2017

# Justice in the Era of Silent Crimes: Addressing the Need to Update International and Domestic Law to Respond to the Threat of Cyber Warfare and Cyber Crimes

Patrick Macaluso
*Duquesne University School of Law, Class of 2017*

# Justice in the Era of Silent Crimes: Addressing the Need to Update International and Domestic Law to Respond to the Threat of Cyber Warfare and Cyber Crimes

Patrick R. Macaluso*

Duquesne Univ. School of Law

*submitted in completion of the writing requirement for a concentration in International and Comparative Law*

## *Introduction*

At the 2016 Eurovision Song Contest held in Stockholm, singer Dami Im, representing Australia, belted her way through a powerful performance of the song 'Sound of Silence,' a pop ballad about the complexities of expressing love in the digital age, when one gazes into a computer screen instead of someone else's eyes. Im's performance earned Australia a second-place finish at the contest in their second year participating.[1] While Im's finish is more commonly seen as representative of Australia's rapid rise in relevance in the Eurovision Song Contest, perhaps more telling is the content of the lyrics of 'Sound of Silence.' In the digital age, millennials use online applications to find dates and partners.[2] Online shopping is increasingly popular, eliminating the

---

* The author wishes to thank the following individuals for helping me with this project: Prof. Barbara Carlin, for her dedication, patience, and support during the research and writing process; Prof. Steven Baicker-McKee for helping facilitate the administrative end; and my colleagues from the Fall 2016 International Criminal Law course—Katie Burns, Jen Vogel, Anthony Hassey, Caleb Pennington, and Kyle Lanning—for helping start the research process.

1. ABC News Australia, "Eurovision 2016: Dami Im claims second place with Sound of Silence," ABC NEWS AUSTRALIA ONLINE (May 15, 2016, 1:34 a.m.), http://www.abc.net.au/news/2016-05-15/dami-in-wows-eurovision-crowd-with-sound-of-silence/7415328.

2. *See, e.g.*, Dakota Kim, "The New Generation of Millennial Matchmakers Wants to Help Your Tinder Game." VICE ONLINE (June 21, 2016, 12:00 a.m.), https://www.vice.com/en_us/article/the-new-generation-of-millennial-matchmakers-want-to-help-your-tinder-game.

need to interact face-to-face with merchants.[3] And perhaps the element of the digital age that resounds mostly to the "Sound of Silence" is crime. The woman sitting silently at the cyber café may be a victim of cyber bullying, identity theft, or she may even be working for a foreign government, gathering digital information to use against the United States.[4]

Cyber threats exist at both the individual and systemic level, involving both state and non-state actors. Both domestic and international legal systems inadequately address the many threats posed by cyber terrorism, cyber warfare, and cybercrimes in general.[5] Individual governments and the international system collectively are unsure how to address the growing threat of cybercrimes to both state and non-state actors. There is little useful guidance within existing legal frameworks that addresses cyber threats. In the coming years, this must change. While the world is fixated on the possible involvement of Russian hackers and cyber operatives in the 2016 United States election, it is at least foreseeable that a cyber-attack on critical infrastructure, such as a water treatment facility, could have disastrous results on a significant number of people.

---

3. *See, e.g.*, Mary Wolfinbarger, Mary C. Gilly, "Shopping Online for Freedom, Control, and Fun," 43 CALIF. MGMT. REV. 34 (2001).

4. *See* DAVID S. WALL, CYBERCRIME: THE TRANSFORMATION OF CRIME IN THE INFORMATION AGE, 1-3 (Polity Press, 2007).

5. *See, e.g.*, Jeffrey T.G. Kelsey, "Hacking Into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare," 106 MICH. L. REV. 1427 (2008).

This paper details the inadequacy of existing legal frameworks to address cyber threats and proposes solutions to start the process. In the first section, I provide a history of cyber warfare and detail several important cases. In the second section, I discuss the current legal framework in the United States as it relates to cyber threats and suggest ways to improve that framework. Likewise, in the third section of this paper, I analyze the international legal framework and suggest ways to improve it. While cyber-attacks have been occurring for many years, the steps suggested in this paper will only be the beginning of what could be a global initiative to address the silent threats in cyberspace. They are necessary steps, but the long-term effects of these steps may not be singularly adequate to comprehensively address cyber threats.

## *I An Overview of Cyber Warfare and Specific Cases*

### A Definitions and Concepts

There are several terms that seem interchangeable at first glance, but it is important to distinguish several terms that will be used in this paper to understand both the broad and narrow concepts.

The term 'cyber' refers to computers broadly, and in this paper it is used to qualify words such as 'threat,' 'attack,' 'warfare,' and 'terrorism.' When used in this context, it is understood to mean pertaining to computers or machines, controlled by humans. It can also be understood as the

opposite of the word 'conventional' within this context. Whereas conventional warfare, for example, refers to the use of physical weapons by one party against the use of physical weapons by another, cyber warfare refers to the use of computer-related tools by one group against another group in a harmful manner.

Distinguishing between states and non-state parties is more difficult than it seems. When a government acts on behalf of its population by means of its political sovereignty, then it is acting as a state within the international system.[6] But there are some circumstances when a group or individual may appear to be a non-state actor, but is functionally a state actor. For example, a victim of a cyber-attack may be considered a state actor, even though the government is not directly involved, if the attack is against a state's critical infrastructure.[7] Critical infrastructure are the physical and institutional systems that keep a society running, such as water treatments systems, electricity grids, emergency response systems, and communications systems.[8] This is particularly relevant in the United States, where the vast majority of its critical infrastructure is privately-

6. *See generally* John Gaventa, *Power and Powerlessness: Quiescence and Rebellion in an Appalachian Valley* 3-32 (1982).

7. *See* Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," 38 INTERNATIONAL SECURITY 41 (2013).

8. Stephen Flynn, *The Edge of Disaster* (2007).

owned.[9] There may also be some degree of uncertainty of whether an actor is state or non-state. For example, the governing apparatus of the majority political party in a certain state may look like both a state actor and a non-state actor. The distinctions may be blurry, but in all of the cases explored in this paper, they are somewhat clearer.

**B State versus State Cyber Warfare**

Traditionally, warfare involves one state – an organized, sovereign political entity – engaged in combat with another state. While the dynamics of war have changed substantially over the years, perhaps the most compelling type of cyber warfare mirrors the most common type of conventional warfare. As cyber warfare becomes more common, states are more comfortable employing cyber-attacks in the pursuit of national interests. These first two cases—The Stuxnet Affair and the Russian Attack on Estonia—not only demonstrate how commonplace state versus state cyber warfare has become, but also how the use of cyber tactics by one state against another is a legitimate means to an end.

---

9. *Id.* Flynn argues that three factors impact American society's capability to respond to disasters (such as a cyber-attack) moving forward: 1) aging critical infrastructure; 2) the reality that the emerging generation of leadership—Gen X—does not seem to care; 3) Poor collaboration between the private and public sectors, especially in sectors of critical infrastructure. *See id. See also* Dennis Mileti, *Disasters by Design: A Reassessment of Natural Hazards in the United States* 17-40 (1999).

1 The Stuxnet Affair

Stuxnet is a computer virus allegedly developed by the United States and Israel. Its primary target was the nuclear facilities in Iran, and the affair was seen internationally as an attempt to halt the Iranian nuclear program.[10] Stuxnet was a failed operation insomuch that it failed to sabotage Iran's nuclear development, but its implementation has serious foreign policy implications. The implications of a major superpower and, arguably, its client employing a cyber-attack against another state are momentous, and may indeed result in the normalization of the use of such tactics on a global scale. We can expect more cyber-attacks, and because of this new reality, the international system must address the parameters, implications, and possibilities of the new world. Stuxnet is only the beginning.

The Stuxnet worm spreads through computers running on Windows very easily and without detection.[11] Users can maintain regular use of their machines without knowing that there is illicit software operating while they use their machines normally.[12] The main goal of the virus is to gain control of industrial facilities—which is not limited to nuclear facilities—without users

10. *See generally* James P. Farwell, "Stuxnet and the Future of Cyber War," 53 SURVIVAL 23 (2011).
11. *See* "W32.Stuxnet," Symantec, last modified September 17, 2010, http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.
12. *Id.*

realizing it.[13] If the virus is successfully loaded onto one machine, it will spread indiscriminately throughout a network.[14] Estimates show that most computers infected with the virus are in Iran (58.85%).[15] Symantec, a cyber security company, describes the premise of the virus as follows:

> Stuxnet searches for industrial control systems, often generically (but incorrectly) known as SCADA systems, and if it finds these systems on the compromised computer, it attempts to steal code and design projects. It may also take advantage of the programming software interface to also upload its own code to the Programmable Logic Controllers (PLC), which are 'mini-computers', in an industrial control system that is typically monitored by SCADA systems. Stuxnet then hides this code, so when a programmer using a compromised computer tries to view all of the code on a PLC, they [*sic*] will not see the code injected by Stuxnet.[16]

In the case of the attack on Iranian nuclear facilities, the virus was used to collect information and sabotage progress. The initial execution of the attack began in the latter years of the Bush administration under the premise that a nuclear-armed Iran was the next biggest threat to American lives. If diplomacy and sanctions should fail, and should the United States fail to build

---

13. *Id.*
14. *Id.*
15. The other affected areas were found to be Indonesia (18.22%), India (8.31%), Azerbaijan (2.57%), United States (1.56%), Pakistan (1.28%) and Others (9.20%). *Id.*
16. *Id.*

an international coalition of opposition to the Iranian nuclear programs, then a pro-active solution to the threat would be necessary to develop.[17]

It is unclear precisely when Iran discovered that they were attacked. In early 2010, one thousand IR-1 centrifuges in the Fuel Enrichment Plant (FEP) at Nantanz were replaced, implying that they were either broken or tampered with.[18] Most observers assumed that they had performed poorly or had malfunctioned.[19] Only later in 2010 did President Mahmoud Ahmadinejad admit that the plants been subjected to cyber-attacks.[20] By no means did Stuxnet destroy the centrifuges. Instead, it damaged them and set the nuclear development program several years back.[21] Furthermore, it gave both the United States and Israel, presumably, valuable information of Iran's nuclear operations.

