 1309, 1313 (1985).

295. *See* Steven J. Heyman, *Foundations of the Duty to Rescue*, 47 VAND. L. REV. 673, 676–77 (1994) (noting (i) historical objections to duty to rescue based on common law, (ii) libertarian arguments that people should retain freedom of action as long as they refrain from hurting others, and (iii) formalist arguments that view private law as comprised only of negative rights). Several U.S. states have enacted duty to rescue statutes. *E.g.*, MINN. STAT. ANN. §604A.01 (West 2010); WIS. STAT. ANN. §940.34 (West 2005); *see also* Eugene Volokh, *Duty to Rescue/Report Statutes*, THE VOLOKH CONSPIRACY (Nov. 3, 2009, 12:24 AM), http://volokh.com/2009/11/03/duty-to-rescuereport-statutes/. The common law also has exceptions, requiring rescue where (1) the victim and the rescuer are in a special relationship such as by contract, (2) the rescuer has already begun to help, creating a reliance interest, or (3) the rescuer created the situation putting the victim in peril. *See* RESTATEMENT (SECOND) OF TORTS §§ 321–24 (1965); Heyman, *supra*, at 675, 753. U.S. law enforcement has a separate duty to rescue, but it is owed to the public, not individuals. Castle Rock v. Gonzales, 545 U.S. 748, 761, 765 (2005).

296. *See, e.g.*, Heyman, *supra* note 295, at 689.

wrestling *within* their governments over where responsibility lies for defending against cyberthreats.[297]

In terms of international DTAs, there is one last issue—what assistance must be offered. The duty may be general, as in the case of the Landmine Convention's provision for assistance "where feasible, from other States Parties to the extent possible."[298] The assistance can also be quite specific, such as recovering and returning space objects.[299] Under the Nuclear Accidents Convention, states asking for assistance have to be as precise as possible in specifying needed assistance.[300] Assisting states, moreover, must give advanced notice of what help they can provide, and, when called on to help, must promptly notify requesting states of whether and what help they can give.[301] Collective security agreements, like those under NATO, provide the most dramatic assistance requirements, where parties agree to assist any other state in the event of an armed attack.[302]

D. Why Should States Agree to an e-SOS?

That DTAs are common does not mean cyberspace must have one. Nations need sufficient reasons to cooperate to reach agreement on any new international norm. In cyberspace, multiple motivations favor states devising an e-SOS. This Article suggests the best reason for an e-SOS is functional necessity.

The Internet has become an indispensable vehicle for human communication, commerce, and control that all states value. Cyberthreats challenge this shared interest and require a joint regulatory response. The DTA could be that response. In fact, under current conditions, it may be the *only* available response, where other regulatory methods are either insufficient or unavailable.

The nature of cyberspace, moreover, creates conditions of reciprocity that may further drive states towards a DTA. In cyberspace, everyone is at risk, and everyone can help. All users may suffer harms from cyberthreats, and all users may—under the right circumstances and conditions—be able to assist

297. The U.S. Departments of Defense and Homeland Security are still sorting out who defends government computer resources, and who should help when private systems or networks face cyberthreats. *See* WHITE HOUSE, CYBERSPACE POLICY REVIEW 1 (2010), *available at* http://www.whitehouse.gov/assets/documents/ Cyberspace_Policy_Review_final.pdf. Most recently, the two sides have devised an accommodation on the division of labor. *See* Thom Shanker, *Pentagon Will Help Homeland Security Department Fight Domestic Cyberattacks*, N.Y. TIMES, Oct. 20, 2010, at A22.

298. Landmines Convention, *supra* note 280, art. 6.

299. Space Objects Treaty, *supra* note 282, art. 5; *see also* ICAO, *supra* note 281, art. 25.

300. Convention on Early Notification of a Nuclear Accident art. 2, Nov. 18, 1986, 1439 U.N.T.S. 275, 25 I.L.M. 1370.

301. *See* Nuclear Assistance Convention, *supra* note 280, art. 2. A similar pre-commitment to specify possible future assistance exists under the Chemical Weapons Convention. *See* CWC, *supra* note 280, art. X(7).

302. North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243 ("Parties agree that an armed attack against one . . . shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them . . . will assist the Party or Parties so attacked.").

to combat such threats. An individual user could help a major state end a DDoS attack against military networks by disconnecting from a botnet. ISPs could route traffic to stop it, while governments have substantial resources to counter-attack the threat as well. States might thus agree on assistance as matter of reciprocity; everyone assists to obtain similar assistance if the tables turn.

Beyond functional necessity and reciprocity, moral considerations could motivate a DTA. Norms like human rights and the laws of war exist in part to identify acts or situations that states consider unacceptable. Not all cyberthreats will be universally reviled; hackers celebrate some hacks for their brilliance, while states value data gleaned from cyberespionage. But states might be motivated to impose a DTA for cyberthreats that cause unnecessary human suffering. In other cases, a victim's identity alone might warrant a DTA, such as cyberthreats on hospitals.[303] The laws of war offer additional examples, prohibiting attacks on drinking facilities, dams, dykes, and nuclear plants "if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population."[304] States could thus use a DTA to identify unwanted cyberthreats because they view their results as worthy of universal condemnation.

