Journal of Strategic Security

Volume 14 | Number 4 Article 5

What is the Role of Cyber Operations in Information Warfare?

Emilio Iasiello
Private Sector, iasiello@aol.com

pp. 72-86

Recommended Citation
Iasiello, Emilio. "What is the Role of Cyber Operations in Information Warfare?." *Journal of Strategic Security* 14, no. 4 (2021) : 72-86.
DOI: https://doi.org/10.5038/1944-0472.14.4.1931
Available at: https://digitalcommons.usf.edu/jss/vol14/iss4/5

What is the Role of Cyber Operations in Information Warfare?

Abstract

Much attention has been focused on the potential consequences of cyber attacks against critical infrastructure and the use of cyber weapons as an asymmetric equalizer. However, as a capability considered to be under the larger umbrella of an information operations (IO)/information warfare (IW) campaign, how significant a weapon is cyber for the strategist in an information environment? As observed in recent IO/IW campaigns targeting U.S. elections in 2016 and 2020, lack of any discernable disruptive cyber attacks may have provided an answer to this, as a cyber power purposefully elected not to implement attacks. Instead, cyber espionage was used, and even at that, played a minor complementary role in the larger effort. This calls into question the efficacy of cyber as an instrument of IO/IW, and the true nature of its role in more strategic soft-power operations. This paper argues that cyber is at best a supportive enabler of campaigns where information is the catalyst to achieve strategic results, reducing cyber attacks as tools best used for signaling, punishment, or implemented in first strike scenarios.

Introduction

During the past few years, the United States has focused on the potential consequences that cyberattacks can inflict against critical infrastructure (CI).[1] These attacks can have far-reaching effects, and the incidents that have transpired against the sector have garnered attention and frequent calls to bolster the country's overall security posture. Cyber espionage campaigns have also proven prolific, garnering news attention based on the target(s), global reach, and the type of information exposed, with the recent 2020 SolarWinds breach underscoring how vulnerabilities in the IT supply chain can lead to detrimental results.[2]

However, cyberattacks are not the only serious threat facing the United States and based on the results of soft-power activities during the 2016 U.S. presidential elections, one must consider if the government's focus on them have not missed seeing the forest for the trees. The 2016 election revealed how ill-prepared the country was to address the soft-power tenets of information warfare (IW), especially those information-enabled campaigns and influence operations that integrated disinformation, misinformation, and propaganda against a civilian population. Here, information and not the ones and zeroes that makeup the digital domain aided Russia in achieving its strategic objectives. That is not to say that cyber operations did not have a function; they did, but only in a supportive, secondary role.

This article reviews the information environment, looks at cyberspace as a warfighting domain, and compares real-life cyberattacks versus cyber espionage as they apply to information warfare campaigns in achieving strategic goals. An examination of real-life cyber activities will reveal that cyberattacks are tactical weapons at best and show that cyber espionage is not only more effective but is also the natural complement to the information activities observed in recent state-driven influence campaigns and disinformation operations.

"Ideas are far more powerful than guns. We don't let our people have guns. Why should we let them have ideas?"
-Joseph Stalin

Information Warfare and the Information Environment

There is no current official U.S. government definition of information warfare (IW). However, the United States has defined information operations (IO) in its Department of Defense (DoD) Joint Publication 3-13, characterizing IO as "the integrated employment, during military operations, of IRCs [information-related capabilities] in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own."[3] Information operations consists of the following core activities: Military deception, electronic warfare, psychological operations, operations security, and computer network operations.[4] While IW and IO seem similar, the key differential lies at the level they are implemented. According to a 2018 report from the non-partisan Congressional Research Service, IW occurs at the strategic level, whereas IO uses information-enabled capabilities to implement the strategy.[5]

The DoD Dictionary of Military and Associated Terms defines the strategic level as "the level of warfare at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic security objectives and guidance, then develops and uses national resources to achieve those objectives."[6] Therefore, for the purposes of this article, information warfare will be defined as the purposeful use and exploitation of the information environment via information-enabled operations with the intent of creating an effect on a target audience. Information-enabled operations, for example influence campaigns, disinformation, misinformation, and propaganda, in this context are those soft power activities that leverage the information environment that includes the cyber domain, as well as more traditional print, radio, and television channels.