The Stuxnet virus is not limited to state-on-state operations. Indeed, the virus is designed to infiltrate any industrial control system.[22] It is possible to replicate Stuxnet in many forms to use

---

17. Wyn Q. Bowen & Jonathan Brewer, "Iran's Nuclear Challenge: Nine Years and Counting," *International Affairs* 87, No. 4 (July, 2011): pp. 923-943.

18. David Albright, Paul Brannan, & Christina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?" *Institute for Science and International Security* (December 22, 2012).

19. *Id.*

20. *Id.*

21. *Id.*

22. Thomas M. Chen & Saeed Abu-Nimeh, "Lessons From Stuxnet," *Computer* 44, No. 4 (April, 2011): pp. 91-93.

against any automated industrial control system.[23] Any company that utilizes supervisory control and data acquisition systems (SCADA) is exposed to the virus.[24] Elements of our critical infrastructure exposed to the virus include oil refineries, health care systems, and nuclear facilities.[25] Because the virus is difficult to detect, it can spread to almost any network that uses SCADA systems or otherwise any industry that has automated functions within its computer systems. Exposure to critical infrastructures within a state threatens large population centers.[26] The Stuxnet virus and potential variations that target industrial systems and critical infrastructure are undoubtedly a serious threat for both the public and private sectors.

2 The Russian Hack on Estonia

Beginning on April 27, 2007, a series of cyber-attacks began against Estonia, attacking many outlets of its critical infrastructure, including the Estonian Parliament, banks, television

23. *Id.*
24. *Id.*
25. Despite the fact that development of new weapons using new technology fits well into the history of warfare, the frightening reality is that states have now made use of technology to conduct warfare against both the private and public sectors of other states and within their own borders. See David Alan Grier, "Sabotage," *Computer* (November, 2010): pp. 6-8.
26. Chen & Abu-Nimeh, *supra*, note 16.

broadcasters, and local governments.[27] The attacks caused a major disruption in everyday business.[28] In 2007, Estonia's digital infrastructure was already very sophisticated, and many different transactions were commonly conducted online, including the signing of legal documents, paying local and federal taxes, and voting.[29] These attacks disrupted many of these functions and caused millions in damages to the Estonian digital infrastructure.[30]

The attacks began amid a disagreement between the Estonian and Russian governments over the status of a controversial Soviet war grave in Tallinn.[31] The Bronze Soldier of Tallinn marked the remains of Soviet soldiers that fought in Tallinn against the Finns and Germans during the Second World War.[32] The Estonian government wanted to relocate the memorial because of

---

27. Peter Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic," Washington Post (May 19, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122_pf.html.

28. *Id.*

29. Estonia was arguably the most technologically advanced country in Europe 2007 in terms of how much government and everyday business could be conducted online. And, despite the hacks of 2007, Estonia remains technologically advanced, especially relative to neighboring states. *See id.*

30. *See* Sean Collins & Stephen McCombie, "Stuxnet: the Emergence of a New Cyber Weapon and its Implications," 7 J. OF POLICING, INTELLIGENCE, AND COUNTER TERRORISM 80 (2012).

31. *See* Linda Kinstler, "How to Survive a Russian Hack: Lessons from Eastern Europe and the Baltics," THE ATLANTIC (Feb. 2, 2017).

32. Arnold Sinisalu, "Propaganda, Information War, and the Esotnian-Russian Treaty Relations: Some Aspects of International Law." 15 JURIDICA INTERNATIONAL 154, 160 (2008).

its location near a busy road intersection.[33] Ethnic Russians living in Tallinn saw this as a pretext to erasing Soviet (and, therefore, Russian) history from Estonia, which had recently joined the European Union and was essentially trying to cleanse itself from any Soviet memories.[34] Amid violent protests and riots by the ethnic Russians, the Estonian government quietly dismantled the memorial on April 27, 2007, and relocated it to a hilltop called Tõnismãgi within the city limits.[35] The cyber-attacks began shortly thereafter on the same day.[36]

The Russian government denies any involvement in these cyber-attacks.[37] While there is little concrete proof that the Russian government was involved with the attacks, military experts agree that an attack of this scale and scope could not have occurred without the government's

---

33. *Id.*

34. *Id.* Estonia's losses in World War II—25% of its population—were among the highest proportionally in Europe. Estonians are Finnic people, whose language is mutually-intelligible with Finnish, and one of only six non-Indo-European languages spoken in Europe—the others being Hungarian (a distantly-related Uralic language), Basque (a language isolate), Maltese (a Semitic language closely related to Arabic) and Turkish. As a result, even after the Estonians capitulated to the Soviets during the war, they often discreetly aided the Finns in their efforts against the Soviets by broadcasting messages when planes were taking off from Tallinn and heading towards Helsinki. Most Estonians do not have happy memories from the Soviet occupation in the post-war years and are enthusiastic about the European Union and Westernization in general. *See generally* Hannes Walter, "Estonia in World War II," Historical Text Archive (accessed Apr. 10, 2017), http://historicaltextarchive.com/sections.php?action=read&artid=383.

35. Sinisalu, *supra*, note 27.

36. Finn, *supra*, note 21.

37. Kinstler, *supra*, note 25.

blessing and aid.[38] Anatoly Tsyganok, a high-level Russian military officer, publicly stated in the newspaper *Gazeta* that even if Russia had been involved in the attack, it did not violate international law because international law at the time did not address cyber-attacks.[39] This public statement is strong circumstantial evidence in support of the proposition that Russia was involved.[40] Russia has pointed to hackers in the Moldovan breakaway region of Transnistria who have claimed responsibility for the attacks.[41] Indeed, a member of a pro-Kremlin group based in Transnistria claimed responsibility for the attacks, though it is doubtful that the attacks would have been logistically possible without some direction and guidance from the Kremlin.[42] In the same year the attacks against Estonia occurred, similar attacks occurred against the Georgian

38. Russia is also suspected of conducting cyber-attacks against Georgia during the Georgia-Abkhazia conflict in 2007. *See* William C. Ashmore, "Impact of Alleged Russian Cyber Attacks," U.S. DEPARTMENT OF DEFENSE, Defense Technical Information Center (May, 2009).

39. A. Novikova, V. Lyubartas, "Voenno-virtuallnyy alyans," GAZETA, No. 23 (Feb. 2, 2008), http://gzt.ru/world/2008.02.07/220025.html.

40. Sinisalu, *supra*, note 26 at 161.

41. Christian Lowe, "Kremlin loyalist says launched Estonia cyber-attack," Reuters International (Mar. 13, 2009, 3:00 a.m.), http://www.reuters.com/article/us-russia-estonia-cyberspace-idUSTRE52B4D820090313.

42. *Id.*

government alongside the Russian invasion of Georgia during the Abkhazia conflict.[43] Russia has yet to acknowledge its involvement with the cyber aspects of this attack.[44]

Russia's very probable involvement with this cyber-attack is indicative of another normalization of cyber warfare in the digital age. States within the international system now have a very specific and vitally important interest in protecting all digital critical infrastructure from exposure to cyber-attacks, especially since there is no remedy available within the international system after an attack has occurred.[45] And as more states continue to employ cyber tactics instead of conventional warfare tactics, the cyber tactics become normalized globally. And, indeed, because international law does not directly address cyber tactics in its rules of war, states are still shielded from any real consequences for using such tactics.

---

43. *See, e.g.*, Lesley Swanson, "The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict." 32 LOY. L.A. INT'L & COMP. L. REV. 303 (2010).

44. The Georgia-Abkhazia Conflict was perhaps the first time in the history of warfare where cyber-attacks were used alongside conventional warfare tactics. *See id.* at 304. Some Russian apologists contend that even though Russia did indeed conduct these attacks, the acts did not amount to a full-scale cyber war. *See* Ethan Zuckerman, "Misunderstanding Cyberwar in Georgia," REUTERS, (Aug. 16, 2008), http://www.reuters.com/article/reutersEdge/idUSGOR66065320080816.

45. *See, e.g.*, Koen Gijsbers & Matthijs Veenendaal, "Protecting the National Interest in Cyberspace," GEORGETOWN J. OF INTL. AFFAIRS 191 (2011).

