

REPORT DOCUMENTATION PAGE					Form Approved OMB No. 0704-0188	
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</p>						
1. REPORT DATE (DD-MM-YYYY) 05/28/2019		2. REPORT TYPE Master's of Operational Studies			3. DATES COVERED (From - To) JUN 2018 - JUN 2019	
4. TITLE AND SUBTITLE Unconventional Cyber Warfare: Creating a Cyber Resistance in the Private Sector				5a. CONTRACT NUMBER N/A		
				5b. GRANT NUMBER N/A		
				5c. PROGRAM ELEMENT NUMBER N/A		
6. AUTHOR(S) Rice, Howard G., Major U.S. Army				5d. PROJECT NUMBER N/A		
				5e. TASK NUMBER N/A		
				5f. WORK UNIT NUMBER N/A		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) USMC School of Advanced Warfighting Marine Corps University 2044South Street Quantico, VA 22134				8. PERFORMING ORGANIZATION REPORT NUMBER N/A		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S) Dr. Brandon Valeriano		
				11. SPONSOR/MONITOR'S REPORT NUMBER(S) N/A		
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited.						
13. SUPPLEMENTARY NOTES						
14. ABSTRACT Non-state actors independently, or as state actor proxies, search for vulnerabilities in the American network enterprise and they found it in 80% unhardened private sector cyber networks responsible for DoD and DHS critical infrastructure. The private sector should adopt an unconventional warfare approach to create a Cyber Resistance as a means of network defense which requires preparation of the environment to limit an adversary's opportunities, active deployment of friendly cyber capabilities, and a transition to external partners to regain network integrity.						
15. SUBJECT TERMS Cyberwarfare; Unconventional; Private Sector; Resistance Capability						
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON	
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC School of Advanced Warfighting	
Unclass	Unclass	Unclass	UU	17	19b. TELEPHONE NUMBER (Include area code) (703) 432-5420 (Admin Office)	

*United States Marine Corps
School of Advanced Warfighting
Marine Corps University
3070 Moreell Avenue
Marine Corps Combat Development Command
Quantico, VA 22134*

FUTURE WAR PAPER

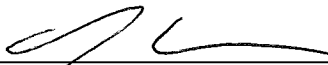
Unconventional Cyber Warfare: Creating a Cyber Resistance in the Private Sector

**SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF OPERATIONAL STUDIES**

Author: Major Howard G. Rice

AY 2018-19

Mentor: Dr. Brandon Valeriano, Marine Corps University Bren Chair of Armed Politics

Approved: 

Date: 5-29-2019

TABLE OF CONTENTS

DISCLAIMER.....	iii
INTRODUCTION.....	1
PRIVATE SECTOR NETWORK VULNERABILITY.....	1
CYBER PROTECTION AND MITIGATION.....	2
ADVERSARY CAPABILITY AND INTENT.....	2
METHODS OF NETWORK INFILTRATION AND EXPLOITATION.....	4
IRREGULAR AND UNCONVENTIONAL WARFARE RELEVANCY.....	5
LEGALITY OF A CYBER RESISTANCE.....	7
ELEMENTS OF A RESISTANCE.....	7
UNCONVENTIONAL CYBER WARFARE (UCW) CONCEPT.....	9
CONCLUSION.....	12
NOTES.....	13
BIBLIOGRAPHY.....	15

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE SCHOOL OF ADVANCED WARFIGHTING OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT

