Why the Law of Armed Conflict (LOAC) Must Be Expanded to Cover Vital Civilian Data

Colonel Beth D. Graboritz
Lieutenant Colonel James W. Morford
Major Kelley M. Truax

> I assess we are seeing what we term *corrosive threats*, in which malicious cyber actors weaponize personal information, steal intellectual property, and mount influence campaigns. Such measures have had and will have strategic effects on our nation and allies.[1]
>
> *- General Paul M. Nakasone, 2019*

INTRODUCTION

In June 2017, during Ukraine's multi-year undeclared war with Russia, the NotPetya worm hit Ukraine as part of a "scorched-earth testing ground for Russian cyberwar tactics."[2] Between 2015 and 2016, Kremlin-backed hackers known as Sandworm focused on Ukrainian government organizations and companies. In the NotPetya cyber-attack against Ukraine, this worm spread automatically, rapidly, and indiscriminately throughout thousands of computers worldwide, crippling multinational companies, including maritime shipping giant Maersk, pharmaceutical giant Merck, food producer Mondelēz International, and even Russia's state-owned oil company, Rosneft. NotPetya is unlike other malware to date because its goal was purely destructive. It mimicked ransomware but was, in reality, more sinister since there was no amount of ransom that could be paid to decrypt a system's data because no decryption key even existed. Damages associated with the 2017 NotPetya attack exceeded $10 billion. While there was no loss of life, former U.S. Department of Homeland Security advisor Tom Bossert equated NotPetya's destructiveness to "using a nuclear bomb to achieve a small tactical victory."[3]

Colonel Beth D. Graboritz recently began serving as the Deputy Director, for the National Security Agency Command, Control, Communications and Cyber Systems Directorate. Previously, she was the Commander, 65th Air Base Group, with four squadrons of 750 personnel located at Lajes Field, Portugal and Morón Air Base, Spain, and served as the Installation Commander for US Forces at Lajes Field, fulfilling the duties of the Commander, US Forces Azores in accordance with US and Portuguese bilateral agreements. Colonel Graboritz received her commission upon graduation from Embry-Riddle Aeronautical University with a Bachelor of Science degree in Aviation Computer Science. She has served in a variety of base-level, command and staff assignments. Additionally, she has deployed several times in support of Operations SOUTHERN WATCH, IRAQI and ENDURING FREEDOM.

Cyber-attacked data was vital to both Ukraine and private companies; ultimately, the attack led to dire second- and third-order consequences to international commerce. NotPetya is a prime example of collateral damage to civilian data through cyberspace operations (CO), where national borders have no meaning, and the scale of destruction is intolerable. Yet, vital civilian data is not generally considered a Civilian Object (capitalized to differentiate it from the more general sense) under the Law of Armed Conflict (LOAC), the international law that governs conduct during armed conflicts. Currently, LOAC defines a Civilian Object as all things that do not fall within the definition of a military objective, with examples that only encompass the physical, brick and mortar domain such as civilian housing, schools, and churches. Thus, data is not afforded the protections of Civilian Objects.

Not surprisingly, data characterization and whether data manipulation, disruption, and destruction constitute an attack is one of many contentious topics now being examined by cyber law experts. Why? Because this is where adversaries conduct CO: in the gray zone between war and peace, where LOAC is murky or inapplicable, and where terms like "Civilian Object" and "cyber-attack" are unclear or incomplete and often esoteric, leaving a wide gap for interpretation and debate. The U.S. Department of Defense (DoD) must advocate for, and the Joint Staff adopt, an updated definition that protects vital civilian data as a Civilian Object, and Congress should incorporate this as national policy, and urge its adoption into international law, and hence be governed by the LOAC.