## B State versus Non-State Cyber Warfare

A state may not always directly attack another state. Sometimes, a state finds that it is within its national interest to target private parties, or any non-state actor, such as a multi-national corporation or an individual not associated with a government. Those private parties might reside in a country the perpetrator opposes. Or sometimes a state may target a private party for strategic reasons. But, a state need not target another state to conduct a cyber-attack, as the following cases will demonstrate.

### 1 Democratic National Committee Email Leak

On July 22, 2016, WikiLeaks—a nonprofit organization that routinely publishes classified government or business information—published a series of emails sent between members of the Democratic National Committee that indicated that they preferred former Secretary of State Hillary Clinton as the Democratic nominee over her challenger Vermont Senator Bernie Sanders.[46] WikiLeaks' alleged source was someone going by the moniker "Guccifer 2.0," who was later

46. Karen Tumulty & Tom Hamburger, "WikiLeaks releases thousands of documents about Clinton and internal deliberations," WASHINGTON POST (July 22, 2016), https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/?utm_term=.507b25e1b2f6.

confirmed by the cybersecurity group CrowdStrike to be based in Russia.[47] Several other cyber security groups that conducted the same analysis agreed with CrowdStrike's conclusion, and one organization—Mandiant—concluded further that the malware used to obtain the information was similar to the malware used in the Russian attack on Estonia, leading to the supposition that the Kremlin was behind the attack.[48]

WikiLeaks published further emails on November 7, 2016, the day before the 2016 U.S. Presidential Election.[49] This particular publication happened simultaneously with a distributed denial of service (DDoS) attack on the DNC website, which flooded the site with so much traffic that it could not function properly.[50] This batch of emails detailed the DNC's tactics to discredit potential vice-presidential candidates, though none of them had mentioned Donald Trump's eventual selection, Indiana Governor Mike Pence.[51] In a secret investigation, the CIA concluded that these leaks were part of a broader Russian effort to smear Hillary Clinton's public image to

---

47. Ellen Nakashima, "Cyber researchers confirm Russian government hack of Democratic National Committee," Washington Post (June 20, 2016).

48. *Id. See also* Dmitri Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee," CrowdStrike Blog, (June 15, 2016), https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

49. Joe Uchill, "WikiLeaks releases new DNC emails day before election," The Hill (Nov. 7, 2016), http://thehill.com/policy/cybersecurity/304648-wikileaks-releases-new-dnc-emails-suffers-cyberattack.

50. *Id.*

51. *Id.*

assist Donald Trump in winning the election.[52] Both Trump and the Kremlin continue to deny these allegations, despite the overwhelming evidence implicating the Kremlin's involvement and increasing evidence that members of Donald Trump's campaign team were in contact with Russian officials.[53]

Russia is a prolific perpetrator of cyber-attacks, and it has conducted these attacks for a variety of reasons. In this case, it did not attack the state directly, but it targeted a non-state actor for the purpose of influencing the outcome of the presidential election. Clearly, Russian President Vladimir Putin preferred a Trump victory.[54] Trump lauded Putin and openly admired his strong-arm style of governance, while Hillary Clinton openly defied Putin during her tenure as Secretary

---

52. Adam Entous, Ellen Nakashima, & Greg Miller, "Secret CIA assessment says Russia was trying to help Trump win White House," Washington Post (Dec. 9, 2016), https://www.washingtonpost.com/world/national-security/obama-orders-review-of-russian-hacking-during-presidential-campaign/2016/12/09/31d6b300-be2a-11e6-94ac-3d324840106c_story.html?utm_term=.fe8101d6abf1.

53. *See, e.g.*, ABC Australia "Kremlin dismisses US Democratic email hack claims as 'absurd' and an 'old trick,'" (July 26, 2016, 3:22 p.m.), http://www.abc.net.au/news/2016-07-27/kremlin-says-idea-it-hacked-us-democratic-party-emails-absurd/7663558. At the time I submitted this paper, several Trump allies, including shamed National Security Advisor Michael Flynn and former campaign manager Paul Manafort are believed to be under FBI investigation for criminal activity involving the Trump campaign and alleged ties to the Russian regime. *See e.g.*, Michael Crowley, "What is the Real Story of Donald Trump and Russia?" Politico (Mar. 1, 2017), http://www.politico.com/magazine/story/2017/03/connections-trump-putin-russia-ties-chart-flynn-page-manafort-sessions-214868.

54. *See, e.g.*, Ruth Deyermond, "Russia's Trump Card? The Prospects for Russia-US Relations After the Election of Donald Trump," 194 RUSSIAN ANALYTICAL DIGEST 2 (2016).

of State and actively took steps to weaken Russian influence in Eastern Europe.[55] The big picture implications of this attack should be alarming to Americans—a weaker state took measures to impact the election in a stronger state.[56] Power politics in the digital age is an entirely different calculus than it was before cyber-attacks were possible. Military might, nuclear arsenals, wealth, global influence, and geography may be less important to state power now than the availability of skilled hackers.[57] A state can now attack a non-state actor in order to influence politics abroad, though the repercussions of the DNC hack may hurt the Russian regime in the future.[58] But states may also choose to target a non-state actor to distract its populations from its domestic problems.

---

55. *Id.*

56. Michael H. Fuchs, et al., "Why Americans Should Care About Russian Hacking," CENTER FOR AMERICAN PROGRESS (Feb. 14, 2017), https://cdn.americanprogress.org/content/uploads/2017/02/13093554/RussianHackingWhyItMatters-brief.pdf.

57. Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," 4 J. OF STRATEGIC SECURITY 49 (2011). *See also* Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," 36 YALE J. INT'L L. 421 (2011).

58. Russia may have overplayed its hand in influencing the U.S. election because it displayed to potential allies looking for an alternative to the U.S. or E.U. as an ally that it is untrustworthy and willing to go to extreme measures to influence global politics. *See* Nigel Inkster, "Information Warfare and the US Presidential Election," 58 GLOBAL POLITICS AND STRATEGY 23 (2016).

2 The DPRK Hack on Sony

On November 24, 2014, a group identifying itself as the 'Guardians of Peace' (GOP) released confidential data illicitly obtained from Sony Pictures.[59] The data contained information about Sony employees and their families as well as Sony's private financial information.[60] The hackers used a sophisticated server message block (SMB) worm to infiltrate the Sony databases and crack security codes, giving the hackers unlimited access to private financial and accounting information.[61] The immediate suspect was obvious—North Korea (DPRK). Quickly, the FBI confirmed that the DPRK government was behind the attack, and that the motive was revenge against Sony Pictures over its production of the film *The Interview*.[62]

---

59. Gabi Siboni & David Siman-Tov, "Cyberspace Extortion: North Korea versus the United States," INSTITUTE FOR NATIONAL SECURITY STUDIES, INSS Insight, No. 646 (Dec. 23, 2014), http://www.inss.org.il/uploadImages/systemFiles/No.%20646%20-%20Gabi%20and%20Dudi%20for%20web.pdf

60. *Id.*

61. Mike Lennon, "Hackers Used Sophisticated SMB Worm Tool to Attack Sony," SECURITYWEEK (Dec. 19, 2014), http://www.securityweek.com/hackers-used-sophisticated-smb-worm-tool-attack-sony.

62. *See, e.g.*, David E. Sanger & Nicole Perlroth, "U.S. Said to Find North Korea Ordered Cyberattack on Sony," NEW YORK TIMES (Dec. 17, 2014), https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=1.

For months, the DPRK government had complained about the film.[63] The film, directed and starring comedian Seth Rogen, focuses on an interview of DPRK leader Kim Jeong-eun.[64] Like many Rogen films, it is a crass and irreverent film, and it paints Kim as a "sad, sentimental man-child" who parties like a typical wealthy American frat-boy.[65] While not as crass as previous films that satirized the DPRK regime, Kim took personal offense to this film and demanded that Sony not release the film months before its scheduled release.[66] In response to the initial hacks, Sony decided not to release the film on its scheduled Christmas release date.[67] While the film received mixed to poor reviews on its own merits, Sony's actions in pulling the film from theatres caused public outrage, and it was seen as the DPRK regime intimidating American consumers.[68] In response, many theatres began showing *Team America: World Police*, an older film by *South*

---

63. *See, e.g.*, Ben Beaumont-Thomas, "North Korea complains to UN about Seth Rogen comedy The Interview,' The Guardian (July 10, 2014, 3:37 a.m.), https://www.theguardian.com/film/2014/jul/10/north-korea-un-the-interview-seth-rogen-james-franco.

64. *See, e.g.*, Mike Hale, "Memo to Kim Jong-un: Dying is Easy, Comedy is Hard," NEW YORK TIMES (Dec. 19, 2014), https://www.nytimes.com/2014/12/20/arts/the-disconnect-of-the-interview.html?partner=rss&emc=rss&smid=tw-nytmovies&_r=0.

65. *Id.*

66. Beaumont-Thomas, *supra*, note 49. For background on other films that have satirized the DPRK regime, *see, e.g.*, Roger Ebert, "Team America: World Police," ROGEREBERT.COM (Oct. 14, 2004), http://www.rogerebert.com/reviews/team-america-world-police-2004.