What is the Information Environment?

Per DoD Joint Pub 3-13, the information environment:

> is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. This environment consists of three interrelated dimensions which

https://digitalcommons.usf.edu/jss/vol14/iss4/5
DOI: https://doi.org/10.5038/1944-0472.14.4.1931

> continuously interact with individuals, organizations, and systems. These dimensions are the physical, informational, and cognitive.[7]

This definition has value in a public sector sense as well as a military one. Information-related capabilities (IRC) modify the dimensions of a target audience to influence their decision-making process to achieve an intended effect. IRCs are planned, created, and conducted via IO channels once a strategy is place. The global and accessible nature of the information environment makes it difficult to a state to completely control, no matter how authoritarian the regime. Information can create intended effects on a target, a capability that benefits from the facility of its production, alteration, and dissemination, as well as how audiences receive it. Ultimately, reactions to it can run contrary to a state's interests.

Cyberspace as a Warfighting Domain

Much emphasis has been placed on the emergence of cyberspace as a separate domain of warfare and protecting military resources that rely on information networks for a variety of vital operations such as command-and-control, supporting the intelligence cycle, logistics, and weapons technologies, among others.[8] In Joint-Pub 3-12, the DoD defines cyberspace as:

> the global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[9]

Therefore, it is unsurprising that the DoD publicly codified cyberspace as a warfighting domain in 2010, identifying it as a "relevant domain for DoD activities as the naturally occurring domains of land, sea, air, and space."[10]

Indeed, the importance of denying adversaries use of the cyber domain while ensuring its ability to operate freely is a key U.S. military objective. Two executive actions taken by the previous two presidents underscore such importance. In June 2013, a former National Security Agency contractor leaked an alleged copy of Presidential Directive 20 (PDD-20) that detailed United States policies for engaging in offensive cyber

operations against adversaries. PDD-20 defines the types of operations allowed under presidential authority.[11] In 2018, then-president Trump rescinded the PDD in favor of a policy framework that enabled military commanders to have more leeway to conduct cyber operations against adversaries.[12] The result has been much quicker than PDD-20 and yielded operational success, at least according to one White House official in 2019.[13]

Cyber Activity Dominates the News…But at What Cost?

Cyberattacks have garnered attention from the press and a global community drawn to how savvy attackers can exploit a complex interconnected world by using as little as a laptop or desktop computer. Cybercrime continues to proliferate with costs estimated to reach USD 10.5 trillion by 2025.[14] Large scale breaches that have exposed individuals' data such as those suffered by Adobe in 2013 (153 million), Adult Friend Finder in 2016 (412 million), and Equifax in 2017 (147 million) have made attackers near-monolithic.[15] Destructive attacks perpetuate this image. The world suffered under a NotPetya ransomware attack that targeted Ukraine then spread globally.[16]

The potential weaknesses of industrial control systems were revealed in such attacks like the 2015 cyberattack against Ukraine's power grid that shut off the lights for 250,000 users and as recently as the February 2021 compromise of a Florida water treatment facility.[17] Collectively, these and many other incidents have fed, and rightly so, the need for governments to design and implement national-level comprehensive cybersecurity strategies that focus on addressing the mitigation of such attacks. However, according to the Center for Strategic & International Studies, only 78 countries had a national strategy guiding national, coordinated deterrents and responses to cyber threats, and several of these were grossly outdated.[18]

Much to the detriment of senior U.S. government leadership, the focus on cyberattacks has overshadowed the more readily implemented soft power IOIW tenets that only require content, a platform, and an audience to execute. This is disconcerting considering that these types of activities have proven instrumental in helping achieve the destabilization of countries with the hope of attaining the strategic objectives of replacing

https://digitalcommons.usf.edu/jss/vol14/iss4/5
DOI: https://doi.org/10.5038/1944-0472.14.4.1931

their governments. Clearly, the outcomes of the "Color Revolutions" revealed how the construction, controlling, and effective dissemination of information can have substantial influence in shaping the outcome of geopolitical events.[19] Similarly, the 2016 U.S. presidential influence campaign revealed how tactical IO operations supported the larger strategic objectives of the Russian IW campaign to instill no confidence in the public about its government and further stoke the flames of social division.