Understanding Current International Cyber Law

Better understanding of the current environment and its challenges requires us to examine existing international law governing data characterization and its application in LOAC. One definitive reference detailing how international law applies to the cyber domain

Lieutenant Colonel James W. Morford is the Deputy Director for Communications and Information (A6) at 7th Air Force. He and his team are responsible for planning, upgrading and maintaining communications and information systems on behalf of the Korean theater's air component. During exercise and contingency, they provide full situational awareness on AFFOR systems' status, capabilities, and any issues, as well as support and guidance to field units on the restoration of C4 systems after outages. He received his undergraduate degree from the University of Arizona, graduate degree from American Military University, Charles Town WV, and graduated Intelligence Officer School at Goodfellow AFB, TX. His operational assignments include tours at Dyess AFB, Texas, Osan AB, Republic of Korea, the Pentagon, Charleston AFB, and Headquarters United States Transportation Command at Scott AFB, with five deployments supporting Operations IRAQI FREEDOM, ENDURING FREEDOM, and INHERENT RESOLVE.

in armed conflict is the *Tallinn Manual 2.0* (hereafter "Tallinn Manual"), as published in 2017. Edited by 19 international law experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence, the Tallinn Manual includes 154 rules governing CO, with extensive commentary on each rule.[4]

Rule 92 in the Tallinn Manual describes a cyber-attack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or *damage or destruction to objects* [emphasis added]."[5] To fully understand whether a CO is, in fact, an attack and thus subject to the LOAC, the scope of the term "Object" is important. Rule 100 in the Tallinn Manual addresses civilian Objects and military objectives, with the definition of Object being derived from the International Committee of the Red Cross (ICRC) Additional Protocols 1987 Commentary (protocols over and above the Geneva Convention of 1949).[6] The English text uses *objects* which means "something placed before the eyes, or presented to the sight or other sense, an individual thing seen, or perceived, or that may be seen or perceived; a material thing." The French text uses *biens*, which means "chose tangible, susceptible *d'appropriation*." So the word in both English and French means something that is "visible and tangible."[7] Further, Article 52 of Additional Protocol I defines a military objective as "those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage," and a Civilian Object as "all objects which are not military objectives."[8] Thus, what we deem as Civilian Objects cannot be cyber-attacked.[9]

The international law experts who collaborated on the Tallinn Manual agreed cyber infrastructure such as computers, computer networks, and other tangible components are considered Objects, but not Data. They also

Major Kelley M. Truax is the Deputy Chief, Strategy and Policy Analysis Division, under the Command, Control, Communications and Cyber Systems Directorate (J6) for U.S. Transportation Command, located at Scott AFB, IL. Her division is responsible for preparing enterprise-level guidance and audits for on-premise and cloud service acquisition, transition, and management in sup-port of combatant command global operations, ensuring the availability of U.S. Transportation Command's global cyber domain, supporting 39,000 users and 77 command and control systems. She received her commission upon graduation from Embry-Riddle Aeronautical University with a Bachelor of Science degree in Computer Science, and later attended Western International University where she obtained a Master of Science in Information Systems Engineering. She has served in a variety of base-level, Forward Operating Agency, Major Command, Combatant Command, and Joint assignments, with a deployment supporting Operations ENDURING FREEDOM, IRAQI FREEDOM and NEW DAWN.

agreed that Object, properly defined, should exclude data because data is neither visible nor tangible.[10] As such, data cannot be characterized as either a civilian or military Object, meaning an attack on data cannot normally be characterized as a cyber-attack; nor can data be afforded the protections of a Civilian Object in armed conflict. Thus, data manipulation, disruption, and destruction are also typically exempt from the LOAC. Yet a minority of experts dissented, arguing that the majority opinion did not consider the severity of consequences if data is manipulated. The minority also believed "essential" civilian data, such as tax records and social security data, should be included in the definition of Civilian Objects for the purposes of LOAC protections.[11]

The majority did note that a CO targeting data may qualify as an attack if it "...foreseeably results in the injury or death of individuals or damage or destruction of physical objects, those individuals or objects constitute the 'object of attack,' and the operation, therefore, qualifies as an attack."[12] This occurred in 2009 when Stuxnet worked its way inside Iran's Natanz uranium enrichment facility,[13] taking control of 1,000 uranium enriching centrifuges, manipulating data so as to cause the centrifuges to spin at varying speeds and ultimately self-destruct, without displaying abnormal parameters to control center operators. Iran was forced to decommission about 20 percent of its centrifuges during the months-long cyber-attack.[14] Stuxnet was the most sophisticated virus or worm yet, and unlike any that came before, masking its corruption with espionage-level stealth, showing the world the destruction CO can wreak in the physical domain.