67. Sanger & Perlroth, *supra*, note 48.

68. *Id.*

*Park* creators Matt Stone and Trey Parker that more grotesquely features now-deceased DPRK leader Kim Jeong-il as a marionette, speaking broken English in a stereotypical Asian accent.[69]

A state may choose to attack a non-state actor for a variety of reasons. On the surface, North Korea's reaction to a crass American film seems petty and characteristic of a rogue, unstable regime. But there may be a deeper truth hidden in Kim's tactics. Georgetown University Professor Victor Cha, an expert on the DPRK regime, believes that the regime is in its last days because of demographic changes, crumbling infrastructure, and greater (but certainly unintentional) access to communications to the outside world.[70] States on the decline tend to create conflicts as a diversion, such that the population rallies behind the state in its effort in the fabricated-conflict, rather than works against the unpopular regime.[71] Examples of such diversionary wars include the Argentine

---

69. Trey Parker voices Kim in the film, and uses the same voice he uses to depict the owner of the Chinese take-out restaurant in the show *South Park*. *See* Katie Rife, "Alamo Drafthouse replaces *The Interview* with *Team America: World Police,"* The AV Club (Dec 18, 2014, 2:02 p.m.), http://www.avclub.com/article/alamo-drafthouse-replaces-interview-team-america-w-213181.

70. Victor Cha, *The Impossible State: North Korea Past and Future*, (2012), 437-444. *See also* Stephan Haggard & Jon R. Lindsay, "North Korea and the Sony Hack: Exporting Instability Through Cyberspace," 117 ASIA PACIFIC ISSUES 1 (2015).

71. This strategy is also known as the "Rally Around the Flag Syndrome." Amy Oakes, "Diversionary War and Argentina's Invasion of the Falkland Islands," 15 SECURITY STUDIES 431 (2006). *See also* Amy Oakes, *Diversionary War: Domestic Unrest and International Conflict* (2012).

invasion of the Falkland Islands and U.S. President James Buchanan's decision to send troops into Mormon Utah to depose Brigham Young as territorial governor.[72]

If more states begin using cyberattacks, both against state and non-state actors, as a diversionary tactic, more diversionary conflicts may develop because it will become much cheaper for a state in decline to start them. Moving forward, the international system is in a more precarious state, and conflicts are likely to become more commonplace, and possibly escalate from cyber-attacks. For the DPRK, it remains to be seen if full-scare war is truly foreseeable.[73]

### C Non-State versus State Cyber Crime

States will generally view attacks against the state by non-state actors as a form of terrorism.[74] Like the term 'terrorism' itself, the term 'cyberterrorism' is controversial among academics and policymakers, because it is not easy to distinguish which kinds of cyber-crimes by non-state actors are mere crimes and which ones are acts of terror.[75] But a fair starting point in

---

72. *Id.*

73. *See, e.g.*, David E. Sanger & William J. Broad, "A 'Cuban Missile Crisis in Slow Motion' in North Korea," NEW YORK TIMES (Apr. 16, 2017), https://www.nytimes.com/2017/04/16/us/politics/north-korea-missile-crisis-slow-motion.html?_r=0.

74. *See, e.g.*, Thomas Homer-Dixon, "The Rise of Complex Terrorism," in *Classic Readings and Contemporary Debates in International Relations*, 3d., Phil Williams, et al., eds. (2006), 653-60.

75. *See, e.g.*, Sara Hower & Kathleen Uradnik, *Cyberterrorism* (2011), 140-49.

distinguishing the terms is identifying the victim. When the target is a state-actor, it may be more likely an act of cyberterrorism. Coming to this conclusion requires an understanding of how to define terrorism in general.

It is impossible to understand the logic of terrorism without first understanding the basic tools needed to control a population. John Gaventa discusses statecraft with the three dimensions of power.[76] Through the first dimension of power, a state controls its population through brute force; resources are controlled by the state in order to alter the citizen's cost-benefit analysis of rebelling.[77] Through the second dimension of power, the state institutes and perpetuates societal biases, taking away resources with which to rebel by adding obstacles.[78] An example of the second dimension of power in the U.S. is the Jim Crow laws in the South.[79] The third dimension of power offers its citizens carrots and sticks so that they feel that the system is inherently just and there is no reason to rebel.[80] In reality, it is forced habituation.

---

76. Gaventa, *supra*, note 6.
77. *Id.*
78. *Id.*
79. *Id.*
80. *Id.*

Terrorism, quite simply, is a tool of an insurgency.[81] It is a punishment-based coercive strategy that is both inherently psychological and inherently violent.[82] It is normally favoured by the weak against the strong – generally, sub-state actors against states – because it is their only realistic option.[83] Generally, the target is the civilian population because the point is to psychologically intimidate the population in order to coerce the ruling power to change its behaviour. In order for a terror attack to take place, a terrorist needs both the motive and opportunity to strike.[84] With this pattern, it must also be noted that terrorism is inherently political because it is linked to insurgencies and political violence. The insurgency is the big picture; terrorism is merely the strategy.[85] In this regard, acts of blatant political rebellion or ties to an insurgency that utilize cyber-tactics can be regarded as acts of cyber-terrorism, regardless of any ethical debates. The perpetrator's goal is politically-motivated. As such, the target may also be a non-state actor. The following two cases, however, demonstrate how non-state actors can target state actors for political purposes.

---

81. Ariel Merari, "Terrorism as a Strategy of Insurgency," in *The History of Terrorism from Antiquity to Al Qaeda*, Gérard Chaliand & Arnaud Blin, eds. (2007), 12-51.

82. *Id.*

83. *Id.*

84. *Id.*

85. *Id. See also* Arnaud Blin, "The United States Confronting Terrorism," in *The History of Terrorism from Antiquity to Al Qaeda*, Gérard Chaliand & Arnaud Blin, eds. (2007), 398-419.

1 Operation Tunisia

"Anonymous" is a loose international network of private hacktivists—computer hackers who conduct their activities with a political motive (political activists who hack).[86] It has its origins in online message boards such as 4chan and Reddit, but there is no leadership structure or individual founder of the organization.[87] Anonymous has been a formidable political force in the past decade, helping to incite political unrest in unstable regimes.[88] The Arab Spring, a series of political rebellions and revolutions in the Arab World starting in 2010, led to regime change in several states. The first state to experience such a change was Tunisia.[89]

Anonymous' involvement in the Tunisian Revolution is known as 'Operation Tunisia.' During this cyber campaign, Anonymous hackers attacked government websites, provided protestors within Tunisia with encryption software so that they could more easily communicate

86. *See generally* Parmy Olson, *We Are Anonymous: Insie the Hacker World of LilzSec, Anonymous, and the Global Cyber Insurgency* (2012).

87. *See id.*

88. Gabriella Coleman, "What It's Like to Participate in Anonymous' Actions," THE ATLANTIC (Dec. 10, 2010), https://www.theatlantic.com/technology/archive/2010/12/what-its-like-to-participate-in-anonymous-actions/67860/.

89. *See, e.g.,* Lisa Anderson, "Demystifying the Arab Spring: Parsing the Differences Between Tunisia, Egypt, and Libya," 90 FOREIGN AFFAIRS 2 (2011); Khair El-din Haseeb, "The Arab Spring Revisited," 5 CONTEMPORARY ARAB AFFAIRS 185 (2012).

with social media, and spoke to Tunisian citizens through YouTube.[90] Anonymous' primary motivation was to incite regime change. For over twenty years, President Zine El Abidine Ben Ali had ruled over Tunisia.[91] Ben Ali, although undoubtedly a dictator, has been considered less problematic than other Middle Eastern leaders because Tunisia enjoyed greater wealth, a vibrant middle class, a fantastic educational system, and a strong labor movement as compared to other countries in the region.[92] But Ben Ali's suppression of free speech augmented a generational divide between millennials and older generations that most Middle East scholars did not foresee.[93] Millennials demanded democratic change, and with Anonymous' help and encouragement, their protests overwhelmed the Ben Ali regime.[94] Ben Ali fled the country and for the first time in two decades Tunisia would have a new government.[95]

Because Tunisia was a relatively stable regime, scholars and policymakers around the world were shocked that it was the first domino to fall in the Arab Spring revolutions.[96] The most

---

90. Anonymous, "Operation Tunisia – A Press Release," YOUTUBE, channel Anonymousworldwar3, (Jan. 5, 2011), https://www.youtube.com/watch?v=BFLaBRk9wY0.
91. Anderson, *supra*, note 89.
92. *Id.* at 3.
93. F. Gregory Gause III, "Why Middle East Studies Missed the Arab Spring: The Myth of Authoritarian Stability," 90 Foreign Affairs 81, 83 (2011).
94. *Id.* at 83-84.
95. *Id.*
96. *See id.*

likely reason why regime change was possible in such a regime is the generational divide between millennials (born between 1984 and 2002) and older generations.[97] Millennials, undoubtedly influenced by Anonymous' internet campaign, took advantage of online social media to spread the revolution and draw inspiration from other political protests in other Arab nations.[98] Without the available technology and platforms of communications, it is unlikely that these revolutions would have occurred, or if they had occurred, they would have required more popular support across generations to be successful.[99]