Information-enabled activities played a critical role in this effort, disseminating propaganda, and distributing disinformation or misinformation leading up to and increasing after the election. These were not attacks designed to disrupt, degrade, or destroy information systems and networks. On the contrary, the successful implementation of these activities required the technical architecture and infrastructure of the cyber domain to remain in perfect working order so that they quickly reached as far as they could and targeted the right consumers.

When reviewing the 2016 influence campaign, Russia pushed highly-charged political and social themes via social media platforms to reach audiences directly and without censor. What's more, when the messages succeeded in incensing their targets, effected recipients passed on these messages, thereby perpetuating the disinformation or misinformation cycle.[20] A 2017 Stanford University study revealed that fake news stories about presidential candidates were shared approximately 37.6 million times in 2016.[21] The tactical results were clear and immediate: By taking advantage of an already polarized environment, Russia inundated audiences with contradictory reports without an immediate or reliable means to help discern truth from half-truth impacted human cognition, thereby heightening confusion and further raising tensions.

Furthermore, Russia complemented its IW campaign with other soft power activities such as propaganda to serve as a platform for Moscow's messaging and cyber espionage to both steal information and instill uncertainty in the minds of the public.[22] The multi-pronged IO assault led Russia to achieve its broader strategic IW goals:

1. To sow discontent in the U.S. public.

2. Undermine public faith in the U.S. election process; and 3) exploit the free press and uncensored nature how the United States produced, disseminated, and consumed news and information.

Perhaps more compelling is that Russia successfully influenced their target audiences by affecting their behavior in the way that was most beneficial to Moscow's interests, in this case, the ongoing U.S. public discontent and distrust of its government.

Cyberattacks Do not Support IW Campaigns

What is even more notable about the 2016 U.S. election, and often overlooked, is the lack of destructive or disruptive cyberattacks executed by Russian agents, or more likely, via cut-outs or proxies working at Moscow's behest. There are several examples of where Russia through these actors has executed such attacks, particularly during times of geopolitical tension. Why this is important is that it stands in marked contrast to Russia's 2008 military intervention in the crisis in South Ossetia, Georgia. At that time, disruptive attacks targeted the networks of major media outlets, in addition to those of the government and financial institutions.[23] As the goal was to reclaim South Ossetia, Russia did not need a soft-power offensive as much as a direct one designed to achieve tactical objectives like impacting the government's ability to disseminate information. In this instance cyberattacks—not cyber espionage—were the appropriate support element. The incidents against Estonia and Ukraine also exemplify this type of behavior.[24]

But clearly Moscow did not take the same approach against its biggest adversary likely because any substantial or blatantly overt cyberattack would have immediately risked response, engagement, potential escalation, and the possible introduction of kinetic weaponry. Even more so, cyberattacks would not have been cohesive with the larger IW strategy that Russia put into place, because by their nature, cyberattacks are tactical in their execution. Like any weapon they have a specific purpose with a narrow window of opportunity to leverage surprise for operational success. As such, cyberattacks are at their best when they achieve limited and immediate results such as state signaling, meting out punishment, or proactive mitigation strikes to disrupt impending or future activity. They

https://digitalcommons.usf.edu/jss/vol14/iss4/5
DOI: https://doi.org/10.5038/1944-0472.14.4.1931

are not as successful supporting more refined operations that require a defter touch.

- Signaling. The 2007 DDoS attacks launched against Estonia for the removal of a Soviet statue exemplifies the use of a cyberattack as a signaling agent. Conducted by Russian nationalists and sympathizers, the attacks impeded people's abilities to access the websites of banks and newspapers and disrupted the Government's ability to communicate with its citizens.[25] At the peak of the crisis, Estonians could not access or use their bank cards and mobile-phone networks.[26] Though Estonia did not wilt under the digital onslaught, the attackers made their point. In 2009, North Korea allegedly conducted DDoS attacks against public and private sector South Korean and U.S. organizations.[27] The attacks occurred one-month after United Nations-imposed economic sanctions and coincided with North Kora's short-range ballistic missile launch, suggesting that North Korea used the attacks to signal its discontent over the new measures.
- Punishment and Retaliation. In 2019, the United States allegedly conducted an unspecified cyberattack against Russia's power grid, as well as against Russia's Internet Research Agency in response to Russian penetration of U.S. nuclear facility and activities during the 2016 presidential elections, respectively.[28] The Operation Ababil DDoS attacks against the U.S. financial sector can also be viewed through the prism of retaliation. In that case, a previously unknown hacktivist group assumed credit for the attacks, claiming they were perpetrated in response to the anti-Islam film "Innocence of Muslims," which sparked worldwide controversy.[29] In 2016, the U.S. Department of Justice later indicted seven Iranians that worked for a company that performed work for the Iranian government.[30] In the face of U.S. sanctions imposed at the time against Iran for its nuclear program, and coming on the heels of the suspected United States-led Stuxnet attack against an enrichment facility, one can infer that Operation Ababil was a proportional retaliation for these perceived transgressions.
- Proactive Strike. In a shift from defensive to offensive cyber operations, in 2019 the U.S. Cyber Command (CYBERCOM) embraced persistent engagement, a proactive strategy to take the fight to the adversary prior to them being able to conduct