E. What Would an e-SOS Look Like?

Existing DTAs clearly suggest states could build a comparable e-SOS system. And they have good motivations to do so. As with earlier DTAs, this one will require elaboration of (1) what cyberthreats to cover; (2) which victims can invoke the duty; (3) how they should do so; (4) who the duty-bearers are; and (5) what type(s) of assistance may be provided.

1. *Which Cyberthreats?*

States could opt for *no* threshold; as discussed, they could create a DTA for *any* cyberthreat against specified targets.[305] For example, any evidence of computer error or malware on a hospital computer network or a SCADA system running a hydroelectric dam could trigger the duty. States could also categorically prohibit DTAs for certain cyberthreats. States might, for example, deny a DTA for cyberthreats targeting computer systems employed to support illegal or unwanted activity such as SCADA systems supporting

303. Cyberthreats to hospitals would include the loss of a hospital's power generating system, or corrupting medical databases so patients receive incorrect medication, transfusions, or dosages. *See* DÖRMANN, *supra* note 136.

304. AP I, *supra* note 136, arts. 12, 54–56. Whether the Stuxnet virus—which targeted very specific nuclear facilities in Iran—violates these provisions is subject to debate, although I would expect its authors (if they were indeed states) to claim that the Iranian facilities did not constitute the type of nuclear electrical energy generation plant covered by AP I, nor was the virus itself likely to release dangerous forces. *See supra* notes 8, 51–52 and accompanying text.

305. *See* AP I, *supra* note 136, arts. 12, 54–56.

biological or nuclear weapons facilities operated in violation of international law.[306]

On the other hand, states might opt for a threshold that looks at the nature of a threat instead of its target. Indeed, with so many cyberthreats in existence, this limiting condition may be necessary whether or not states decide to apply a DTA to designated targets. Cyberthreats can impact data confidentiality, integrity, authenticity, and availability.[307] They do so in ways that vary widely in terms of timing, scale, and indirect effects, whether as a result of computer error, cyberexploitation, or cyberattack. Only some of these threats will generate unwanted harms.

Figuring out where to draw that line is no easy task. Nonetheless, the typology identified in Part I provides some potential guidelines for doing so. For starters, states could differentiate cyberthreats based on their severity. The most obvious candidates for a DTA would be those that are extensive (as opposed to moderate or nominal) in terms of (a) timing, (b) scale, *and* (c) indirect effects. Obviously, time constraints may make it difficult for victims to adequately assess each factor, but intuitive recognition of such circumstances will undoubtedly be possible in the most extreme cases. And, in other cases, *ex ante* agreement on which cyberthreats are severe (and publicity of that agreement's contents) could give victims the necessary frame of reference against which to judge the severity of the actual cyberthreat they face. For example, a DTA could automatically cover an immediate, widespread compromise of SCADA systems running power generators that produce a nation-wide blackout.

Harder questions lie in deciding what to do about cyberthreats that are extensive in only one or two respects. Should logic bombs, which are not severe in terms of timing, generate a DTA if extensive in terms of scale and potential indirect effects? The 2009 discovery of malware on U.S. SCADA systems for the power grid would have crossed that line.[308] What about a small-scale attack on a single target—say a major bank—but which immediately wipes out the bank's financial records? In contrast, a grim cyberthreat in terms of timing and scale may not warrant as much concern if its indirect effects are nominal; the 2003 Slammer worm worked almost immediately and infected all susceptible systems, but lacked any real indirect punch.[309] Extensive indirect effects, in other words, could be considered a required element. On the other hand, it may be difficult to appreciate immediately a cyberthreat's full set of indirect effects. So long as an attack is

306. Such an approach would thus deny states like Iran the capacity to invoke a DTA when their uranium enrichment plants come under a cyberattack such as the Stuxnet virus. *See supra* notes 8, 51–52 and accompanying text. On the other hand, states could opt to afford a DTA to victim states even in such circumstances if the cyberthreat itself would cause severe loss of life or systemic economic losses.

307. *See supra* Part I.

308. *See supra* note 49 and accompanying text.

309. Although it produced a DDoS side-effect, the Slammer worm's indirect effects were no more than moderately extensive. *See supra* note 34 and accompanying text.

immediate and widespread it could warrant attention given the potential for what initially appears harmless to mask (or become) something more devastating.

The difficulty in differentiating unwanted cyberthreats may actually favor adoption of a more general formula. States could simply indicate a DTA for "severe cyberthreats." At sea, for example, states have not defined "distress" with greater precision.[310] Rather, it clearly encompasses certain situations—a ship sinking—but leaves lesser situations of distress to be elaborated in practice.[311] A similar approach could work in cyberspace.

Beyond severity, states must also decide if the DTA should turn on a specific cause for the threat. For example, should it cover computer error alone—with no evidence of a cyberattack or exploitation? I think it should. The objective of a DTA is to avoid or mitigate unwanted harms.[312] Whatever the cause, where harm exists, states should help ward it off. It does not matter if it came from lawful or unlawful activity; the DTA only focuses on assisting victims. Moreover, given the sophistication of some cyberattacks, apparent internal errors may actually have hidden external causes.