INTRODUCTION

The character of war continues to evolve as the world becomes increasingly interconnected within the cyber domain. Unfortunately, this creates a greater potential for conflict that produces far fewer casualties than a physical war could produce.¹ The term *warfare* makes discussions regarding the cyber realm muddy, and as senior leaders pursue relevant frameworks to address the impact of this competition below armed conflict within the digital frontier.² Despite the ever-increasing global interconnectivity in the cyber ecosystem, the United States government takes a very detached approach to the private sector or civilian institution (non-federal) cyber networks largely because of current authorities, lack of necessary experts, and the non-kinetic nature of the domain. This is compounded by the failure of the private sector to actively engage and share information. The private sector and civilian institutions find themselves out-matched against a resource-rich nation-state, state-sponsored adversary, or a determined non-state actor who seeks to acquire critical information or disrupt a network.³ The cost to the adversary is minimal, but inversely the cost to the non-federal organization can be catastrophic not just for the integrity of the company, but also for the employees and clients to which the information applies. The private sector should adopt an unconventional warfare approach to create a Cyber Resistance as a means of network defense which requires preparation of the environment to limit an adversary's opportunities, active deployment of friendly cyber capabilities, and a transition to external partners to regain network integrity.

PRIVATE SECTOR NETWORK VULNERABILITY

Network vulnerability begins with the security culture established by the *C-Suite* (Chief Executive Officer, Chief Operating Officer, Chief Finance Officer) or senior company

leadership. In some cases, the leadership attitude is indifferent to cyber incursions because executives believe they are just better left without regulation, and that nothing adverse will ever happen to their organization. Companies regularly absorb financial losses incurred by security breaches rather than reveal vulnerabilities in cybersecurity systems, to protect reputations and shareholder values.⁴ In a 2016 study of several companies on the Dow Jones, after the report of cybercrime stock prices dropped, but the amount was statistically insignificant and they quickly recovered.⁵ What the same study did not assess was the reduction of future investors and the loss of customer confidence post cybercrime public notification. Common-sense observers may conclude that this is an incentive to tighten security to protect investment, but companies see the cost of cybersecurity higher than the losses incurred from cyber theft. In the last ten years, companies like Home Depot, Target, and JP Morgan experienced only slight *blowback* from shareholders and consumers after an announcement of cybercrime.⁶ Federal cybersecurity regulation or tasking, especially in private industry that supports national defense, is perceived as an affront to organizational flexibility or innovation when the responsibility rests with the company or institution.⁷ The theft of the Lockheed Martin F-35 Joint Strike Fighter (JSF) design, which cost the company an undisclosed amount, potentially saved Chinese research and development costs to produce their J-31 fighter, which looks *strikingly* similar.⁸ Although the loss of JSF data may not have helped the Chinese or led them to catch up in innovation, the situation demonstrates that the adversary is targeting the defense industry vulnerabilities. Over the last decade, industrial espionage attacks that compromised the JSF project were executed by both insider attacks and outside hackers of the defense organizations.

CYBER PROTECTION AND MITIGATION

Cyber data, network infrastructure, and hardware have tremendous value to any private sector organization, and one way to protect that value is with cyber insurance, which assures that all is not lost in the event of an attack. Despite comprehensive corporate cyber coverage, insurance companies are exploiting clauses and finding loopholes to not pay. The 2017 *NoPetya* cyber strike affected companies globally and provided insurance companies the ability to cite the common clause within an agreement, but rarely used the war exclusion clause, which protects insurers from cost-related damage from the war. The claim from insurance companies that companies affected was collateral damage from a war-related cyber strike from Russia on Ukraine. Many cyber insurance policies, written with a narrow scope, cover costs related to data loss with credit checks and legal fees, but not hardware.⁹ Traditional insurance as protection for companies is almost a superficial and limited layer in the private sector network defense arsenal against determined adversaries.