2 2016 Dyn Cyber Attack

On October 21, 2016, a DDoS attack began against Dyn, Inc., a top internet performance management company in the United States.[100] While Dyn is a private company, the enormity of this attack, its impact on the American digital critical infrastructure, and the vulnerabilities of that critical infrastructure it exposed qualifies this attack as an attack against the broader population of

97. *See* Gilad Lotan, et al., "The Revolutions Were Tweeted: Information Flows During the 2011 Tunisian and Egyptian Revolutions," 5 Int'l J. of Communication 1375 (2011).
98. *Id.*
99. *Id.*
100. *See, e.g.*, Darrell Etherington & Kate Conger, "Large DDoS attacks cause outages at Twitter, Spotify, and other sites," TECHCRUNCH (Oct. 21, 2016), https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/.

the United States, and, therefore, it is a non-state versus state attack.[101] The attack caused major disruptions on several websites, including Amazon, Etsy, Spotify, Twitter, Reddit, the New York Times, the Washington Post, and Netflix.[102] These are all major commercial entities that either exclusively or heavily rely on internet access. And while the attack was mitigated within hours, it left many wondering if an attack like this could happen again and if it could last longer, thus disrupting the flow of their daily lives.[103] Holes in critical infrastructure create opportunities for non-state actors to target private companies with the intent of causing harm to the entire state, and this threat is especially augmented in the United States where the vast majority of critical infrastructure is privately owned.[104]

---

101. The United States government addressed this attack. The FBI, Department of Homeland Security, and the CIA investigated the attack and considered it an attack against the United States despite the direct victim being a private company. *See* Riley Walters & Jacob Jordan, "U.S. Must Remain Vigilant to Counter Cyberattacks," THE DAILY SIGNAL (Oct. 26, 2016), http://dailysignal.com/2016/10/26/how-a-cyberattack-took-down-twitter-netflix-and-the-new-york-times/.

102. *Id. See also* Etherington & Conger, *supra*, note 100.

103. *See* Brian Krebs, "DDoS on Dyn Impacts Twitter, Spotify, Reddit," KrebsOnSecurity (Oct. 21, 2016), https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/.

104. Paul Rosenzweig, "The Reality of Cyber Conflict: Warfare in the Modern Age," THE HERITAGE FOUNDATION (2016), 2017 Index of U.S. Military Strength, http://index.heritage.org/military/2017/essays/reality-cyber-conflict/.

Security professionals remain unsure who was behind the attack. The U.S. Government, as well as other entities, are certain that it was a non-state actor or group of non-state actors behind the attack.[105] Supporters of WikiLeaks and members of Anonymous have claimed responsibility for the attack, but researchers are skeptical of these claims and believe it more likely to have been an unorganized and spontaneous attack by a single individual or a relatively small group of individuals.[106] This particular attack, along with Anonymous' involvement in regime change, are both forms of 'hacktivism,' where non-state actors use the internet to attack other users or entities on the internet for a specific purpose, often political.[107]

Hacktivists use the internet for all sorts of political purposes. They incite regime change, protest government restrictions on free speech, attempt to win hearts and minds in favor of a particular political ideology, and act in vengeance for what they perceive as illicit government actions.[108] With the rise of national populism all around the world, cyber hacktivism has become

---

105. Drew FitzGerald, "National Intelligence Director Says Data Suggests 'Nonstate Actor' Was Behind Cyberattack," WALL STREET JOURNAL (Oct. 25, 2016, 5:02 p.m.), https://www.wsj.com/articles/national-intelligence-director-says-data-suggests-nonstate-actor-was-behind-cyberattack-1477423059.

106. Eric Geller & Tony Romm, "WikiLeaks supporters claim credit for massive U.S. cyberattack, but researchers skeptical," POLITICO (Oct. 21, 2016, 8:05 p.m.), http://www.politico.com/story/2016/10/websites-down-possible-cyber-attack-230145.

107. Noah C.N. Hampton, "Hacktivism: A New Breed of Protest in a Networked World," 35 B.C. INT'L & COMP. L. REV. 511 (2012).

108. *Id.*

an outlet for political dissent, and it will undoubtedly continue to be a dissent for the millennial generation, who largely rejects this ideology. We will undoubtedly see more from hacktivists in the future, but hacktivists need not carry a noble political purpose to operate. Some may recklessly commit crimes that adversely impact civilian populations.[109] Because of this reality, both the private and public sectors must work towards strengthening critical infrastructure, such that a malicious attack that would impact the civilian population can be mitigated.[110]

### D Non-State versus Non-State Cyber Crimes

Not all cybercrimes have a political purpose. Individual cyber criminals or groups of criminals may use their hacking skills for a variety of personal reasons. Revenge, attention, and "just for fun" are all motivating factors for targeting non-state entities.[111] While the following cases may not have had any major geopolitical implications within the international system, they do highlight the terrifying reality that no private digital data is truly private or safe. Luckily, because these cases are clearly acts of low-level crime, it may be easier for the international system to come together and find solutions to prosecute such crimes.

---

109. *Id.*
110. *See* Flynn, *supra*, note 8.
111. *See* Johan Sigholm, "Non-State Actors in Cyberspace Operations," SWEDISH NATIONAL DEFENSE COLLEGE, Student Paper, 11 (Apr. 10, 2013), http://journal.fi/jms/article/view/7609/6083.

1 Ashley Madison Data Breach

In July, 2015, a group that called itself "The Impact Team" hacked into the databases of Ashley Madison, a dating website for married people that seek extramarital affairs.[112] The hackers successfully obtained several gigabytes worth of personal data pertaining to the site's patrons, including names, addresses, and credit card numbers.[113] They threatened to release this data if the site was not immediately shut down.[114] When the site was not shut down, the group followed through on its promise and released the private data, which included over 15,000 email addresses from government and military servers alone.[115] All over the country, people—especially men—panicked about the possibility of being exposed as an unfaithful spouse.[116] Avid Life Media, the parent company of Ashley Madison, condemned the data breach as "not an act of hacktivism [but] an act of criminality."[117]

---

112. Daniel Victor, "The Ashley Madison Data Dump, Explained," New York Times (Aug. 19, 2015), https://www.nytimes.com/2015/08/20/technology/the-ashley-madison-data-dump-explained.html?_r=0.

113. *Id.*

114. *Id.*

115. *Id.*

116. *Id.*

117. *Id. See also* Ashley Madison, Press Release (Aug. 18, 2015), http://media.ashleymadison.com/statement-from-avid-life-media-inc-august-18-2015/

Ashley Madison paid $1.66 million penalty to the Federal Trade Commission ("FTC") for "lax data security and deceptive practices" and a civil settlement of $17.5 million to a class of individuals impacted by the breach "was suspended based on the inability of [the parent company] to pay."[118] The FTC has been vigilant about handing penalties to companies that clearly need to enhance their security mechanisms.[119] This is good news for private consumers who are increasingly dependent on internet commercial transactions and private digital data generally.[120] In this regard, the Ashley Madison affair represents something more important than the incident itself—the Ashely Madison affair has made it clearer to the general public that our personal private data is not safe, and that hackers do not have boundaries.[121] Not many have sympathy for Ashley Madison users because extramarital affairs are socially unacceptable, but similar data breaches have happened to other companies conducting business on the internet, including retailer Target

118. REUTERS, "Ashley Madison Owner Reaches $1.6 million Settlement," repub. by NEW YORK TIMES (Dec. 14, 2016), https://www.nytimes.com/2016/12/14/business/ashley-madison-settlement.html.

119. Steve Mansfield-Devine, "The Ashley Madison Affair," 15 NETWORK SECURITY 8 (2015).

120. *Id.*

121. *Id.*

and video-game giant Sony.[122] Ashley Madison's embarrassing media exposure will perhaps incite major industry changes in cyber security, such that our personal private data is safer.[123]

2 "The Fappening"

Hackers do not always hack to find personal financial information. Sometimes, hackers hack just to embarrass others. The 2014 iCloud data breach did just that. On August 31, 2014, several hundred nude photographs, mostly of female celebrities, were posted on popular image board websites 4chan and Reddit.[124] Among the victims were actress Kate Upton and her boyfriend professional baseball player Justin Verlander, actress Mary Elizabeth Winstead, and Academy Award-winner Jennifer Lawrence.[125] The leak caused an uproar in the celebrity community worldwide, sparking numerous condemnations of the act as a sex crime and an ugly

122. *See, e.g.*, Hiroko Tabuchi, "$10 Million Settlement in Target Data Breach Gets Preliminary Approval," NEW YORK TIMES (Mar. 19, 2015), https://www.nytimes.com/2015/03/20/business/target-settlement-on-data-breach.html; Nick Bilton & Brian Stelter, "Sony Says PlayStation Hacker Got Personal Data," NEW YORK TIMES (Apr. 26, 2011), http://www.nytimes.com/2011/04/27/technology/27playstation.html.

123. Mansfield-Devine, *supra*, note 119.

124. Mike Isaac, "Nude Photos of Jennifer Lawrence Are Latest front in Online Privacy Debate," New York Times (Sep. 2, 2014), https://www.nytimes.com/2014/09/03/technology/trove-of-nude-photos-sparks-debate-over-online-behavior.html.