The prospect of excluding cyberexploitations from any DTA is equally troubling. By definition, cyberexploitations do not alter or disrupt the integrity or availability of the targeted system(s); rather, they merely allow exfiltration of data back to the exploit's source. Governments highly value their ability to do this. Thus, it is unclear whether states would ever explicitly agree to extend a DTA to cyberexploitations. On the other hand, cyberexploitations *can* be severe in terms of their timing, scale, and indirect effects. And it is almost impossible to know if what starts as data theft is just data theft or a prelude to something worse.[313] Categorically excluding cyberexploitations would risk excluding some cyberattacks as well.

By defining cyberthreats according to their severity, a DTA could avoid these issues. It would not matter if a cyberthreat involved internal error, cyberexploitation, or cyberattack. This is not to suggest cause is irrelevant to the DTA; it may play an important role in what assistance is rendered. But the triggering condition for the duty would not depend on cause so much as the existence of a severe threat. This would also ensure that assistance comes more quickly; finding out the cause(s) of a cyberthreat takes time that might otherwise delay needed assistance.

---

310. *See supra* note 250 and accompanying text.

311. *See* UNCLOS, *supra* note 245, art. 98.

312. *See, e.g.*, *supra* notes 250, 280 and accompanying text.

313. *See* Lin, *supra* note 33, at 78 (describing how a payload may have capabilities for both exploitation and destruction).

2. *Who Can Call for Assistance?*

Assuming a severe cyberthreat, states will need to decide who can invoke the DTA. They certainly could opt to limit that right to states. Most existing international legal DTAs do so.[314] States should, however, consider extending the right to invoke the duty to victims. Certainly, a state could call for help when its own systems or networks faced a severe threat. But if others facing such a threat have to go to their state before getting help, that could slow the rate at which assistance comes.[315] And in cyberspace, timing may be critical given the capacity of cyberthreats to produce immediate or near-immediate impacts.

If victims can trigger the DTA, states still need to define who exactly is a victim. For example, in a DDoS attack, is the victim the user unable to access a business web service, the business under attack, or the ISP routing all the excess data? The possibility that one or all of these groups is a victim creates both a problem and an opportunity for the DTA. It is a problem because the more victims there are, the more requests get made. Limiting requests to sufficiently severe cyberthreats should counterbalance this possibility. But, at some point, like a DDoS attack, there is a chance of too many victims asking for help too many times, overwhelming whatever assistance mechanism states devise.

So many potential victims offer states an opportunity, however, for *ex ante* control of the assistance mechanism. Among the categories of potential victims—states, ISPs, critical infrastructure industries, banking institutions, individual users, etc.—states could authorize some to invoke the DTA, but not others. Depending on how widely or narrowly states classify "victims" for these purposes, different requests for assistance can be anticipated, both in number and in kind. Limiting victims to states and ISPs, for example, would presumably lead to fewer overall requests for help and likely lead to more requests involving cyberspace architecture than those causing distress to corporations and other institutions, let alone individual users. Other variations among victims are possible, and states would need to weigh carefully how the categories of victims selected will help avoid or mitigate the underlying harms the DTA addresses.[316]

An SOS system operates by providing assistance to those who ask for it. International law, however, also imposes several DTAs independent of a victim asking for help.[317] States could, therefore, decide to require assistance automatically once a state becomes aware of a severe cyberthreat whether

314. *See supra* note 285 and accompanying text.

315. There is also the prospect of states filtering cyberthreats for political reasons, or making them up to observe whatever technical capacity is revealed in subsequent assistance. *See* LIBICKI, *supra* note 23, at 104.

316. Indeed, there is also a risk that a DTA limited to specific victims might incentivize or drive cyberattacks towards other, unprotected, victims.

317. *See supra* notes 290–93 and accompanying text.

through its own monitoring or via second-hand reports. Privacy advocates and libertarians might object to any unasked for interference in private systems and networks. If the state assistance extends beyond its borders, moreover, other states may object as well. Russia, for example, has declined to join the Convention on Cybercrime because it would automatically allow foreign law enforcement to conduct data searches inside Russia.[318]

On the other hand, if a DTA was merely a duty to warn, it might face fewer objections. Thus, states might have an obligation to do nothing more than let victims (or potential victims) know once it identifies a severe cyberthreat, whether or not it has received an e-SOS. Just knowing a threat exists could be sufficient assistance for some victims to marshal the necessary resources to avoid or lessen any harm.

3. *How to Call for Help.*

The ability of states to require a DTA at sea was a function of technological innovation. Telegraph and radio devices made the SOS possible, and even then, only after states required all vessels to have such equipment on board did the SOS develop.[319] With its instant communication, the Internet is a much easier environment in which to call for help. Thus, states should have little difficulty adopting a universal distress signal for victims authorized to use it.[320] The only real question may be to whom they transmit it. Should victims have to signal distress to an intermediary before assistance is called in, or might victims be able to signal a need for help directly to those individuals, groups, or states that might provide it?