> cyberattacks against the United States. Per press reports, CYBERCOM executed operations against Iranian and Russian networks months leading up to the 2020 presidential election, temporarily paralyzing some and neutralizing ransomware tools.[31] In its ongoing conflict with Ukraine, Russia allegedly launched a cyberattack to impact Ukraine's power grid in 2015, causing a temporary loss of power. A 2016 instance impacted another Ukrainian substation. These cyberattacks sought to destabilize Ukraine as it sought to distance itself from Russia, as they came in the wake of a political revolution with Russian annexation of Crimea.[32]

The above incidents combined with other destructive cyberattacks, for example, the 2017 WannaCry ransomware attack and the 2012 attack against Saudi Aramco, clearly reveal the serious and severe damage that cyberattacks can inflict.[33] However, it is also clear that these attacks did not achieve long-lasting effects. Granted, while that may not have been the intent, the fact remains that the attacks occurred, effects realized, and victims eventually mitigated and recovered from them.

Cyber Espionage Incidents Facilitate IW Campaigns

A review of some of the more notable cyber espionage activities reveals that the softer cousin of a cyberattack has infinitely more value in supporting strategic IW campaigns. This is largely since cyber espionage is more focused on manipulation and exploitation than disruption or destruction. Cyber espionage requires fastidious patience on the part of operators who execute surreptitious activities, clandestinely gain unauthorized access into targets, and maintain a presence on targeted systems and networks. Once inside, operators can perform a variety of activities that support a nation state's long-term strategic goals, typically in the form surveillance, monitoring a target's activities, and the theft of sensitive data, intellectual property, or proprietary information.

However, as evidenced in the Russian 2016 IW campaign, cyber espionage is not limited to intelligence collection but can also serve a supporting role in a larger multi-faceted operation. According to the 2017 U.S. Intelligence Community Assessment *Assessing Russian Activities and Intentions in Recent US Elections*, cyber operations ranged from stealing and leaking

https://digitalcommons.usf.edu/jss/vol14/iss4/5
DOI: https://doi.org/10.5038/1944-0472.14.4.1931

information to further fueling social discontent and instilling uncertainty over the integrity of the election.[34] Since IW's intent is to generate a specific effect on a target audience, these information-enabled activities take advantage of the information environment for the purposes of creating a psychological effect. Putting this into context makes one wonder what other cyber espionage activities have occurred and contributed to similar strategic IW campaigns.

The following more prolific cyber espionage examples are indicative of campaigns with possible broader implications than the events themselves. What's more, they complement a state's future IW campaign planning by exploiting the information environment in a way that values data over the networks on which they rest or traverse. These activities include purposeful leaking, compromising the integrity of the data, crafting propaganda or disinformation narratives, and instilling distrust by publicly exposing sensitive material.