Current US Law and Policy Applicable to CO

Shifting to domestic law and policy, the US adheres to international law regarding the conduct of CO and uses it as the basis for domestic laws and policies, but also recognizes the complexities and inconsistencies within

the cyber environment. DoD authority to conduct military CO is governed by statute. For example, Title 10 U.S. Code authorizes the DoD to conduct military CO in response to malicious cyber activity.[15] Fiscal Year 2012 (FY12) National Defense Authorization Act (NDAA), Section 954 states, "Congress affirms DoD has the capability, and upon the direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies, and interests."[16] FY13 NDAA directed U.S. Cyber Command (USCYBERCOM) to protect the networks and critical infrastructure of the US, both offensively and defensively,[17] and the FY17 NDAA elevated USCYBERCOM to a Combatant Command underscoring the importance of this task.[18]

Based on Congress' direction to conduct CO, DoD formulated policies to govern the conduct of CO and manage associated risks. "Targeting" under Joint Publication 3-60 is defined as "an entity (person, place, or thing) considered for possible engagement or action to alter or neutralize the function it performs for the adversary," without explicitly including data as an entity.[19] When reviewing targets for legal sufficiency, military staff judge advocates consider laws of war, U.S. Code, rules of engagement, commander's guidance, and other limiting factors. They also carefully consider risks to noncombatants, i.e., civilians and Civilian Objects. Because cyber law and cyber-attack capabilities continually evolve, the US must frequently revise policies governing CO.

Understanding the Characterization of Cyber Espionage and Intelligence Collection

Data is characterized differently depending on whether it pertains to cyber espionage and intelligence collection. International law as applied to espionage is murky, and legal scholars differ as to what is legal, depending upon the purposes of espionage, but all generally agree that it *may* be legal. A contradiction exists inside US law, with the NDAA 2019 modifying Title 10 U.S. Code (Armed Forces) § 130g (renumbered § 394) to "[The Secretary of Defense shall] conduct, military cyber activities or operations in cyberspace, including clandestine military activities or operations in cyberspace, to defend the US and its allies, including in response to malicious cyber activity carried out against the United States or a United States person by a foreign power." Further, Title 50 U.S. Code (War and National Defense) Chapter 36 (Foreign Intelligence Surveillance) § 1802 allows the President to authorize foreign intelligence surveillance against foreign powers via electronic surveillance, provided there is no substantial likelihood of collection where a U.S. Person is a party.[20] At the same time, Title 18 U.S. Code (Crimes and Criminal Procedures), Chapter 37, in some detail defines a wide variety of espionage-like acts as illegal. Doubtless, most foreign powers have a similar legal dichotomy; as an example, China has both the Counter-Espionage Law of 2014[21] and the National Intelligence Law of 2017.[22]

Controversy exists as to cyber espionage, which can reasonably be defined as the "exercise of state power within the bounds of another state,"[23] no doubt breaking the second state's espionage laws, and thereby implicating sovereignty issues. The Tallinn Manual suggests "although peacetime cyber espionage by states does not *per se* violate international law, the *method* by which it is carried out might do so [emphasis added]."[24] For example, the experts' majority

opinion in the Tallinn Manual was that a cyber-attack on another State's infrastructure clearly violated sovereignty if it created damage (even unintended), yet opinion differed as to implants, or malware, that caused no particular damage.[25] But manipulating or damaging targeted vital data during cyber espionage, as Object is now defined, is wholly unprotected under LOAC.