4. *Who Must Assist?*

A critical issue for any e-SOS will be identifying the class of states, groups, or individuals that must provide help when called. Again, states are the most likely duty-bearers in light of existing practice.[321] But, as the DTA at sea shows, states could spread the duty more widely. Doing so has its risks; the nature of the Internet is that an e-SOS can reach everyone online. Such a broad duty could make sense for catastrophic cyberthreats. More likely, states will not want to impose the assistance burden so widely, particularly given that assisting expends time and resources that might be devoted elsewhere.

On the other hand, rather than reaching too many, the DTA burden might fall on too few in terms of those who have the most to offer by way of assistance. Certain major states, ISPs, and Internet companies have skills and resources that many other Internet users lack. To the extent victims know

318. Markoff & Kramer, *supra* note 230.

319. WEDLAKE, *supra* note 242, at 50.

320. Given the potential for a would-be attacker to also try to jam the e-SOS signal, the system would probably need to operate independent of any victim's own network or systems.

321. *See supra* notes 286–89 and accompanying text.

this, there is a risk the more capable actors will bear the brunt of assistance requests. States could avoid this, however, by devising a system to sort out who has to respond to an e-SOS in particular cases.

How could they do this? Despite the rhetoric of a borderless Internet, states might find it easiest to tie the DTA to the territorial jurisdiction(s) within which the threat lies. For example, the duty to recover and return space objects applies to the state where the object is found.[322] By way of analogy, the physical location(s) associated with a cyberthreat might determine who bears the DTA. That duty could then either lie with the state(s) concerned, or, as with the SOS, more widely to include private actors present in that state with a capacity to help.

Geographic or jurisdictional links between the victim and the duty-holder are not the only—nor necessarily the best—ways to identify duty-bearers online. Technological proximity might be a more fair and efficient standard. Under this view, the cause of the threat would determine who has to help fix it; if a DDoS attack arrives on a server via one or more ISPs, those ISPs would have a DTA. If a cyberattack traces back to a state's territory, that state would have a DTA, *whether or not* the attack originated there.[323] A state could, for example, block traffic from proceeding onto a victim whenever that traffic was being routed through its servers.[324] In other words, the DTA would seek to burden not those with a general capacity to combat cyberthreats, *but those best situated to deal with the precise cyberthreat at issue.*

Tiering could be a third way for states to distribute the DTA. By tiering, I mean a graduated DTA, with primary duty-bearers, secondary duty-bearers, etc. In case of a severe cyberthreat, the primary duty-bearer could be identified on jurisdictional, technological, or other grounds. But if that duty-bearer determined it could not handle the situation, it would itself have a right to ask for further assistance from some additional group of duty-bearers, who could if necessary extend the assistance chain even further down the line. Such a graduated assistance mechanism would have the advantage of allowing all severe cyberthreats to be addressed, while providing opportunities to allocate the costs of that assistance more efficiently by not burdening every potential duty-bearer in every case.

The motivations states have to create a DTA may also implicate where they place the burden. If reciprocity is essential, duty-bearers should align with the victims who can invoke the duty.[325] In other words, if only states and ISPs can ask for help, only states and ISPs would provide it. But if states focus more on the moral and functional motivations for a DTA, asymmetric

322. Space Objects Treaty, *supra* note 282, art. 5.

323. Where the cyberthreat is apparent computer error, technological proximity may be more difficult and states might opt for jurisdictional links instead.

324. There is a risk, of course, of cyberattacks that appear to target a victim, but which are actually targeting the state under a DTA; for example, routing multiple attacks through a state under a DTA to observe, burden, or even overwhelm its capacity to respond.

325. *See supra* note 303 and accompanying text.

relationships would become possible. All victims would not need to be duty-bearers, or vice versa. For example, even if individual users could not invoke a DTA, states might want to require assistance from them. In the event of a severe DDoS attack, the victimized business or ISP might want individual users to have a duty, once asked, to take steps to disconnect their system from the botnet perpetuating the attack.[326]

5. *What Assistance Gets Rendered?*

States can mandate assistance on various grounds, such as effort, results, technology, purpose, or the victim's selections. In terms of effort, duty-bearers could be bound to do what they reasonably can to help victims. This reasonable effort might mean a considerable amount of help, whether deploying code or re-writing it, loaning bandwidth, working to shut-down a botnet, or tracing-back an attack if possible. Or, it might not. Intelligence agencies, for example, could argue that they can only warn of problems given legal limitations on their ability to help.[327] Or, they might insist that any assistance given be treated as confidential to avoid revealing sources and methods. In some cases, no effort may be required if assisting would be unreasonable; for example, putting additional lives in danger or exacerbating the damage.

In lieu of efforts, a DTA could require assistance that gets results. For example, ISPs might be required to shut down computers involved in a botnet. Or, a state might be required to deny attackers use of its networks. Defining assistance in terms of results may do more to avoid or minimize severe cyberthreats, although the costs on those assisting are likely to be higher.