- SolarWinds. The December 2020 disclosure of the SolarWinds breach exposed another exploitation of a company that ultimately provided access into several high-profile U.S. government organizations (to include but not limited to Departments of Commerce, Defense, Energy, Justice, State, and Treasury, among others) as well as most of the Fortune 500 companies.[35] Per reporting, an estimated 18,000 organizations were impacted although not all of these experienced a follow-on intrusion.[36] This extensive breach represents one of the most complex and sophisticated cyber intrusions to date based on the victims and the types of activities the attackers engaged in once they gained access. For example, the attackers compromised the email accounts of top Treasury officials, and in the case of one computer security company, the attackers stole proprietary penetration tools used to test customer networks.[37]

  While officials continue to investigate the compromise, its purpose is consistent with a nation state's cyber exploitation of network accesses, and in some cases, information theft as well. However, the U.S. government immediately acknowledged the severity of this intrusion, and an emergency meeting with the National Security Council invoked a directive to create a special group to manage the

government's response to the breach.[38] As of February 2021, the U.S. government has not responded to the attackers, believed to be either Russian state actors or those working on its behest. The new U.S. president immediately called the breach a top priority, and highlighted deficiencies in U.S. cybersecurity.[39] As one online computer periodical stated, the SolarWinds "hack is a wakeup call for taking cybersecurity action."[40]

- Equifax. In March 2017, Equifax, one of the major credit reporting agencies that assesses the financial stability of most people in the United States, suffered a breach exposing the sensitive personal and financial data of 147 million people.[41]Among the types of data stolen included names, addresses, dates of birth, Social Security numbers, drivers' licenses numbers, and credit cards, among others.[42] As opposed to the Office of Personnel Management (OPM) breach in 2015, the Equifax had all the hallmarks of being perpetrated by cyber criminals, given the financial focus of the credit reporting agency. However, the U.S. government ultimately attributed the activity to the Chinese government in a 2017 indictment by the Department of Justice.[43] Due to the importance of such an agency to the fiscal health of citizens who need it to establish a record of financial responsibility for everything ranging from seeking employment to purchasing homes, loss of such data can impose serious national security consequences as well. The 2017 U.S. *National Security Strategy* acknowledged that hostile cyber activity such as that observed in the Equifax compromise could potentially have cascading effects across multiple sectors of the economy.[44] Unsurprisingly, this incident shows the far-reaching consequences of a breach of this magnitude.
- OPM Breach. In June 2015, the U.S. Office of Personnel Management (OPM) disclosed that it had twice suffered a breach impacting its employees in 2014, putting their SF-86 forms, and therefore their sensitive personal data at risk, as well as security clearance information.[45] The breach potentially put at risk information resident in other databases such as Department of Defense service records and Department of State passport records.[46] Approximately 22.1 million individuals were impacted by the breach, which many believe was perpetrated by the Chinese government, and for which a Chinese national was indicted in 2017 for being linked to malware used in the OPM compromise.[47] The

https://digitalcommons.usf.edu/jss/vol14/iss4/5
DOI: https://doi.org/10.5038/1944-0472.14.4.1931

breach is an intelligence collection boon, as the types of data stolen would certainly support other espionage activities to include but not limited to continued human and cyber intelligence targeting. However, one 2018 report revealed that unknown actors used the stolen data to commit fraud suggesting that cyber criminals and not a nation state committed the breach.[48] Regardless how the individuals obtained the data to commit the fraud, based on the type of target (a U.S. government organization holding sensitive personal security clearance data), there is understandable skepticism that this was the effort of criminals. Unsurprisingly, the U.S. government's failure to secure some of the most sensitive information of its employees raised the question of what the government was doing to bolster cybersecurity. This has become a cause-effect reflex that is par for the course when large breaches garner the attention of the international community.

Conclusion

The threat of a catastrophic cyberattack and the potentially severe damage it can cause is a real concern. However, an information attack is the bigger threat and one that has already taken place. Future attackers are likely studying what happened so as to refine their operations and streamline their processes for future targeting. Looking from a lessons-learned perspective on the IW activities that occurred in the months leading up to and after the 2016 U.S. presidential elections, the soft power elements of IW proved instrumental in exploiting the social and political tensions festering in the country. What's more is that the Russian IW campaign took advantage of what has long been the United States' core strength—freedom to produce and disseminate uncensored content. The 2016 IW campaign revealed that the soft nature of cyber espionage naturally lends itself to supporting information-enabled activities involved in conducting larger IW strategic efforts precisely because they seek to exploit information rather than destroy or disrupt systems that process and distribute it. A cyberattack accompanying the 2016 campaign would have undoubtedly worked contrary to the pollical objectives Russia sought, uniting the U.S populace rather than dividing it.