An increasingly interconnected, or networked, globe will only muddy the waters further. Network infrastructure is mostly owned and operated by nominally civilian institutions, yet law and reality complicate the matter from a military operations standpoint. Huawei, China's telecommunications giant, for example, for years has been installing networking hardware in countries worldwide, and is a leader in global 5G development and deployment. Nominally a private corporation,[26] the CEO, Ren Zhengfei, is a prior Information Technology officer in China's Peoples' Liberation Army with close government ties.[27] An editorial report by Dr. Murray Tanner in *Lawfare Blog* notes that China's 2017 National Intelligence Law places an affirmative burden on all Chinese peoples and entities to provide "access, cooperation, or support for Beijing's intelligence-gathering activities."[28] And many laws are so broad they cover a wide range of eventualities. No great leap is required, then, to see that Huawei not only is *obligated* but *likely* to forward information of major intelligence value to the Chinese government whenever possible. From a CO perspective, is the legal status of civilian data residing on Huawei equipment outside of China to be classified as a Civilian Object and hence LOAC-protected, or a military Object, and thus fair game for cyber-attack?

In the US, no state-owned communications enterprises exist. Dr. Tanner contrasts China's National Intelligence Law with the U.S. Executive Order 12333 and its "detailed definitions, procedures, limitations and prohibitions regarding a number of intelligence activities, including government collection, retention, and dissemination of information on US persons and corporations."[29] That said, the Foreign Intelligence Surveillance Act compels private carriers, when requested by the Attorney General, to "furnish all information, facilities, or technical assistance necessary to accomplish the electronic surveillance [against foreign powers, outlined above] in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier is providing its customers."[30]

Why the Current Definition of Object is Inadequate

National interests wholly unprotected by LOAC already have been compromised by the CO destruction or manipulation of vital civilian data that is not currently considered an Object. In 2007, the decision by Estonia to relocate a World War II memorial from the center of its capital, Tallinn, to a military cemetery outside the city, ignited tensions between ethnic Russians and Estonians, which were further enflamed by false Russian reports. Within days of the decision, Estonia experienced weeks of major denial of service, impairing banking, media outlets, and government institutions. Access to ATMs and online banking was crippled, as were government employee communications,[31] thereby demonstrating the ease whereby CO can manipulate access to data to exploit tensions, and create disturbances and instability, even in a NATO

country like Estonia, in efforts to extort political outcomes. Military reprisal by NATO was avoided by acting below the level of armed conflict; despite the crippling damage wrought, this was not even classified as a cyber-attack.

On December 23, 2015, 225,000 Ukrainians were denied power for hours after a cyber-attack took down part of Ukraine's power grid. Three electricity distribution companies reported being unable to remotely restore power from the control room computers, which required workers to switch to manual controls and travel to 30 substations to restore power.[32] Almost a year to the day, Ukraine experienced a similar cyber-attack against an electric transmission station causing an hour-long outage. The chilling difference of the later attack was its autonomous nature of producing mass power outages, displaying the most evolved and adaptable grid-sabotaging malware seen yet, thereby threatening critical infrastructure and power grids worldwide, including the US.[33]

These two examples illustrate a growing category of CO designed to sabotage critical civilian infrastructure by altering data that is unprotected under LOAC. As the Tallinn Manual points out, the real-world effects of these CO could be deemed as cyber-attacks given their physical impact. Expanding or clarifying the definition of Object to include civilian data not only would help legitimize a proportional response by the victim; it also would disincentivize the targeting of that civilian data in the first place.