Separate from duties of effort or result, assistance might be defined in technological terms. Technology, of course, will likely be deployed in assisting against any cyberthreat. But, a DTA might actually specify assistance in the form of code. Software companies could thus be required to develop patches to their code where vulnerabilities exist, whether or not they still supported that software.[328] Or, a DTA might require specific technological assistance, such as trace-backs or storage of logs associated with cyberthreats.

Assistance may also be defined by its purpose. Here too, care is warranted in the selection. The Convention on Cybercrime, for example, has a DTA, on

326. For similar practices concerning infringing copyright content, see 17 U.S.C. § 512(c) (2010); Greg Sandoval, *AT&T First to Test RIAA Antipiracy Plan*, CNET NEWS (Mar. 24, 2009, 9:53 PM), http://news.cnet.com/8301-1023_3-10203799-93.html.

327. Alternatively, the risks of liability that might disincentivize assistance can be dealt with in creating the DTA. Various U.S. states have "Good Samaritan" laws to protect those who help from liability that might otherwise have arisen from their acts of assistance. *See, e.g.*, 42 PA. STAT. ANN. § 8331 (West 2010).

328. With Stuxnet malware impacting SCADA systems, for example, Microsoft provided patches for software it supported, but not older versions such as Windows XP SP2 and Windows 2000, leaving them vulnerable. Mills, *supra* note 51.

request, "for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data."[329] Thus, assistance is limited to fulfilling a specific purpose—combating cybercrime. Richard Clarke and Robert Knake have proposed their own "obligation to assist" as part of a "Cyber War Limitation Treaty," that would require states "to hunt down, shut off, and bring to justice those who use their cyberspace to disrupt or damage systems elsewhere."[330] The purpose of that obligation would only "be concerned with cyber war."[331]

Given the difficulties this Article has identified in differentiating conditions of cybercrime from cyberwar, limiting assistance to one or the other contexts is problematic. It creates opportunities for duty-bearers to deny help. A state could deny legal assistance relating to cybercrime, by insisting the issue was one of cyberwar; or a state might reject an obligation to assist against a cyberattack on the premise that the attack was just a cybercrime. The purpose of assistance would be better if defined to align with the purpose of the DTA itself, namely to avoid or mitigate severe cyberthreats.

Finally, an e-SOS model could follow its namesake; marshaling available assistance first, and then letting the victim select which assistance to accept. Victims would not have to be helpless when it came to those who helped them; they could weigh the costs and benefits of different types of assistance, who was offering it, and in what form. A victim might be able to choose whether to accept help from its ISP or a competitor. A victim might accept an NSA offer of assistance, subject to confidentiality, or accept help from a more public source.

Thus, states have substantial flexibility in devising an e-SOS. That flexibility reinforces the case for a DTA. An e-SOS does not need to duplicate pre-existing commitments at sea or in other contexts. Rather, states could focus on the threats as they exist in cyberspace, and identify who is best suited to deal with them and in what ways they should do so.

F. How to Develop a DTA for Cyberspace

Many proponents of cyberthreat regulation have advocated for a comprehensive, multilateral treaty to delineate rules of the road in cyberspace.[332] Such a treaty process is the ideal forum within which to devise an international e-SOS. It would afford states a vehicle for working out answers to the various questions about who would benefit from—and be burdened by—a DTA.

Even if states are not yet ready, however, to conclude a global agreement on an e-SOS, that does not mean they must dispense with the idea entirely.

---

329. Convention on Cybercrime, *supra* note 18, art. 25(1).

330. CLARKE & KNAKE, *supra* note 1, at 178, 268–69.

331. *Id.* at 271.

332. *See, e.g.*, Sharon R. Stevens, *Internet War Crimes Tribunals and Security in an Interconnected World*, 18 TRANSNAT'L L. & CONTEMP. PROB. 657, 711 (2009); Brown, *supra* note 19, at 215–21.

States could generate the same norm in other ways. Sometimes, unilateral state action—through domestic law or regulation—can trigger the formation of an international rule. The U.S. Leiber Code, for example, played this role in the laws of war.[333] Or, a group of interested states might decide to articulate a DTA regionally first, as the Council of Europe already did for cybercrime.[334] To the extent states view severe cyberthreats in security terms, a DTA might even find its origins in a collective security arrangement, such as NATO.[335]

Assuming states are ready to adopt a legally binding DTA, they will need to decide how precisely to do so. Like all law, international law contains principles, standards, and rules. Principles set forth considerations for evaluating conduct rather than providing a norm for conduct itself.[336] Standards impose norms on future conduct, but do so in ways that require *ex post* analysis of compliance. Rules, in contrast, provide *ex ante* norms for future conduct.[337] The discussion so far has assumed that states would seek a rule or standard for an e-SOS. If they are unwilling, or unable to do so, however, a more general principle could still have value. In international environmental law, for example, several duties—such as the duty to warn of adverse transboundary environmental impacts—exist as principles.[338]

If states are unwilling or unable to reach a legal agreement on an e-SOS, they could instead formulate it as a political commitment. Political commitments are a well-established practice where states sign agreements they intend to follow, but for which compliance is dictated in moral or political, rather than legal, terms.[339] Unlike a treaty, which only states and international organizations can join, political commitments can also include additional actors.[340] Thus, a political commitment for an e-SOS could include stakeholders like ICANN and major ISPs.