ADVERSARY CAPABILITY AND INTENT

States, non-state actors, or select proxy force adversaries actively search for vulnerabilities within the less hardened private sector organizations (health care, financial organizations, academic institutions, the full range of businesses, etc.) to attack, gain a foothold, penetrate, and exploit their interdependent systems. For the adversary the capability investment is minimal, the risk remains foreseeably negligible, and the exploitation highly rewarding. An adversary cyber infiltration and exploitation of a private sector network can exact a tremendous cost to sensitive data, time, money, and prestige. Health care data can be sold for false identity development or to leverage a patient, with a personal health issue, to extort funds similar to the 2018 Singapore

health care data breach of 1.5 million patients.¹⁰ An adversary can exploit financial institutions for financial gain much like the targeted phishing campaign in 2017 when personnel involved with the United States Securities and Exchange Commission (SEC) filings received email exploiting employees to gain advanced knowledge of filings to commit securities fraud.¹¹ For a small fee, an adversary can produce false institutional certifications with illegally acquired academic data or pose as a faculty member to access funds from the organization. Whatever the motivation of the adversary, the private sector would benefit from making itself a harder target to reduce the risk to the organization and the data for which it is responsible. There is no shortage of recent cases in which a foreign government targeted a federal or non-federal organization for malign purposes. North Korea (nK) targeting SONY for releasing *The Interview*, a comedy about a plot to assassinate North Korean leader Kim Jong-un. A proxy group called the Guardians of Peace (GOP) cost SONY 15 million dollars in lost revenue from publishing unreleased movies and subsequently damaging its network with malware.¹²

METHODS OF NETWORK INFILTRATION AND EXPLOITATION

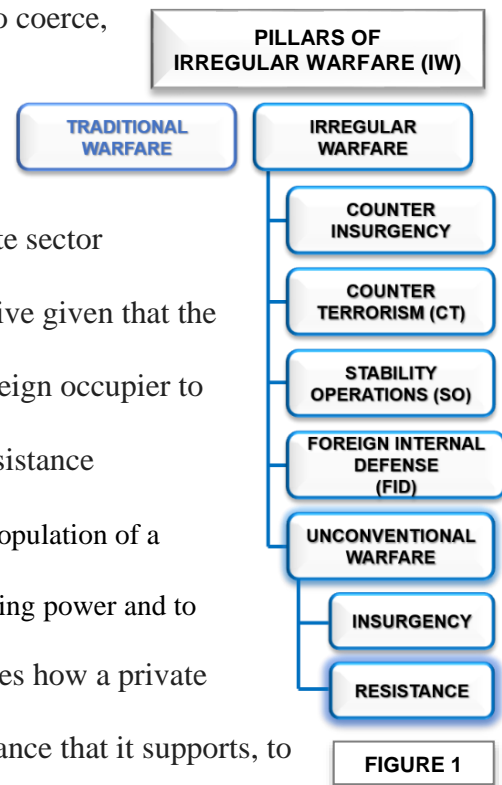
There are two types of people that conduct espionage: insiders and outsiders. Insiders are usually employees with legitimate, or sometimes illegitimate, reasons to access facilities, data, computers, or networks. A common statistic within the cybersecurity realm is that 85% of all corporate espionage is conducted by employees and costs businesses up to \$100 billion a year.¹³ Attorney General Jeff Sessions stated in a November 2018 Justice Department document that Micron Technology Incorporated was the victim of Chinese corporate espionage. Micron controls about 20 to 25 percent of the dynamic random-access memory industry—a technology not possessed by the Chinese until very recently.¹⁴

Places on the world wide web, like the *Dark Web*, are only reachable by using special software, which allows users to remain anonymous and gain access to non-attributional open source tactics, techniques, and procedures for an adversary to infiltrate and exploit a private organization's data.¹⁵ Some regularly employed hacking methods are the *system, remote, wireless, and physical*. A *system hack* assumes the attacker already has access to a low level, a privileged user account on the system. *Remote hacking* is when an adversary attempts to penetrate a system remotely across the network or internet. *Wireless Hacking*, or whacking, is eavesdropping on wireless networks like a radio or Bluetooth interception. Finally, *physical hacking* is when the attacker enters a facility to access the network or sensitive data by social engineering and tricking a person into revealing a password or other valuable information. Additionally, dumpster diving is messy, but a very successful technique for acquiring trade secrets and other valuable information.