Cybersecurity challenges continually test the private and public sectors, and the U.S. government through the Department of Homeland Security

and the National Institute of Technology and Standards provides the private sector with guidance and recommendations to counter cyber threats. Industry-led Information Sharing and Analytic Centers complement these efforts by increasing and facilitating the information-sharing process. However, while the U.S. government has developed and enacted national strategies addressing cybersecurity,[49] there is no equivalent for the soft power elements—namely propaganda and disinformation—of IW performing the same public service. Solely focusing on the ones-and-zeroes glaringly fails to address the information aspects of the larger information security ecosystem.

More than mid-way through 2021, the U.S. government continues to show its reliance on tech companies and news media outlets fostering increased collaboration in an effort to counter such threats on social media platforms. However, given a recent survey revealing that most Americans believe that politics is what drives these organizations to censor their platforms, this is a mistake.[50] Advising these companies on what to censor and block is akin to the activities of our adversaries that view such information control as necessary to regime survival. Worse, these activities do not unify an already divided United States but exacerbate already existing tensions. The U.S. government should heed this clarion bell as it heads down the dangerous path of becoming exactly like the authoritarian regimes that it denounces, which may ultimately be Russia's greatest IW objective of all.

Endnotes

1 "Cyberattack" references the purposeful denial, disruption, degradation, and/or destruction of information systems or the information resident on these systems. In this context, cyberattacks are not strategic as much as tactically achieving a specific end-result such as debilitating a target.

2 "Cyber espionage" references the purposeful exploitation of information systems for the purposes of gaining illicit access to sensitive and/or confidential data for theft or manipulation. In this context, cyber espionage activities are more nuanced and therefore complement other information-enabled activities (e.g., propaganda, disinformation, influence operations, etc.) that support more strategic objectives.

3 Department of Defense, *Information Operations*, JP 3-13 (Washington, DC: Joint Chiefs of Staff, 2014), ix, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

4 Catherine A. Theohary, *Defense Primer: Information Operations*, CRS Report No. IF 10771 (Washington, DC: Congressional Research Service, 2020), 1, https://crsreports.congress.gov/product/pdf/IF/IF10537/7.

https://digitalcommons.usf.edu/jss/vol14/iss4/5
DOI: https://doi.org/10.5038/1944-0472.14.4.1931

[5] Catherine A. Theohary, *Information Warfare: Issues for Congress*, CRS Report No. R45142 (Washington, DC: Congressional Research Service, 2018), 2, https://crsreports.congress.gov/product/pdf/R/R45142.
[6] Department of Defense, *DoD Dictionary of Military and Associated Terms*, (Washington, DC: Joint Chiefs of Staff, 2021), 203, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.
[7] Department of Defense, *Information Operations*.
[8] Department of Defense, *Quadrennial Defense Review Report*, (Washington, DC: Department of Defense, 2010), 37-38, https://archive.defense.gov/qdr/QDR%20as%20of%2029JAN10%201600.pdf.
[9] Department of Defense, *Information Operations*.
[10] Department of Defense, *Quadrennial Defense Review Report*, 37.
[11] White House, *Fact Sheet on Presidential Policy Directive 20*, (Washington, DC: White House, 2013), https://fas.org/irp/offdocs/ppd/ppd-20-fs.pdf.
[12] Sean Lyngaas, "PPD-20 Elimination Opens Arguments Over How U.S. Should Conduct Offensive Hacking Operations," *CyberScoop*, August 16, 2018, https://www.cyberscoop.com/ppd-20-eliminated-cyber-war-donald-trump-mike-rounds/.
[13] Lyngaas, "PPD-20 Success Has Yielded 'Operational Success,' Federal CISO Says."
[14] Steve Morgan, "Cybercrime to Cost the World $10.5 Trillion Annually By 2025," *Cybercrime Magazine*, November 13, 2020, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.
[15] Dan Swinhoe, "The 15 Biggest Data Breaches of the 21st Century," *CSO Online*, January 8, 2021, https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.
[16] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History, *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
[17] SANS, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, March 8, 2016, https:// media.kasperskycontenthub.com/wp-content/uploads/sites/58/2016/12/21181126/E-ISAC_SANS_Ukraine_DUC_5.pdf; Department of Homeland Security, *Compromise of a U.S. Water Facility*, Alert AA21-042A (Washington, DC: Department of Homeland Security, 2021), https://us-cert.cisa.gov/ncas/alerts/aa21-042a.
[18] CSIS, *Global Cyber Strategies Index*, https://www.csis.org/programs/strategic-technologies-program/cybersecurity-and-governance/global-cyber-strategies-index.
[19] Emilio Iasiello, "Russia's Improved Information Operations: From Georgia to Crimea," *Parameters* 47, No.2 (Summer 2017), 59, https://www.almendron.com/tribuna/wp-content/uploads/2018/11/8-iasiello-russiasimprovedinformationoperations.pdf.
[20] Scott Shane, "Some of the Popular Images and Themes Posted on Social Media," *The New York Times,* December 17, 2018, https://www.nytimes.com/2018/12/17/us/russian-social-media-posts.html.
[21] Hunt Allcott and Matthew Gentzkow, "Social Media and Fake News in the 2016 Election," *Journal of Economic Perspectives* Volume 31, Number 2(Spring 2017), 212, https://web.stanford.edu/~gentzkow/research/fakenews.pdf.
[22] Intelligence Community Assessment, "Assessing Russian Activities and Intentions in Recent US Elections," ICA 2017-01D, January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.
[23] Przemysław Roguski, "Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace," *Just Security*, March 6, 2020, https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/.
[24] Ran Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective," in *Proceedings of the 7th European Conference on Information Warfare and Security* (Estonia: CCDCOE, 2008), https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/; Laurens Cerulus, "How Ukraine