There also are examples of adversary CO not manipulating or destroying the targeted data. In January 2015, the second-largest health insurer in the U.S. was targeted, reportedly exposing extremely sensitive data for as many as 80 million current and former customers and employees, including social security numbers, birth dates, and addresses.[34] Post-attack analysis of the Anthem cyber-attack supported the conclusion that this was a practice run for the OPM breach that followed within months, both tracing back to China.[35]

The largest US compromise of sensitive personal information was disclosed in April 2015, with the hack commencing as early as November 2013. The personal information of some 21.5 million current and former government employees and job applicants was stolen,[36] as were security clearance forms and digital images of government employee fingerprints.[37] The far-reaching extent of this breach not only impacts past and current employees and job applicants, but also, all others listed on the security clearance forms, such as spouses, parents, siblings, and college roommates. This breach poses US national security risks that may haunt generations to come. US government costs of credit monitoring services may eventually top $1 billion,[38] and some of that stolen data has surfaced in subsequent financial fraud cases.[39]

As these two examples show, the repercussions are directly or indirectly tied to national security and should not be ignored. Expanding the LOAC's reach with a more inclusive definition of Object is overdue. This no doubt will not always dissuade an adversary from deciding to launch attack, but surely international law should characterize such attacks as illegal.

Moreover, victim States would be justified in retaliating, and calling upon partner States to also retaliate, sanction, censor, etc. The LOAC, properly expanded, should give an adversary pause before attacking civilian data of another country. It's worth highlighting here other responses to such attacks, such as Sony, refusing to be cyber-bullied, responding to North Korea's CO to block the release of a movie satirizing Kim Jong-un by publishing the movie online,[40] and Israel's May 2019 response against a Hamas cyber group with a kinetic strike on its building.[41]

The Case for a Broader Definition of an Object

Confidentiality, integrity, and availability of vital civilian data are key to U.S. national interests, both from economic and political perspectives. Industries have risen and fallen based on advantages gained or lost by proprietary and intellectual property, which, like civilian data, is not classified as an Object or protected by LOAC. Compromise of this type of data often falls within the realm of corporate espionage. Objects as now defined in the Tallinn Manual, simply lags behind the rapidly changing uses and misuses of cyberspace worldwide. For example, what used to be gold, silver, silk, and spices as primary bartered wares has given way to electronic banknotes and cryptocurrencies, all still accepted as forms of payment but, by the above definitions, not real or tangible, yet dramatically impacting our global economy.

Dr. Robert G. Papp, the CIA's former director of the Center for Cyber Intelligence, urged a cyber treaty, a treaty that would ban nations from using cyber weapons in the virtual domain, to help govern these issues for the international community, akin to the 1967 Outer Space Treaty or the 1959 Antarctic Treaty.[42] Substituting the word cyber into those treaties unfortunately oversimplifies the challenge here, but these frameworks are models that could help. Any cyber treaty effort should aim to create a common framework from which all responsible parties can create "expectations and develop a set of principles, rules and procedures, and norms about how states behave with respect to an entire domain."[43] Creating a common baseline is crucial. Without that, it is hard to imagine any incentives or rewards for honoring a treaty, or ways to identify expectations, or workable enforcement consequences for violators.[44]

The US, by adopting a national policy that defines civilian data as an ICRC Civilian Object, not only takes a high ground in cyberspace; it will also reassure allies and neutral powers that, even in peacetime, CO will abide by LOAC concepts of *military necessity, proportionality, and distinction*. The US pledged in the 2018 National Cyber Strategy, to "promote a framework of responsible state behavior in cyberspace built upon international law, adherence to voluntary non-binding norms of responsible state behavior that apply during peacetime."[45] More broadly defining Object to include vital civilian data will enable U.S. planners to categorize it more effectively as either a military or Civilian Object and treat it accordingly. This clarity should benefit all States. The US should also advocate for the incorporation of these changes to LOAC and other international laws in pursuit of universal, responsible state behavior in cyberspace. Simultaneously, the Joint Staff should revisit "target" as defined in Joint Publication 3-60 so as to include data as a targetable entity if it meets the criteria of a military objective, and DoD

should submit a legislative proposal for the National Defense Authorization Act for 2020 to identify, classify, and legally define data as an Object.