IRREGULAR AND UNCONVENTIONAL WARFARE RELEVANCY

The Correlates of War Project at the University of Pennsylvania maintains a compiled data set that captures all conflicts of various types of war for the last 200+ years. Based on that data and its historical trend, the next major conflict that the U.S. will face will be irregular.¹⁶ From the Department of Defense's perspective, cyber warfare is a subset of Operations in the Information Environment (OIE) that shapes both traditional and irregular warfare (IW) within pre or post-crisis or to likewise to influence enduring operations.¹⁷ Cyber operations as a low-cost, high pay off, small footprint capability that can have strategic effects can handily find a home among special operations elements of warfare and the domains that they cross to shape the battlefield. The National Defense Act of 2016 defines Unconventional warfare (UW) as, "*activities*

conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, or guerrilla force in a denied area.”¹⁸ UW as a means of private sector network defense is appealing from a private sector perspective given that the doctrinal purpose of a *resistance movement* is to expel a foreign occupier to regain sovereignty. Under current U.S. Joint Doctrine, a resistance movement is “an organized effort by some portion of the civil population of a country to resist the legally established government or an occupying power and to disrupt civil order and stability.”¹⁹ The definition easily correlates how a private sector company could use the concept of UW and the resistance that it supports, to expel a cyber infiltrator from a network



For the UW concept in private cyberspace network to be effective the leadership and users of that system would require an organizational culture change in planning, preparation, and execution. In the Department of Defense (DoD), UW is a pillar of *irregular warfare*, which is defined as a violent struggle among state and non-state actors for legitimacy and *influence over the relevant population(s)*.²⁰ (FIGURE 1) In the case of a cyber network attack, the relevant population would be the users of that system and their ability to conduct their service on that system. The opposite type of warfare is characterized as *traditional warfare*, which is a violent struggle between *nation-states or coalitions and alliances of nation-states or force*. This form of warfare exists as a military force on the force with both conventional forces and special operations force (SOF) across all domains but does not successfully reflect the state on a non-

state actor, or state on proxy forces. The DoD Joint Publication 3-05.1 Unconventional Warfare manual states that UW are activities conducted to enable a resistance movement or insurgency to coerce, *disrupt*, or overthrow a government or *occupying power* by operating through or with an *underground, auxiliary, and guerilla force* in a *denied area*.²¹

LEGALITY OF CYBER RESISTANCE

The Computer Fraud and Abuse Act (18 U.S. Code § 1030. Fraud and related activity in Connection with Computers) states that anyone accessing a computer without authorization even in active cyber defense (ACD) against hackers is illegal.²² Hack-backs present a challenge since effective forensics and attribution are necessary to ensure that the actual adversary is targeted and not an innocent network user. There are a few ACD techniques that are less invasive that do not violate U.S. code like *honeypots* and *beacons*. These can identify the attacker or embedded links in documents that the intruder can use to gather false information. In 2017, Congress proposed the Active Cyber Defense Certainty Act (ACDCA) that enables the private sector to conduct ACD with FBI oversight and protect companies against prosecution.²³

ELEMENTS OF A RESISTANCE

Not all elements of a military doctrinal or traditional resistance are necessary to develop a cyber network resistance, but understanding the traditional elements ensures the full range of concepts within that framework is successful in regaining network sovereignty after a breach. Indigenous populations that engage in a traditional resistance employ critical elements that increase the probability of success against an occupying force. The *underground* conducts operations in areas that are inaccessible to guerrillas, such as urban areas under the control of adversary forces.

In the cyber domain, the underground operator could be a specialized forensic analyst that facilitates the establishment of pathways to honeypots or beacons to increase the probability of adversary identification.