A related "process" question for any DTA involves the extent of institutionalization to impose alongside any substantive duty, whether drafted in

333. *See* LIEBER'S CODE AND THE LAW OF WAR, *supra* note 112, at 1–2. Thus, although this Article focuses on an international DTA, I would not object to a domestic e-SOS. A national approach could be tailored to public policies (like U.S. commitments to privacy) and allow experimentation in terms of how DTAs might work. On the other hand, if different nations diverge too greatly in approaches, opportunities for international consensus are lost.

334. *See* Convention on Cybercrime, *supra* note 18.

335. NATO, in fact, has already acknowledged that a cyberattack could qualify as an armed attack, requiring assistance from other state parties. *See* GROUP OF EXPERTS, NATO 2020: ASSURED SECURITY; DYNAMIC ENGAGEMENT 9 (2010).

336. *See* RONALD DWORKIN, TAKING RIGHTS SERIOUSLY 22–28 (1977).

337. *See, e.g.*, Daniel Bodansky, *Rules vs. Standards in International Environmental Law*, 98 AM. PROC. SOC'Y INT'L L. 275, 276 (2004); Louis Kaplow, *Rules Versus Standards: An Economic Analysis*, 42 DUKE L.J. 557, 562 (1992).

338. *See* United Nations Conference on Environment and Development, Rio de Janeiro, Braz., June 3–14, 1992, *Rio Declaration on Environment and Development*, princ. 19, para. 1, U.N. Doc. A/Conf.151/26 (Vol. I) (Aug. 12, 1992).

339. Duncan B. Hollis & Joshua Newcomer, *"Political" Commitments and the Constitution*, 49 VA. J. INT'L L. 507, 516–17 (2009).

340. *Id.* at 521 (political commitments need not be limited to states or international organizations).

legal or political terms. States could establish institutional mechanisms (or even an international organization) to monitor and oversee any assistance mechanism. Alternatively, states may turn to existing institutions to perform this role.[341] In lieu of an international organization, states could designate national outlets—such as the existing Computer Emergency Response Teams—to facilitate assistance against cyberthreats.

What about compliance? States could—as Russia has suggested[342]—adopt compliance procedures. These procedures would allow other states, or any international institution so designated, to review calls for—and provisions of—assistance in light of the content of any DTA adopted. There are precedents for this in international law, although they are more exceptions than the rule.[343] More likely, states would take charge of enforcing compliance by their own nationals. As between themselves, an e-SOS—like much of international law—would appear to generate compliance largely through its status *as* international law, rather than via sticks or carrots. States could be legally responsible in the event of breach, triggering reputational sanctions or any other responses allowed by international law.[344]

IV. The Benefits (and Costs) of an e-SOS

Adopting an e-SOS would impose new costs. There would be transaction costs in having a call-and-response system. Those bound would have an affirmative duty to act (whether in terms of effort, results, etc.), and acting will of course cost in terms of time, resources, and money. ISPs, for example, can cut off a DDoS attack but usually insist on getting paid to do so.[345] Similarly, individual users may resent the costs of recovering their systems from a botnet they neither knew nor cared about previously. Militaries may see costs in revealing their cybercapacities, even if necessary to help a victim.

Now, these specific "costs" might actually involve net "benefits" if they negate or lessen the impacts of a severe cyberthreat. Indeed, these costs are likely to generate the *primary* benefits of having an e-SOS system. It would

341. *See, e.g.*, Int'l Multilateral Partnership against Cyber Threats ("IMPACT"), http://www.impact-alliance.org/ (last visited March 6, 2011) (established by the International Telecommunications Union, IMPACT has thirty-seven participating states).

342. *See* Karl Frederick Rauscher & Andrey Korotkov, Working Towards Rules for Governing Cyber Conflict 32–33 (2011).

343. *See, e.g.*, CWC, *supra* note 280, Annex on Implementation and Verification.

344. *See, e.g.*, Draft Articles on Responsibility of States, *supra* note 139, at 31; Brewster, *supra* note 147, at 234–36 and accompanying text.

345. CSIS Report, *supra* note 16, at 5 ("In today's network environment, DDOS attacks are technically easier to detect and tamp down, and most Internet Service Providers (ISPs) offer such mitigation to their clients—for a price. 'Generally ISPs very much have the mentality that we just haul traffic[,]' said Adam Rice, chief security officer of Tata Communications, the world's largest wholesaler of internet service. 'If you pay for the [mitigation] service, we'll kill [a DDOS attack] before it gets to you, but otherwise providers tend to watch it go by.'").

seek to generate assistance from specified individuals, groups, or states, rather than just those with the time, resources, *and* inclination to help.[346]