Became a Testbed for Cyber Weaponry," *Politico*, February 14, 2019, https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/.

[25] Joshua Davis; 2007; "Hackers Take Down Most Wired Country in Europe;" *Wired*, August 21, 2007. http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

[26] Robert Coalson, "Behind the Estonia Attacks," *Radio Free Europe/Radio Liberty* (blog), March 6, 2009, http://www.rferl.org/content/Behind_The_Estonia_Cyberattacks/1505613.html.

[27] Choe Sang-Hun and John Markoff, "Cyberattack Jam Government and Commercial Websites in U.S. and South Korea," *The New York Times*, July 8, 2009, https://www.nytimes.com/2009/07/09/technology/09cyber.html.

[28] David E. Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," June 15, 2019, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

[29] Ellen Messmer, "DDoS Attacks Against Banks Raise Question: Is this Cyber War?" *Network World*, October 24, 2012, http://www.networkworld.com/news/2012/102412-bank-attacks-cyberwar-263664.html.

[30] Department of Justice, "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," news release, March 24, 2016, https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged.

[31] David E. Sanger and Julian E. Barnes, "U.S. Tried a More Aggressive Cyberstrategy, and the Feared Attacks Never Came," *The New York Times*, November 9, 2020, https://www.nytimes.com/2020/11/09/us/politics/cyberattacks-2020-election.html.

[32] Donghui Park, Julia Summers, and Michael Walstrom, "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks," *The Henry M. Jackson School of International Studies News*, October 11, 2017, https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.

[33] Johnathan Berr, "WannaCry Ransomware Attack Losses Could Reach $4 Billion," *CBS News*, May 16, 2017, https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/; John Leyden, "Hack on Saudi Aramco Hit 30,000 Workstations, Oil Firm Admits," *The Register,* August 29, 2012, https://www.theregister.com/2012/08/29/saudi_aramco_malware_attack_analysis/.

[34] Directorate of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections* (Washington, DC: Directorate of National Intelligence, 2017), ii-iii, www.dni.gov/files/documents/ICA_2017_01.pdf.

[35] Sara Wilson, "SolarWinds Recap: All of the Federal Agencies Caught Up in the Orion Breach," *FedScoop,* December 22, 2020, https://www.fedscoop.com/solarwinds-recap-federal-agencies-caught-orion-breach/; Mia Jankowicz and Charles Davis, "These Big Firms and US Agencies All Use Software from the Company Breached in a Massive Hack Blamed on Russia," *Business Insider,* December 15, 2020, https://www.businessinsider.com/list-of-companies-agencies-at-risk-after-solarwinds-hack-2020-12.

[36] Catalin Cimpanu, "SEC Filings: SolarWinds Says 18,000 Customers Were Impacted by Recent Hack," *ZDNet*, December 14, 2020, https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack/.