The *auxiliary* is a portion of the civilian population that provides active clandestine support (logistics, intelligence, communications, etc.) to the guerrilla force or the underground. Within the cyber network, this group would be a trained information technology specialist with access to conduct maintenance, execute relevant cyber threat training, and able to educate the population if necessary. The *public components* negotiate with the nation-state government or occupying power on behalf of resistance movement objectives, and will typically make overt appeals for external support. The C-Suite would fill the role to communicate with the adversary if they make overt contact, or interface with an external support organization like the Department of Homeland Security to facilitate the expulsion of an intruder. A traditional *guerrilla* force organizes to conduct military and paramilitary operations in enemy-held, hostile, or denied territory. In a private sector network, the individual(s) conducting an ACD against the adversary would be the most comparable to the guerilla force or guerilla operator. The capabilities of the auxiliary and guerilla forces could be similar, but a separation of forensics and attribution creates improved delineation of responsibilities. This would increase the depth of friendly capabilities and ensure that one operator is not the single point of failure on the outset of an adversary incursion. The *shadow government* habitually is an element and activity performed by an irregular organization that replaces the governance functions (security, health services, and taxation), and operates in the denied area of an occupied territory. The C-Suite would also act in

this capacity until they reestablish friendly network integrity and likewise perform as a *government-in-exile* displaced from its country [organizational network] of origin.²⁴

UNCONVENTIONAL CYBER WARFARE CONCEPT (UCWC)

A persistent adversary will ultimately penetrate a cyber network with any one or combination of capabilities. With suitable preparation grounded in a UW mentality and resistance framework, an organization can reduce the malign influence, the risk to the system, and set conditions for regaining network integrity.

The first stage is *planning*. One issue with an Unconventional Cyber Warfare approach within the resistance context is the defender must acknowledge occupation is conceivable by the attacking adversary and ultimately lose network integrity. Unfortunately, this realization is necessary to effectively plan with an uninitiated or untrained employee population, but accepting that they are planning to fail by not taking action is not appealing and will quickly be remedied. There are planning stages to progress from a current state to the desired state for the network. Conducting a baseline assessment on a network, employee, and leadership capabilities can be uncomfortable to conduct, but necessary to establish a baseline assessment for insider threat. Leadership messaging, internally and externally, that cybersecurity processes are changing and becoming a focus of the organizational culture can act as a deterrent to insider and outsider adversaries. Building external cyber support relationships to address a crisis response situation is critical since the worst time to make friends is during a crisis. A private sector organization partnering with the National Cybersecurity and Communications Integration Center (NCCIC) from the Department of Homeland Security (DHS) which the Nation's flagship cyber defense,

incident response, and operational integration center creates a layer of defense.²⁵ Since the DHS is responsible for reducing the Nation's risk of systemic cybersecurity and communications challenges, a cyber contact team could provide an assessment to the leadership of the organization on vulnerabilities and establish a partnership for continued integration with the company.

The second stage is *the preparation*. Private sector enterprise training is necessary to establish a starting point for a common understanding of the potential adversaries, internal cyber processes, policies, and employee accountability. Currently, multiple cyber organizations provide training and certification to companies that seek to improve their cyber knowledge and understanding of various adversaries. Private sector companies like Cyber Intelligent Partners (CIP)²⁶ and FireEye²⁷ conduct network assessments, provide planning and facilitate preparation to establish a baseline for network and employee integrity. The private organization should canalize an adversary attack to the network in the designated area that is favorable for the defense. In so doing, the resistor is creating a defense not only in depth but also under conditions that are favorable to the defender to mass capability to isolate or defeat an adversary. Private sector continual assessment on network, employee, and leadership capabilities to identify high-risk employees can mitigate the risk of internal attacks. Conducting organizational rehearsals to certify with senior leadership, and validating network procedures with an external organization like DHS can create confidence in the system and deter adversaries. The organization can develop a BOT (automated application used to perform simple and repetitive tasks that would be time-consuming, mundane, or impossible for a human to perform) capability to defend network at various contact layers to disrupt adversary penetration. Finally, the company can create

pathways and pits (honeypots and beacons) of deceptive data for an adversary to exploit which have no value but provides the intruder a place in the network.