125. *Id.*

violation of personal privacy.[126] The affair became popularly known as both 'Celebgate' and 'The Fappening.'[127]

The sources of the leaked photos were the individual's iPhones.[128] Apple provides its iPhone users with free cloud storage, which allows the users to store photos, videos, personal data, and music on an external drive that can be accessed from any internet-ready device.[129] Google offers a similar cloud service with several Android-ready phones.[130] Cloud storage is a useful and convenient tool for individuals and companies that rely on digital data in their daily lives, but there is still much debate in the computer science community on how to make cloud storage more secure and less vulnerable to data breaches such as the Fappening.[131] While that debate continues, the criminal justice system is better-equipped to handle prosecuting non-state actors for these types of

---

126. *See, e.g.*, Jenn Selby, "Emma Watson on Jennifer Lawrence nude pcitures leak: 'Even worse than seeing women's privacy violated is reading the comments'" INDEPENDENT (Sep. 2, 2014, 8:03 a.m.), http://www.independent.co.uk/news/people/emma-watson-on-jennifer-lawrence-naked-photo-leak-even-worse-than-seeing-womens-privacy-violated-is-9705570.html.

127. The term 'Fappening' is a portmanteau of the word 'fap,' an onomatopoeic slang term for male masturbation, and '*The Happening*,' a science fiction film by M. Night Shyamalan. *See* Fernando Alfonso III, "Alleged nude photos of Jennifer Lawrence leaked from 4chan," The Daily Dot (Aug. 30, 2014), https://www.dailydot.com/upstream/jennifer-lawrence-4chan-nudes-leaked/.

128. Isaac, *supra*, note 124.

129. *Id.*

130. *Id.*

131. *See, e.g.*, Bernd Grobauer, et al., "Understanding Cloud Computing Vulnerabilities," 9 IEEE SECURITY & PRIVACY 50 (2010).

acts, although work still must be done to ensure that cybercrimes stand on their own as crimes and are recognized as special kinds of crimes. The FTC has already begun that trend by punishing companies that fail to provide adequate digital security to protect user data.[132] But these acts are undoubtedly criminal acts, and civil fines against the companies with inadequate data will not stop crimes from happening, although it may make them harder to commit if the companies build more competent security mechanisms.

### *III Prosecuting Cyber Crimes in the United States*

The U.S. Constitution only requires that one federal court exist, and beyond this requirement Congress has authority "to ordain and establish" other courts, which includes the U.S. District Courts and the U.S. Court of Appeals.[133] Congress has established other courts throughout its history, perhaps most notably the courts created by the Foreign Intelligence Service Act (FISA). FISA established courts that are accessible only to the federal government, and its findings are almost never made public.[134] The FISA courts issue warrants at the government's request to allow search warrants against foreign spies in the United States.[135] Because of the significantly increased

---

132. *See, e.g.*, Tabuchi, *supra*, note 122.
133. *See* U.S. CONST. Art. III, sec. 1
134. David B. Cohen & John Wilson Wells, *American National Security and Civil Liberties in an Era of Terrorism*, 34 (2004).
135. *Id.*

use of these types of search warrants and the cloud of secrecy surrounding the FISA court system, it has been described an "almost parallel Supreme Court."[136]

While it is possible to see a role for the FISA courts in combatting cybercrimes, the FISA courts alone are not sufficient. Congress should consider establishing special federal courts that specifically prosecute cybercrimes. Alternatively, it could dedicate resources within the trial-level U.S. District Courts that would solely focus on prosecuting cybercrimes. Other countries have already done so. For example, India established special cybercrime courts in Mumbai in 2016, and they may establish more in other jurisdictions soon.[137] They were first established because there was a "pressing need to rethink about the application of law and delivery of justice under [new] circumstances" and that these circumstances warranted a new court that would focus solely on how to prosecute these crimes within the parameters of current and developing laws.[138] Likewise, the Philippines was in the process of developing such courts, with special focus on child

136. Eric Lichtblau, "In Secret, Court Vastly Broadens Powers of N.S.A." New York Times (July 6, 2013), http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html.

137. Lievanta Millar, "Cops Want Special Courts That Try Only Cyber Criminals," MUMBAI MIRROR (Feb. 18, 2016, 1:45 a.m.), http://mumbaimirror.indiatimes.com/mumbai/other/cops-want-special-courts-that-try-only-cyber-criminals/amp_articleshow/51031675.cms.

138. TNN, "Special courts needed for cases of cyber crime," INDIA TIMES (Sep. 19, 2016, 8:43 a.m.), http://timesofindia.indiatimes.com/city/ahmedabad/Special-courts-needed-for-cases-of-cyber-crime/articleshow/54400724.cms.

pornography and financial hacking, but these plans have been abandoned since the election of proto-nationalist Rodrigo Duterte.[139]

Establishing special courts would allow the United States to more efficiently prosecute cyber criminals within its borders. Most of these criminals would be non-state actors, but hackers acting on behalf of a foreign state could fall under these courts' jurisdiction if they indeed are physically within the United States. These courts would create a sort of centralized governance through which the U.S. Department of Justice could more efficiently allocate resources to combat these specific crimes.[140] This is an important and useful strategy in the coming years as we begin to develop more robust cybercrime statutes and begin to understand cybercrimes more as a society and more broadly within the legal field.[141]

These special courts can also serve as a forum for civil litigation relating to cybercrimes. Most civil court dockets are filled with mundane business and employment disputes, and often those cases have cyber elements to them.[142] New courts specifically for cyber cases could help to

---

139. Ina Reformina, "DOJ wants 10 special courts for cybercrimes," ABS-CBN NEWS (Apr. 16, 204 6:24 p.m.), http://news.abs-cbn.com/focus/04/16/14/doj-wants-10-special-courts-cybercrimes.

140. Susanna Bagdasarova, "Brave New World: Challenges in International Cybersecurity Strategy and the Need for Centralized Governance," 119 PENN ST. L. REV. 1005 (2015).

141. *Id.*

142. Jonathan Mayer, "Cybercrime Litigation," 164 U. PA. L. REV. 1453 (2016).

distinguish between mundane cases and cases that involve serious data breaches, such as the Target data breach.[143] While some scholars believe that civil litigation should not exist for cybercrimes, this would be a serious mistake that would hurt consumers.[144] The cases discussed previously demonstrate that consumers stand to lose the most from a cyber breach, and they should have access to legal remedies when they are victims of such breaches.[145]

In addition to the special courts, Congress should enact a uniform set of laws that define the names, elements, and range of penalties for specific cybercrimes. Vermont enacted a statute that could be used as a starting point for Congress.[146] It defines, for example, theft or destruction of a computer; alternation, damage, or interference with a digital device; unauthorized access; and access for fraudulent purposes.[147] These statues cover several possible instances of cybercrimes, especially those that would be committed by non-state actors. The new court system would most likely be most useful at prosecuting non-state actors, whereas most state actors, and non-state

143. *Id.*

144. Mark A. Rush, Lucas G. Paglia, "Preventing, Investigating, and Prosecuting Computer Attacks and E-Commerce Crimes: Public/Private Initiatives and Other Federal Resources," 14 NO. 8 SOFTWARE L. BULL. 3 (2001).

145. *See id.*

146. Matthew S. Borick, "A Look at Vermont's Computer Crimes Statute," 34-SUM VT. B.J. 38 (2008).

147. *Id.*

actors that target states and civilian populations on a large-scale would be best prosecuted within the international system.

## *IV Strategies for the International System*

In the aftermath of World War II, the deadliest conflict in human history, the victorious allies established the United Nations (U.N.) to maintain international peace and security.[148] An historical milestone in international law, the United Nations established a treaty system that condemned the use of war by its member states, except in the case of self-defense.[149] Article 2 of the U.N. Charter provides that "[a]ll members should settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered."[150] It further provides that "[a]ll members shall refrain in their international relations from the threat or use of force against the integrity or political independence of any state[.]"[151] These provisions were written in 1945, long before cyber warfare was a possibility. And since the Charter was established, the international system has not come together to address cyber warfare as it pertains to the U.N. Charter definitions of war, aggression, and self-defense. It is time for this to change.

148. Arnie J. Schaap, "Cyber Warfare Operations: Development and Use Under International Law." 64 A.F. L. REV. 121, 143 (2009).
149. *Id. See also* U.N. Charter art. 51.
150. U.N. Charter art. 2(3).
151. U.N. Charter art. 2(4).

## A Re-writing International statutes and treaties to reflect technology

While there is little realistic hope that today's international political climate is conducive to re-writing far-reaching treaties such as the U.N. Charter, re-imagining the U.N. Charter considering technological developments in the post-war era is a fantastic start in addressing the issues posed by cyber warfare in the international system. The Charter's language on aggression, war crimes, and self-defense must be updated.