[37] Michael Novinson, "Top Treasury Email Accounts Exposed in SolarWinds Hack: Report," *CRN,* December 21, 2020, https://www.crn.com/news/security/top-treasury-email-accounts-exposed-in-solarwinds-hack-report#:~:text=On%20Dec.,wrote%20in%20a%20blog%20Dec; Catalin Cimpanu, "FireEye Releases Tool for Auditing Networks for Techniques Used by SolarWinds Hackers," *ZDNet*, January 19, 2021, www.zdnet.com/article/fireeye-releases-tool-for-auditing-networks-for-techniques-used-by-solarwinds-hackers/.

https://digitalcommons.usf.edu/jss/vol14/iss4/5
DOI: https://doi.org/10.5038/1944-0472.14.4.1931

[38] Justin Katz, "NSC Invokes 2016 Directive to Respond to SolarWinds Hack," *FCW,* December 15, 2020, https://fcw.com/articles/2020/12/15/solarwinds-hack-nsc-ucg.aspx.
[39] Eric Geller, "Biden Aide Calls SolarWinds Top Priority as New Details Emerge," *Politico,* January 4, 2021, https://www.politico.com/newsletters/weekly-cybersecurity/2021/01/04/biden-aide-calls-solarwinds-top-priority-as-new-details-emerge-792539.
[40] Chris Dimitriadis, "SolarWinds Hack Is a Wakeup Call for Taking Cybersecurity Action," *CSO Online,* January 6, 2021, https://www.csoonline.com/article/3602649/solarwinds-hack-is-a-wakeup-call-for-taking-cybersecurity-action.html.
[41] Josh Fruhlinger, "Equifax Data Breach FAQ: What Happened, Who Was Affected, What Was the Impact?" *CSO Online,* February 12, 2020, https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html; Federal Trade Commission, "Equifax Data Breach Settlement," January 2020, https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement.
[42] Josh Fruhlinger, "Equifax Data Breach FAQ: What Happened, Who Was Affected, What Was the Impact?"
[43] Department of Justice, "Chinese Military Personnel Charged with Computer Fraud, Economic Espionage, and Wire Fraud for Hacking into Credit Reporting Agency Equifax," news release, February 10, 2020, https:// www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking#:~:text=In%20total%2C%20the%20attackers%20ran,data%20compilations%20and%20database%20design.
[44] White House, *National Security Strategy of the United States of America* (Washington, DC: White House, 2017), https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.
[45] Office of Personnel Management, "OPM to Notify Employees of Cybersecurity Incident," news release, June 4, 2015, https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/; Evan Perez and Shimon Prokupecz, "First on CNN: U.S. Data Hack May be 4 Times Larger than the Government Originally Said," *CNN*, June 22, 2015, https://edition.cnn.com/2015/06/22/politics/opm-hack-18-milliion/index.html.
[46] Michael Adams, "Why the OPM Hack Is Far Worse Than You Imagine," *Lawfare Blog,* March 11, 2016, https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine.
[47] Ellen Nakashima, "Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say," *The Washington Post,* July 9, 2015, http://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/; Peter Suciu, "Is China Using Hacked OPM Data?" *Clearance Jobs,* April 19, 2019, https://news.clearancejobs.com/2019/04/19/is-china-using-hacked-opm-data/.
[48] "Four Years Later, Data from OPM Breach Used to Commit Fraud," *Cyber Talk*, June 20, 2018, https://www.cybertalk.org/2018/06/20/4-years-later-data-opm-data-breach-used-commit-fraud/.
[49] White House, *National Cyber Strategy of the United States of America*; White House, *International Strategy for Cyberspace* (Washington, DC: White House, 2011), https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
[50] Emily A. Vogels, Andrew Perrin, and Monica Anderson, "Most Americans Think Social Media Sites Censor Political Viewpoints," *Pew Research Center* (blog), August 19, 2020, https://www.pewresearch.org/internet/2020/08/19/most-americans-think-social-media-sites-censor-political-viewpoints/; Glenn Halbrooks, "How Media Censorship Affects the News You See," *ThoughtCo*, July 14, 2020, https://www.thoughtco.com/how-media-censorship-affects-the-news-you-see-2315162.