The third stage is the adversary *contact*. This does not have to be physical contact, but identification that there is an indicator of a possible insider or outsider attack. This is where the training of employees pays off in early intervention of a network or coworker behavioral anomaly. The employee is the private sector's first line of resistance to an attack and penetration. Thwarting an adversary intrusion by notifying the Security Division to organize resistance capabilities and messaging to employees and external partners of possible attack are first steps to crisis management.

The fourth stage is adversary *penetration and exploitation* of the network. The adversary will attack to circumvent, co-op, or destroy the primary firewall to establish freedom of network movement and exploit that penetration. Within a traditional foreign occupation, an adversary's objective is to displace the [executive] leadership and force them to act as an element in exile; subsequently, they no longer have control of their nation [network]. Concurrently, through the adversary exploitation of the system, they impose their will on all users of that system whether it is a denial of service or malign employee influence. During the preparation stage, the resistance capabilities to disrupt the adversary exploitation with defending bots are tasked with forcing a path of least resistance to the adversary. The end of that path appears to be the original penetrated network but is a separate mirrored network without valuable data. With the adversary isolated but still attached to the system, the government/leadership in exile can now request support from outside organizations.

The fifth stage is *the transition*. An internal or external network crisis capability that should be trained, exercised, and coordinated in the preparation stage can now assert itself from within the system over the top of the occupying adversary or externally from a supporting effort. Forensics and attribution to determine the origin of the adversary are critical to ensuring that future threats are not only reduced within an attacked system but also prevented throughout the cyber ecosystem.

CONCLUSION

A change in private sector resistance posture creates a deterrence effect for both an internal and external adversary, which allows for preparation of the digital environment in disrupting an adversary's capabilities, and thus increases the prospect of regaining network integrity.

Unfortunately, looking into history does not provide a ready-made plan of action to defend a sovereign network that must maintain global connections while still providing a service to its users and customers. However, the application irregular warfare can stimulate innovation to create depth and engage an adversary from a position of advantage even when the enemy infiltrates a private network. Protection of critical information can mean the difference between victory and defeat on the battlefield, or revenue and cost in the dynamic private sector, but only if it is guarded with effective unconventional planning and preparation to cause the adversary to rethink about swallowing a *jagged pill* by entering a network with a strong resistance to create conflict.