### 1 Act of aggression

Article 39 of the U.N. Charter permits the Security Council to determine whether any act by any member state constitutes an act of aggression.[152] The Rome Statute, effective in 2002, established the International Criminal Court, which has jurisdiction among its signatory states to try cases of aggression.[153] In 1976, the U.N. General Assembly passed an annex to the charter defining 'aggression' as "the use of *armed* force by *a State* against the sovereignty, territorial integrity or political independence of another State, or in *any other manner inconsistent with the Charter*[.]" (emphases added).[154]

---

152. U.N. Charter art. 39; *see also* Theodore Meron, "Defining Aggression for the International Criminal Court," 25 SUFFOLK TRANSNAT'L L. REV. 1, 1-2 (2001).

153. U.N. General Assembly, *Rome Statute of the International Criminal Court* (last amend. 2010), July 17, 1998, art. 5. (effective July 1, 2002). [Rome Statute].

154. U.N. General Assembly, *Resolution 3314 (XXIX). Definition of Aggression*, December 14, 1976, art. 1 [Resolution 3314].

The definition of aggression is necessarily dependent on armed force, pre-dating the possibilities of cyber warfare. It also appropriately focuses on state versus state warfare, because the original purpose of the U.N. is to promote interstate peace and cooperation.[155] Finally, the current definition of aggression allows a catch-all to define something inconsistent with the Charter's purpose as aggression, which does not necessarily require the use of arms to constitute aggression. But even with this catch-all provision, the definition of aggression is insufficient in the era of cyber warfare. It must be changed to either qualify a cyber-attack as an armed attack per the current definition, or eliminate the requirement that an attack involve arms to constitute aggression.

One threshold question to explore when a cyber-attack occurs is what was the purpose of the attack? Many states employ cyber tactics for the purpose of information gathering and espionage, which is not considered to be a traditional act of war, and, indeed, predates international rules of war.[156] While a state employing cyber tactics to uncover classified state information will likely spark some sort of conflict with another state, espionage is not equivalent to a cyber-attack that targets a state's critical infrastructure or population. An attack such as the Stuxnet worm and

155. *See, e.g.*, Schapp, *supra*, note 41.

156. George F. Will, "Defining 'acts of aggression' in the age of cyber warfare," NEW YORK POST (Apr. 13, 2016, 8:44 p.m.), http://nypost.com/2016/04/13/defining-acts-of-aggression-in-the-age-of-cyber-warfare/.

the Russian attack on Estonia, therefore, qualify as cyber-attacks per this threshold question, rather than acts of cyber espionage.[157]

There is much debate as to whether a cyber-attack is an act of war. Ironically, after the Stuxnet worm was discovered, the Pentagon declared that any cyber-attack against the U.S. would be declared an act of war.[158] Journalist Glenn Greenwald pointed out the irony in this policy after the U.S. was essentially caught red-handed employing such attacks:

> Needless to say, if any cyber-attack is directed at the U.S.—rather than by the U.S.—it will be instantly depicted as an act of unparalleled aggression and evil: Terrorism. Just last year, the Pentagon degreed that any cyberattack on the U.S. would be deemed 'an act of war.'[159]

Before Stuxnet was unfolded, the Obama White House commissioned a study on cyberspace and its role within the international system and its potential role in international conflict, which found:

> States have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace . . . . Certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners . . . . when warranted, the United States will respond to hostile acts in cyberspace as we would any other threat to our country.[160]

---

157. *See id.*

158. Reuven Cohen, "The White House and Pentagon Deem Cyber-Attacks 'An Act of War," FORBES (Jun. 5 2012, 7:22 p.m.), https://www.forbes.com/sites/reuvencohen/2012/06/05/the-white-house-and-pentagon-deem-cyber-attacks-an-act-of-war/#17c7859f68ef.

159. *Id.*

160. *Id.*

The United States has clearly in the past several years taken the position that a cyber-attack is an aggressive act that would be construed as an act of war. Despite the irony that the U.S. employs these attacks, this particular view on cyber-attacks is a practical and realistic one in this era. Without recognizing even the most minor and seemingly-innocuous cyber-attacks as equivalent to a conventional attack opens the possibility that more attacks will occur unchecked, and that we will thrust head-on into a world of "drip, drip cyber-attacks" where the impacts of such attacks will eventually compound and have devastating effects on populations an critical infrastructures.[161] Geopolitical forecaster George Friedman has predicted that such cyber-attacks will define conventional warfare by the second half of the 21st Century, ultimately culminating in a world war involving cyber and space weapons.[162] The effect of equating cyber-attacks with conventional attacks within international law could very likely be that states are much more hesitant to conduct such attacks against populations and critical infrastructures of another state,

161. Ellen Nakashima, "When is a cyberattack an act of war?" THE WASHINGTON POST (Oct. 26, 2012), https://www.washingtonpost.com/opinions/when-is-a-cyberattack-an-act-of-war/2012/10/26/02226232-1eb8-11e2-9746-908f727990d8_story.html?utm_term=.a600a07224dc; *See also* Michael J. Glennon, "National Security and Double Government," 5 HARVARD NAT'L SEC. J. 1 (2014).

162. George Friedman, *The Next 100 Years: A Forecast for the 21st Century* (2009), 193-222.

and instead reserving such attacks for use against non-state actors and insurgencies.[163] The definition of aggression should not be dependent on the use of guns and ammunition, but should instead be more results-oriented.[164] Perhaps, simply, the target of the attack should be dispositive in deciding what constitutes aggression. Does the attack aim to impact populations, critical infrastructure, or the government of the target state? If it does, then there should be no doubt that such an attack is an act of aggression, even if conventional weapons are not used.

The Council of Europe's Convention on Cybercrime was the first multilateral treaty that attempted to equate cyber-attacks with conventional attacks, although the effect of the council has been much less far-reaching, mostly as a tool to combat cyber-crimes by non-state actors, such as identity theft and child pornography.[165] This model should be replicated for more than just European signatories. Indeed, it is the responsibility of the developed world—The United States and the Anglosphere particularly at the forefront—to place pressure on the international system to

---

163. *See, e.g.*, Michael Gervais, "Cyber Attacks and the Laws of War," 30 Berkeley J. Int'l L. 525 (2012).

164. The current understanding of the 'use of arms' is obsoletely tied to the Geneva Convention's understanding of an armed force, which defines an armed force with four elements: (1) a formal command structure; (2) a distinctive emblem; (3) the open-carrying of arms; (4) acting in accordance to the customs of war. At least three of these elements are completely obsolete in a cyber setting, and only the first element could be relevant in such a setting, though the victim would not know if there is a formal command structure. *See* Annex I to the Geneva Conventions, Art. I. [needs better citation.]

165. *Id.* at 532-33.

define such parameters within cyber warfare. Perhaps, however, the United States has not prioritized this issue because of the Stuxnet Affair.[166]

One possible way to replicate the Council of Europe model is for the UN to pass an additional resolution qualifying the definition of aggression to include more than just an armed attack. For example, the crime of aggression could also refer to the use of cyber tactics by one state, or a non-state actor or group proven to be sponsored by a state, against the cyber infrastructure, critical infrastructure, or otherwise the population of another state. Such a change in the definition would be broad enough to capture a state's actions against both another state and non-state actors. It would also be broad enough to capture most technologically foreseeable cyber actions a state could employ in the near future. On the other hand, it is unlikely such a measure could pass the UN Security Council because of Russia and China's veto power.[167] And while this measure would help address the growing threat of state-sponsored cyber aggression, it does not

166. Glennon, *supra*, note 54 at 23-24.

167. Both Russia and China would likely see such a resolution as an attack on their right to self-defense. And, even if such a measurement were to pass the General Assembly, it is unlikely that the Security Council would ever support its enforcement in practice. *See, e.g.*, Richard Clarke, Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (2012).

address the threat posed by non-state actors are not directly proven to be sponsored by another state.[168]

2 War crime?

The international legal definition of a war crime has evolved over the years from a series of conventions. War crime laws are mostly focused on how a military interacts with civilian populations and how it treats prisoners of war.[169] But cyber-attacks, especially industrial-level ones like the Stuxnet worm, can potentially impact large populations such that an international humanitarian crisis is triggered. In such a case, international law should apply to those who conducted the attack and allow for prosecution.

Cyber-attacks that target critical infrastructure and populations should be considered the same as a conventional attack with the same targets. An industrial level computer virus, for

168. Changing the norms of war to reflect changes in technology is vitally important to all states in the international system, but the UN only has the power, theoretically, to enforce international law at the state level. And because of the complexities of the international system (i.e., both Russia and the United States using such tactics, but being geopolitically opposed to one another), things are only likely to change when a big state such as the U.S. becomes a victim of a cyber-attack like the one in Estonia. *See* James Andrew Lewis, "Compelling Opponents to Our Will: The Role of Cyber Warfare in Ukraine," in *Cyber War in Perspective: Russian Aggression Against Ukraine*, Kenneth Geers, ed. (NATO, 2015).