Whether the costs of this e-SOS are too high depends on how one views the status quo. After all, many known cyberthreats already result in substantial informal assistance among states, individuals and companies. For example, a hotline phone system, the Inter-Network Operations Center Dial-By-ASN (INOC-DBA), already connects "Network Operations Centers and Security Incident Response Teams of Internet infrastructure providers, operators of Internet exchanges, critical individuals within the Internet security, policy, emergency-response, and governance community, and equipment vendors' support personnel."[347] Assistance may also come through communities constructed by personal relationships or trusted introductions. In other cases, informal assistance develops as an *ad hoc* response to a particular cyberthreat. In 2008, for example, malware known as the "Conficker worm" exploited a vulnerability in a Microsoft program, and by January 2009 had infected five to fifteen million computers. A "Conficker Working Group" was formed in February 2009 among industry leaders, academia, ICANN, and others who have since reduced the number of infected systems to around 300,000.[348] Some might view a DTA as unnecessary given such existing informal assistance. Worse, an e-SOS might de-motivate some of those who currently assist from doing so in the future.[349]

But current informal assistance networks are both inadequate and inefficient. Most cyberthreats—80% by some estimates—go unreported given the existing self-reliant ethos.[350] Nor is it evident that undisclosed threats are somehow less severe than those that do become public. Second, even where assistance occurs, nothing dictates which cyberattacks should generate assistance, let alone who should provide it.

An international legal DTA would respond to both deficiencies. Many cyberthreat victims now stay silent because there is no guarantee disclosure will improve their situation, but there is some certainty of negative reputational effects. A DTA would change the landscape by giving victims a clear benefit for coming forward to weigh against any negative message from admitting an incapacity. By motivating at least some victims to come forward who do not already do so, a DTA may prompt a cascading response where

346. The law of salvage suggests that these costs need not lie exclusively with duty-holders. It might be possible for states to provide those who give assistance with some remuneration for their expenses. This could be done through any number of domestic or international financial mechanisms, including something as simple as a "victim pays" formula. *See supra* note 276 and accompanying text.

347. *INCO-DBA Hotline Phone Q&A*, PACKET CLEARING HOUSE, https://www.pch.net/inoc-dba/docs/qanda.html (last visited Mar. 6, 2011).

348. *See* THE RENDON GRP., CONFICKER WORKING GROUP: LESSONS LEARNED 3, 10–11, 19 (2011).

349. *Cf.* Eugene Volokh, *Duties to Rescue and the Anticooperative Effects of Law*, 88 GEO. L.J. 105, 108–09 (1999).

350. *See* CERT, *supra* note 212.

other victims are prompted to come forward by the simple fact that it has become more acceptable to do so.

A DTA could also improve the quantity and quality of assistance that victims currently receive. When Estonia asked Russia to cut off DDoS attacks it said originated from Russian territory, Russia insisted it was not responsible and did nothing. If it had a DTA, Russia would have much more difficulty doing nothing, and instead would have had to do something (perhaps cutting off the DDoS traffic).

An e-SOS system could also deter would-be attackers. Once a DTA is established, states will need to consider the costs and benefits of complying with that duty as part of any decision to launch their own cyberattacks or exploits. If states determine that they will be duty bound to provide assistance in response to their own attack, they might not attack at all. They could decide to avoid any risk of being associated with an attack, or—even if they are confident in anonymity—the benefits obtained may be outweighed by the combined cost of launching the attack *and* then helping to remediate it.

Hacktivists, hackers, and cybercriminals face the same set of benefit-cost tradeoffs. A DTA could generate assistance sufficient to cease any significant impact of a severe DDoS attack, whether through provision of additional bandwidth, cessation of hostile traffic, or destruction of the offending botnet. If cybercriminal organizations using these attacks to extort funds know their attacks will not cause enough harm, they are unlikely to make the effort.

In other words, the DTA could perform the very deterrent function now lacking in rules on cybercrime and cyberwar. Of course, not all attackers would necessarily be deterred; given the low costs of attacking, some may continue to take as many bites at the apple as they can. Others—particularly hackers seeking to establish their technical prowess—might view an e-SOS as simply a further challenge to be overcome.

But even if deterrence is imperfect, an e-SOS would render networks more resilient in the face of such threats. In computer science, resilience is the capacity of systems or networks to provide or maintain acceptable levels of service when facing errors and challenges to normal operations.[351] Thus, a DTA could fall short of eliminating a cyberthreat but still provide benefits by lessening its harm to a tolerable level for the victim system or network. For example, if a SCADA system for a power grid goes down, a DTA could help bring it back on-line faster (at less cost to customers), than if the owners of the injured infrastructure had to go at it alone.

There are other candidates for improving existing deterrence and resilience involving cyberthreats. As discussed, states could try to rewire cyber-

351. *E.g.*, Kang-Won Lee et al., *Improving the Resilience of Content Distribution Networks to Large Scale Distributed Denial of Service Attacks*, 51 COMPUTER NETWORKS 2753, 2757 (2007).

space architecture to fix the attribution problem, ban cyberweapons, impose minimum security requirements, or authorize government monitoring of private systems. None of these are inexpensive options. Indeed, the DTA is likely to cost less because it only imposes new costs in cases of severe cyberthreats, rather than imposing sunk costs for changing the entire system one way or another.[352] In any case, each of these alternatives has already garnered substantial opposition from one or more interest groups.