Notes

-
- ¹ “Joint Doctrine Note 1-18 Strategy,” Joint Chiefs of Staff Electronic Library, 25 April 2018, accessed February 1, 2019, <https://www.jcs.mil/Doctrine/Joint-Docctrine-Pubs/Joint-Docctrine-Notes>.
- ² Discussions with Dr. Brandon Valeriano, on 5 March 2019.
- ³ “DHS Cybersecurity Strategy,” Department of Homeland Security, May 17, 2018, 2, accessed December 02, 2019, <https://www.dhs.gov/publication/dhs-cybersecurity-strategy>.
- ⁴ Amitai Etzioni, “The Private Sector: A Reluctant Partner in Cybersecurity,” *Privacy in a Cyber Age*, 2015, 58, doi:10.1057/9781137513960_6.
- ⁵ Amie Jones, “Cybercrime Effects on Stock Prices” (2016). Honors College Theses. 1. <https://digitalcommons.murraystate.edu/honorstheses/1>
- ⁶ Ibid, Jones.
- ⁷ Scott Kannry Levite, and Wyatt Hoffman, “Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance,” Carnegie Endowment for International Peace, accessed May 01, 2019, <https://carnegieendowment.org/2018/11/07/addressing-private-sector-cybersecurity-predicament-indispensable-role-of-insurance-pub-77622>.
- ⁸ Ibid, 59
- ⁹ Adam Satariano and Nicole Perlroth, “Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong,” *The New York Times*, April 15, 2019, accessed May 23, 2019, <https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html?login=google>.
- ¹⁰ Kate O’Flaherty, “Why Cyber-Criminals Are Attacking Healthcare -- And How To Stop Them,” *Forbes*, October 05, 2018, accessed May 01, 2019, <https://www.forbes.com/sites/kateoflahertyuk/2018/10/05/why-cyber-criminals-are-attacking-healthcare-and-how-to-stop-them/#3a031bcd7f69>.
- ¹¹ Steve Miller, “FIN7 Spear Phishing Campaign Targets Personnel Involved in SEC Filings,” 2017, accessed November 02, 2019, www.fireeye.com/blog/threat-research/2017/03/fin7_spear_phishing.html.
- ¹² Gabi Siboni and David Siman-Tov, “Cyberspace Extortion: North Korea versus the United States,” *INSS Insight* No. 646, December 23, 2014.
- ¹³ “Corporate Espionage: The Spy on Your Payroll,” *Forensicon*, May 28, 2014, 1, accessed November 02, 2019, <https://www.forensicon.com/forensics-blotter/corporate-espionage-spy-payroll/>.
- ¹⁴ “PRC State-Owned Company, Taiwan Company, and Three Individuals Charged With Economic Espionage,” The United States Department of Justice, November 09, 2018, accessed December 02, 2019, <https://www.justice.gov/opa/pr/prc-state-owned-company-taiwan-company-and-three-individuals-charged-economic-espionage>.
- ¹⁵ “Dark Web | Definition of Dark Web in English by Oxford Dictionaries,” Oxford Dictionaries | English, 1, https://en.oxforddictionaries.com/definition/dark_web.
- ¹⁶ “About the Correlates of War Project.” Correlates of War. April 05, 2014. Accessed November 02, 2019. <http://www.correlatesofwar.org/>.
- ¹⁷ “Joint Doctrine Library,” Joint Chiefs of Staff, I-5, accessed November 02, 2019, <http://www.jcs.mil/Doctrine/>.
- ¹⁸ Thornberry, “H.R.1735 - 114th Congress (2015-2016): National Defense Authorization Act for Fiscal Year 2016,” Congress.gov, October 22, 2015, Sec.1097, accessed May 20, 2019, <https://www.congress.gov/bill/114th-congress/house-bill/1735>.
- ¹⁹ “Unconventional Warfare Pocket Guide,” 5, U.S. Army Special Operations Command, April 2016.
- ²⁰ “JP-1 Doctrine for the Armed Forces of the United States,” Executive Summary pg. X, accessed November 02, 2019, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf.
- ²¹ “JP 3-05.1 Joint Special Operations Task Force Operations,” 10, accessed December 2, 2018, https://fas.org/irp/doddir/dod/jp3_05_01.pdf.
- ²² “18 U.S. Code § 1030 - Fraud and Related Activity in Connection with Computers.” Legal Information Institute. Accessed February 24, 2019. <https://www.law.cornell.edu/uscode/text/18/1030>.
- ²³ “Text - H.R.4036 - 115th Congress (2017-2018): Active Cyber Defense Certainty Act.” Congress.gov. November 01, 2017. Accessed May 01, 2019. <https://www.congress.gov/bill/115th-congress/house-bill/4036/text>.
- ²⁴ Ibid, 15.

²⁵ "CERT | United States Computer Emergency Readiness Team," US, accessed May 01, 2019, <https://www.us-cert.gov/>.

²⁶ "Cyber Intelligence & Security | USA | Cyber Intelligent Partners," Cyber Intelligence & Security | USA | Cyber Intelligent Partners, 1, accessed December 02, 2019, <https://www.cyberintelligentpartners.com/>.

²⁷ "Network Security and Forensics Solutions," FireEye, 1, accessed December 02, 2019, <https://www.fireeye.com/solutions/nx-network-security-products.html>.