169. *See generally* International Committee of the Red Cross, Comite International Geneve, https://www.icrc.org/en/war-and-law/treaties-customary-law/geneva-conventions.

example, could be used to poison the water treatment systems of a major city. In November, 2011, not long after the discovery of Stuxnet, the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) reported that they discovered a foreign cyber-attack against the computer control systems of a water utility plant in Illinois. The virus caused one of the water pumps to burn out, thus affecting the water supply to certain segments of a community.[170] When checking the log-in information in the Supervisory Control and Data Acquisition (SCADA) system, the FBI found that the virus came from a Russian IP address.[171] More than likely, this was a private venture rather than a state sponsored. It is unlikely that Russia would have found the reward of attacking the United States directly in such a manner worth the risk of detection.[172] This reality only opens greater possibilities – if a potential adversary wishes to create a real public health crisis, a water control system is an ideal target. Water is the cornerstone to any critical

170. Although the DHS and FBI were unwilling to disclose which specific water utility was affected by the virus, and Stuxnet was not the virus that infected the system, the broader implications of the attack are clear. See Mark Clayton, "Cyberattack on Illinois water utility may confirm Stuxnet warnings," THE CHRISTIAN SCIENCE MONITOR, Nov. 18, 2011.

171. *Id.*

172. Russia engages in commerce with the United States, and although they can be considered, at worst, geostrategic adversaries, an attack on American critical infrastructure could actually hurt them in terms of commercial gain and international trade. Furthermore, if exposed, it could stand to ruin what little soft power they have within the international system. States will engage in conflict if and only if it advances their narrow interests. See Joseph Nye, "Redefining the National Interest," 78 FOREIGN AFFAIRS 22 (1999)

infrastructure because everyone needs water and most operations require water in at least small quantities.

The DHS tried to downplay the attack, stating that "there is no credible corroborated data that indicates a risk to critical infrastructure entities or a threat to public safety." Experts in the private sector, however, believed this assessment was flawed because of the result—an unknown foreign entity had attacked a part of the U.S. critical infrastructure.[173] Luckily, this cyber incident did not cause any injury, illness, or death. But a similar and successful attack on a large population center such as New York is not unforeseeable given this similar, but smaller-scale attack. If hundreds of thousands of people become sick because of a cyber-attack against a water-treatment facility, would this not be similar to an armed attack against a civilian population?[174] Because of these devastating possibilities, additional language should be adopted into the Geneva Conventions that would recognize cyber-attacks against civilian populations or against critical infrastructure

173. Matthew J. Schwartz, "Next DIY Stuxnet Attack Should Worry Utilities," INFORMATION WEEK SECURITY, (Nov. 22, 2011), http://www.informationweek.com/security/management/next-diy-stuxnet-attack-should-worry-uti/232200029.

174. For cases in which military officials were prosecuted for harming civilian populations, *see, e.g.*, Yamashita v. Styer, 317 U.S. 1 (1946); Prosecutor v. Tadić, Int'l Crim. Tribunal for the Former Yugoslavia App'l Chamber, Case No. IT-94-1-AR72, 35 I.L.M. 32 (1996); Prosecutor v. Jean Paul Akayesu, Int'l Crim. Tribunal for Rwanda, ICTR-96-4 (1998).

that could result in loss of civilian lives as a war crime which can be prosecuted to the same effect as war crimes conducted by more conventional means.

Luckily, scholars around the world have begun efforts within international bodies to address the potential humanitarian crises posed by cyber warfare. In the United Nations, efforts are underway to identify potential victims of a humanitarian crisis and explain why enhancing cyber security at a multi-national level is an important first step in combatting the threats of state-sponsored and all other types of cyber warfare.[175] Likewise, the International Red Cross is concerned with the protection of civilians in both the public and private spheres because of the threats of cyber warfare and has begun dialogues in regards to updating existing laws to reflect technological changes.[176] Once laws are updated to reflect technology, the international system can begin making new ways to enforce them.

---

175. United Nations Office for the Coordination of Humanitarian Affairs, "Humanitarianism in the Age of Cyber Warfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies," OCHA POLICY AND STUDIES SERIES (2014).

176. Cordula Droege, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians," 94 INT'L R. OF THE RED CROSS 533 (2012).

## B Establish special courts and tribunals to prosecute cybercrimes by state actors

The International Criminal Court (ICC), established by the Rome Statute, is potentially the best institution in which international cybercrimes can be prosecuted.[177] Within the ICC, a special prosecution group should be established to prosecute such crimes, whether the crimes are by state actors or non-state actors.[178] While the framework within the Rome Statute is sufficient to prosecute such crimes, there are two vital elements necessary for success: American support of the ICC and a shift in the legal framework of how cybercrimes are understood.[179]

The ICC needs a new international legal framework that addresses cyber warfare, making it even more important for bodies such as the UN to re-define terms such as 'act of aggression.'[180] Not only will this help protect state and non-state victims, but also infrastructural victims of the international system. For example, port authorities in the Straits of Malacca, the Panama Canal, and the Suez Canal may be the direct victims of a cyber-attack, but because these places are

177. 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 (2010).

178. *See id.*

179. *Id.* at 63.

180. *See* Martin N. Schmitt, "Computer Network Attach and the Use of Force in International Law: Thoughts on a Normative Framework," 37 COLUM. J. TRANSNAT'L L. 885, 894 (1999).

strategic points of international commerce, spillover effects from these attacks can reach consumers across the globe, potentially sparking an economic crisis that could devastate local economies.[181]

For enforcement purposes, however, it is important that the ICC receives the support of the United States. As the world's military leader and, the election of Donald Trump notwithstanding, the generally-accepted leader of the Western World, the United States must support the efforts within the international system to address cyber-crimes.[182] Without American support, the ICC lacks a great deal of power to enforce international laws in general, not just laws on cyber-crimes.

The ICC eliminates the need for *ad hoc* tribunals such as the International Tribunal for the Former Yugoslavia (ICTY). Instead, it would allow cyber-crimes to be prosecuted like other war crimes would be. A heightened *mens rea* standard of full intent would not be necessary. Instead, the ICC would require lower standards of *dolus eventualis* and recklessness.[183] These standards target individual actors, but given past international criminal prosecutions that hold commanding

181. *Id.* at 896.

182. *See* Ophardt, *supra*, note 74.

183. *Dolus eventualis* is met when the perpetrator objectively foresees his acts as being harmful or causing injury or death. Recklessness sounds more in negligence, but is still an acceptable standard for war crimes in the ICC. *See* Dan Saxon, "Violations of International Humanitarian Law by Non-State Actors during Cyberwarfare: Challenges for Investigations and Prosecutions," 21 J. CONFLICT SECURITY L. 555 (2016).

officers responsible for the acts of their subordinates, it is possible that the framework of the ICC and the standards applicable in war crime cases would allow both state and non-state actors to be prosecuted and brought to justice.[184] But given the distrust of international institutions in general, brought by the alarming rise of national populists movements worldwide, it is not foreseeable that the ICC will find the institutional help it needs in order to make these prosecutions possible.

## Concluding Remarks

Cybercrimes are on the rise. The legal community has an important responsibility to begin understanding who commits cybercrimes, who the possible victims are, and what the parameters, implications, and possibilities are when these crimes are committed. To more effectively understand the 'Sound of Silence,' we must understand the different motivating factors behind cybercrimes. There are several motivating factors, among them financial gain, revenge, petty fun, and larger political purposes such as regime change, winning hearts and minds, and diversionary war.

The case studies in this paper pointed to several larger truths about cybercrimes and cyberwarfare. The Stuxnet Affair showed that the most powerful states are willing to engage in cyber warfare. The Russia hack of Estonia showed that states in decline will use cyber warfare for

184. *See id. See also Yamashita; Tadić*.

petty revenge and to prove its own strength. The DPRK hack of Sony was a possible display of diversionary warfare, implying the weakness of Kim Jeong-eun's regime. The DNC hack demonstrates the changing nature of political pains and the ease at which a foreign state can interfere, ensuring their preferred candidate's victory. The Dyn attack exposed weaknesses in privately-held digital infrastructure on which the state itself is dependent. Anonymous and Operation Tunisia showcased the millennial generation's technological savviness and how they use that skill as a medium of political change. The Ashley Madison data breach showed that it takes a sex scandal for people to care about digital data breaches. And the Fappening proves that morality need not be a consideration for a hacker's motivations.

Domestically, we can develop a new understanding of cybercrimes by developing new laws and establishing special courts dedicated to combatting them. As cybercrimes become more prolific, prosecutions must become more aggressive. Congress should firstly consider protecting the American consumer against cybercrimes and then consider how new laws and special courts can be used to protect the country's critical infrastructure, such that a cybercrime can only have a small impact on the entire population.

Within the international system, it is necessary to begin the daunting task of re-writing criminal statutes to re-define several concepts, such as 'act of aggression.' This is necessary because digital crimes were unforeseeable when old treaties defining war crimes were enacted.

This is a new age, and our laws must be updated to reflect technological change. Technology is not necessarily an enemy, but when allowed to operate unchecked technology is dangerous.

The responsibility to change the world for the better and protect the world against cybercrimes falls largely on the millennial generation—a generation that has been viciously maligned as spoiled, entitled, lazy, and irresponsible.[185] It is undoubtedly a daunting task. But as the new guard comes into positions of power and influence, the 'Sound of Silence' will likely become just a bit louder.

185. *See, e.g.*, Ben Shapiro, "7 Reasons Millennials Are the Worst Generation," BREITBART (Feb. 3, 2015), http://www.breitbart.com/big-government/2015/02/03/7-reasons-millennials-are-the-worst-generation/.