The DTA, in contrast, can be deployed in multiple ways depending on which threats states decide to address, and the methods of private and public assistance they deploy. In contrast to other responses to cyberthreats, an e-SOS also has a substantial ring of freedom. It works without rewiring the Internet to deprive it of existing protections for privacy and freedom of speech. No regular government monitoring of a computer system or network is required. On the contrary, victims can decide whether and when they need help. Under my preferred version, moreover, they may even be able to select for themselves which help to requisition and which to let pass.[353]

All of these benefits, moreover, operate in conjunction with existing law. A DTA complements—rather than conflicts with—existing approaches to cyberthreats. It supplements self-reliance when the victim becomes incapacitated. Nor does it seek to supplant existing proscriptions on cybercrime and cyberwar. Assistance will not preclude attribution efforts, and if those efforts do bear fruit, criminals can be prosecuted or states held accountable for their actions. States may even opt to craft a DTA to include assistance *in* attribution. If this assistance works, it may eventually improve the ability of proscriptions to work (and deter) as intended.

V. Conclusion

On October 29, 2007, pirates attacked a North Korean cargo ship, the *Dan Hong Dan*, laden with sugar off the coast of Somalia. The captain sent out a distress call as the pirates took control of the bridge. A U.S. warship—the *James E. Williams*—responded, sending a helicopter to the scene and ordering the pirates to surrender. Fighting ensued with the North Korean crew killing two pirates, and capturing five others. On its arrival, the *Wil-*

352. It is true that alternating the technology might appear to impose only a one-time cost, while setting up and maintaining a DTA system would involve repeated expenditures over time. But I am not certain that even shifting the technology to a system with better (let alone perfect) attribution can be done in one shot; more likely, the endless cat-and-mouse game between those seeking anonymity and those seeking attribution would continue with new methods of making cyberthreats anonymous requiring further technological updates or changes.

353. On the other hand, even as its freedom favors the Internet and victims, it would require duty-bearers, whether foreign states or private parties, to serve social ends.

liams provided medical treatment to three North Korean crewmembers injured in the fighting. The vessel itself escaped unharmed.[354]

The United States has no diplomatic relations with North Korea, has thousands of troops stationed along its border, and is doing everything short of force to forestall its nuclear ambitions.[355] And yet, the *Williams* helped repel the pirates and save the North Korean vessel and its crew from further harm.[356] The U.S. Navy respected its adversary's SOS and the legal duty to assist it imposed. At sea, the SOS is a powerful norm that avoids and remediates harm in an often inhospitable environment.

As cyberspace becomes increasingly inhospitable, states should consider the utility of a similar e-SOS. Cyberthreats are a massive problem and they are getting worse. Property—intellectual and real—may be lost, infrastructure endangered, and lives put at risk.

To date, policymakers and scholars have erred in relying on proscriptive models to accomplish cybersecurity. Because technology allows those who wish to remain anonymous to do so, to pass themselves off as someone else, or even to disguise any evidence of their responsibility at all, the existing rules have little deterrent force. Cybercriminals are not deterred, assuming they will never get caught if they are good at what they do, and only rarely get caught when they are not. States are similarly enjoying the newfound potential of cyberespionage and other cyberoperations, safe in the knowledge of plausible deniability.

An e-SOS offers an alternative path. Even if we cannot regulate those who cause threats or the vehicles by which they are delivered, we can address victims' harm. An e-SOS does this by giving victims a new way to avoid or mitigate severe cyberthreats, whatever their cause. International law contains ample precedents for a DTA, and the conditions generating the SOS itself have much in common with the existing cyberthreat environment.

Moreover, states clearly can create an e-SOS if they so desire. They can adjust it to particular threats, victims, and vehicles for assistance. They could do it by global agreement, or other methods. Doing so may lessen the real damage done by existing cyberthreats and deter others, all without displacing traditional methods of cybersecurity.

At sea, every ship and its crew make their own way. But when all else fails, the SOS is there to bring them comfort. Cyberspace has always favored

---

354. *See, e.g.*, *US Ship Helps North Korea Vessel Crew Overpower Somali Pirates*, AGENCE FRANCE PRESSE, Oct. 30, 2007, http://afp.google.com/article/ALeqM5hQLMlkR4kES5yt9Zfyy7YA8V1B8Q; *Crew Wins Deadly Pirate Battle off Somalia*, CNN.COM, Oct. 30, 2007, http://edition.cnn.com/2007/WORLD/africa/10/30/somalia.pirates/index.html.

355. *See generally* COUNCIL ON FOREIGN RELATIONS, INDEPENDENT TASK FORCE REPORT NO. 64: U.S. POLICY TOWARDS NORTH KOREA (2010) (exploring the various policy courses available to the U.S. government regarding North Korea).

356. Nor was this an isolated incident. *See* IMB REPORT, *supra* note 262, at 35 (detailing how on September 5, 2009, the U.S. Navy assisted a North Korean vessel attacked by pirates).

self-reliance, but the current dangers may be too much for individuals, groups, and states to handle alone. It is now time for them to accept a helping hand: an e-SOS.