Bibliography

- 18 U.S. Code § 1030 - Fraud and Related Activity in Connection with Computers. Legal Information Institute. Accessed February 24, 2019. <https://www.law.cornell.edu/uscode/text/18/1030>.
- About the Correlates of War Project. Correlates of War. April 05, 2014. Accessed November 02, 2019. <http://www.correlatesofwar.org/>.
- "CERT | United States Computer Emergency Readiness Team." US. Accessed May 23, 2019. <https://www.us-cert.gov/>.
- Corporate Espionage: The Spy on Your Payroll. Forensicon. May 28, 2014. Accessed November 02, 2019. <https://www.forensicon.com/forensics-blotter/corporate-espionage-spy-payroll/>.
- Cyber Intelligence & Security | USA | Cyber Intelligent Partners. Cyber Intelligence & Security | USA | Cyber Intelligent Partners. Accessed December 02, 2019. <https://www.cyberintelligentpartners.com/>.
- DHS Cybersecurity Strategy." Department of Homeland Security. May 17, 2018. Accessed December 02, 2019. <https://www.dhs.gov/publication/dhs-cybersecurity-strategy>.
- "Dark Web | Definition of Dark Web in English by Oxford Dictionaries." Oxford Dictionaries | English. https://en.oxforddictionaries.com/definition/dark_web.
- Etzioni, Amitai. "The Private Sector: A Reluctant Partner in Cybersecurity. Privacy in a Cyber Age, 2015, 93-100. doi:10.1057/9781137513960_6.
- Graves, Tom. Text - H.R.4036 - 115th Congress (2017-2018): Active Cyber Defense Certainty Act. Congress.gov. November 01, 2017. Accessed May 01, 2019. <https://www.congress.gov/bill/115th-congress/house-bill/4036/text>.
- Howard, Michael, Peter Paret, and Rosalie West. Carl Von Clausewitz: On War. Princeton: Princeton University Press, 1984.
- Joint Doctrine Library. Joint Chiefs of Staff. Accessed November 02, 2019. <http://www.jcs.mil/Doctrine/>.
- Jones, Amie. Cybercrime Effects on Stock Prices. Master's thesis, Murry State University, 2016.
- JP 3-05.1 Joint Special Operations Task Force Operations. Accessed December 2, 2019. https://fas.org/irp/doddir/dod/jp3_05_01.pdf.
- Levite, Scott Kannry, and Wyatt Hoffman. "Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance." Carnegie Endowment for International Peace. Accessed May 01, 2019. <https://carnegieendowment.org/2018/11/07/addressing-private-sector-cybersecurity-predicament-indispensable-role-of-insurance-pub-77622>
- Network Security and Forensics Solutions. FireEye. Accessed December 02, 2019. <https://www.fireeye.com/solutions/nx-network-security-products.html>.

O'Flaherty, Kate. "Why Cyber-Criminals Are Attacking Healthcare -- And How To Stop Them." Forbes. October 05, 2018. Accessed May 01, 2019.

<https://www.forbes.com/sites/kateoflahertyuk/2018/10/05/why-cyber-criminals-are-attacking-healthcare-and-how-to-stop-them/#3a031bcd7f69>.

PRC State-Owned Company, Taiwan Company, and Three Individuals Charged With Economic Espionage. The United States Department of Justice. November 09, 2018. Accessed December 02, 2019.

<https://www.justice.gov/opa/pr/prc-state-owned-company-taiwan-company-and-three-individuals-charged-economic-espionage>.

Satariano, Adam, and Nicole Perlroth. "Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong." The New York Times. April 15, 2019. Accessed May 23, 2019.

<https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html?login=google>.

Thornberry. "H.R.1735 - 114th Congress (2015-2016): National Defense Authorization Act for Fiscal Year 2016." Congress.gov. October 22, 2015. Accessed May 1, 2019.

<https://www.congress.gov/bill/114th-congress/house-bill/1735>.