CONCLUSION

More inclusively defining Object would allow for appropriate LOAC protections for vital civilian data targeted in a cyber-attack. This alone may not prevent another Sandworm from launching NotPetya and destroying vital civilian data, but it would provide State and organizational victims a far more robust legal standing to respond directly or seek other indirect actions. An adversary knowing of this legal protection is more likely deterred than one that is considering a cyber-attack that international law arguably sanctions. Cyber-attack victims deserve the right to strike back proportionately, take legal action, and/or seek international support, including reparations for the damage caused by the cyber-attack. Redefining Object to include vital civilian data is one of many keys that will help resolve the myriad challenges international and domestic law and policies face in addressing CO in armed conflict. With or without a more inclusive definition, any nation can strike back in self-defense, or pursue appropriate actions when other international law violations occur, such as violation of sovereignty. Expanding the definition of Object to protect vital civilian data so that it can be LOAC-protected, with accompanying broader definitions adopted by DoD, the Joint Staff, and Congress, will put much needed teeth in deterrence that is missing today.

DISCLAIMER

Opinions expressed here are solely those of the authors and do not represent the official policies or endorsements, either ex¬pressed or implied, of the DoD, USCYBERCOM, or any U.S. Government agency.

ACKNOWLEDGMENT

The authors are grateful for the contributions to the research presented here by U.S. Navy Commander Peter Pascucci, now serving as Deputy Staff Judge Advocate for U.S. Special Operations Command; U.S. Army Colonel Gary Corn, now serving as the Staff Judge Advocate for U.S. Cyber Command; and Mr. Bryan Bird, now serving as the Cyber and National Security Law Attorney for U.S. Transportation Command.

NOTES

1. U.S. Senate Committee on Armed Services, *Hearing to Review Testimony on United States Special Operations Command and United States Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2020 and the Future Years Defense Program*, 116th Congress, February 14, 2019 (statement of General Paul M. Nakasone, Commander, United States Cyber Command).
2. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired: Security,* August 22, 2018, accessed May 9, 2019, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
3. Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (Doubleday, 2019), 17-18, 197-8.
4. Michael N. Schmitt and Liis Vihul, eds., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Op-erations* (Cambridge, UK: Cambridge University Press, 2017), p.i. Positions expressed in the Tallinn Manual are based on interpretations of International Law by the experts in their personal capacity and do not reflect the official position of any particular nation or organization.
5. Ibid., 415.
6. Ibid., 437.
7. International Committee of the Red Cross (ICRC) Additional Protocols 1987 Commentary (1987), Art. 47, 2007-2008.
8. Ibid., 435.
9. Ibid., 434.
10. Ibid., 437.
11. Ibid., 437.
12. Ibid., 416.
13. Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired: Security,* November 3, 2014, accessed May 10, 2019, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.
14. Gordon Corera, "What Made the World's First Cyber-Weapon So Destructive?" *BBC: iWonder,* accessed May 10, 2019, http://www.bbc.co.uk/guides/zq9jmnb.
15. U.S. Code Title 10, § 130g.
16. National Defense Authorization Act of Fiscal Year 2012, § 954.
17. National Defense Authorization Act of Fiscal Year 2013.
18. National Defense Authorization Act of Fiscal Year 2017.
19. Joint Chiefs of Staff, *Joint Targeting*, Joint Publication 3-60 (Washington, DC: US Joint Chiefs of Staff, Janu-ary 31, 2013), I-1.
20. As defined in Exec. Order No. 12333.
21. China Law Translate, "Counter-Espionage Law of the People's Republic of China," *China Law Translate*, No-vember 1, 2014, accessed May 16, 2019, https://www.chinalawtranslate.com/anti-espionage/?lang=en.
22. Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," *Lawfare*, July 20, 2017, accessed May 9, 2019, https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.
23. Craig Forcese, "Pragmatism and Principle: Intelligence Agencies and International Law," *Virginia Law Review*, July 9, 2016. Accessed May 11, 2019. http://www.virginialawreview.org/volumes/content/pragmatism-and-principle-intelligence-agencies-and-international-law.
24. Tallinn Manual 2.0, 168.
25. Ibid., 173.
26. In their article for Columbia Law School, "Beyond Ownership: State Capitalism and the Chinese Firm," the authors Milhaupt and Zheng note, "Functionally, [state-owned enterprises] and large [privately-owned enterprises] in China share many similarities in the areas commonly thought to distinguish state-owned firms from privately owned firms: market access, receipt of state subsidies, proximity to state power, and execution of the government's policy objectives." https://www.law.columbia.edu/node/5344/beyond-ownership-state-capitalism-and-chinese-firm-curtis-j-milhaupt-and-wentong-zheng.
27. "The Company that Spooked the World," *Economist*, August 4, 2012, accessed May 8, 2019, https://www.economist.com/briefing/2012/08/04/the-company-that-spooked-the-world.
28. Tanner, "Beijing's New National Intelligence Law: From Defense to Offense."

NOTES

29. Ibid.
30. U.S. Code Title 50, §1802.
31. Damien McGuinness, "How a Cyber Attack Transformed Estonia," *BBC News: Europe,* April 27, 2017, ac-cessed May 10, 2019, https://www.bbc.com/news/39655415.
32. Chris Vallance, "Ukraine Cyber-Attacks 'Could Happen to UK,'" *BBC News: Technology,* February 29, 2016, accessed May 10, 2019, https://www.bbc.com/news/technology-35686493.
33. Andy Greenberg, "'Crash Override': The Malware that Took Down a Power Grid," *Wired: Security,* June 12, 2017, accessed June 10, 2019, https://www.wired.com/story/crash-override-malware/.
34. Kim Zetter, "Health Insurer Anthem is Hacked, Exposing Millions of Patients' Data," *Wired: Security,* February 5, 2015, accessed May 12, 2019, https://www.wired.com/2015/02/breach-insurer-exposes-sensitive-data-millions-patients/.
35. Brendan I. Koerner, "Inside the Cyberattack that Shocked the US Government," *Wired: Security,* October 23, 2016, accessed May 11, 2019, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.
36. Evan Perez, "FBI Arrests Chinese National Connected to Malware Used in OPM Data Breach," CNN: Justice, August 24, 2017, accessed May 11, 2019, https://www.cnn.com/2017/08/24/politics/fbi-arrests-chinese-national-in-opm-data-breach/index.html.
37. Brendan I. Koerner, "Inside the Cyberattack that Shocked the US Government," *Wired: Security,* October 23, 2016, accessed May 11, 2019, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.
38. Josh Fruhlinger, "The OPM Hack Explained: Bad Security Practices Meet China's Captain America" *CSO,* No-vember 6, 2018, accessed May 12, 2019, https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-prac-tices-meet-chinas-captain-america.html.
39. Derek Hawkins, "The Cybersecurity 202: 'A Wake Up Call.' OPEM Data Stolen Years Ago Surfacing Now in Finan-cial Fraud Case," *The Washington Post: Cybersecurity 202 Newsletter,* June 20, 2018, accessed May 11, 2019, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/06/20/the-cybersecurity-202-a-wake-up-call-opm-data-stolen-years-ago-surfacing-now-in-financial-fraud-case/5b2924ca1b326b3967989b66/?utm_ter-m=.4ea7357ae96d.
40. Michael Cieply and Brooks Barnes, "Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm," *The New York Times,* December 30, 2014, accessed May10, 2019, https://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html?module=inline.
41. Shannon Vavra, "It Was 'Inevitable' That Bombs Would Fall in Response to a Cyberattack," *Cyberscoop: Government,* May 6, 2019, accessed May 7, 2019, https://www.cyberscoop.com/hamas-cyberattack-israel-air-strikes/.
42. James Carden, "Time to Pursue an International Cyber Treaty?" *The Nation,* April 30, 2019.
43. Ronald Deibert, "Tracking the Emerging Arms Race in Cyberspace," *Bulletin of the Atomic Scientists* 67, (Janu-ary-February 2011): 1-8.
44. P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know®* (New York: Oxford University Press, 2014), 185-193.
45. Donald J. Trump, *National Cyber Strategy of the United States of America* (Washington, DC: The White House, September 2018), 20.