JOURNAL OF LAW AND CYBER WARFARE

Volume 6 | Summer 2017 | Issue 1

Instegogram: A New Threat and Its Limits for Liability

Jennifer Deutsch & Daniel Garrie*

Social media networks represent the largest, most dynamic risk to organizational security and allocating liability.[1] Recently, a new risk was developed combining digital image steganography and social media into the corporate environment. Last year, researchers demonstrated that "malware hidden in images posted to social media sites can be used for command and control (C2) channels."[2] While neither steganography nor social media are new, it is novel to combine both as a tool for malware distribution.[3] This article considers whether a company can be held liable to a third-party for unknowingly posting an image with embedded malware.

Generally, steganography involves placing a hidden message within a transport medium, in such a way that the casual observer is not aware that a message had been sent. Digital image steganography is the practice of hiding code inside images. While the hidden code slightly alters the original image's appearance, changing its color tone and

* *Jennifer Deutsch* is a consultant for Law & Forensics and is a staff editor for the Journal of Law & Cyber Warfare.
Daniel Garrie is the Editor-in-Chief for the Journal of Law & Cyber Warfare. He is also the Managing Partner of Law and Forensics, a Forensic Neutral for JAMS, and a Partner with ZEK.

[1] *What is Social Media Security*, ZEROFOX, https://www.zerofox.com/social-media-security (last visited Apr 17, 2017).

[2] Amanda Rossseau, Daniel Grant & Hyrum Anderson, *Instegogram: Leveraging Instagram for C2 via Image Steganography*, ENDGAME (2016), https://www.endgame.com/blog/instegogram-leveraging-instagram-c2-image-steganography (last visited Jan 28, 2017).

[3] *Id.*

making it appear more pixilated than a clean version,[4] the difference is subtle and easily goes unnoticed.[5]

Recently, malicious actors have successfully used digital image steganography to conceal the command and control operations required to operate malware.[6] Inherently, steganography with malware C2 channels embedded is an appealing tool to malicious actors because of its stealthiness.[7] Moreover, "malicious actors have leveraged these social media platforms to bolster their existing operations" because the online content is dynamic.[8] Websites constantly update and with each update comes a new opportunity for infiltration.[9]

A new scheme known as "Instegogram" "mirror[s] the utilization of social networks for C2, while exploring the

---

[4] *Id.*

[5] Rene Millman, *Huge Malvertising Campaign Uses Steganography to Hide malware in plain sight*, SC MAGAZINE UK (2016), https://www.scmagazineuk.com/huge-malvertising-campaign-uses-steganography-to-hide-malware-in-plain-sight/article/530879/ (last visited Feb 8, 2017).

[6] Rossseau, *supra* note 2.

[7] Verine Etsebeth, *Malware Attacks: Corporate Responsibility and Liability*, EMERALD GROUP PUBLISHING (2007), http://www.emeraldgrouppublishing.com/learning/management_thinking/articles/pdf/malware.pdf. (last visited Jan 2017).

[8] *Id.*

[9] Kacy Zurkus, *Social media, the gateway for malware*, CSO ONLINE (2016), http://www.csoonline.com/article/3106292/social-networking/social-media-the-gateway-for-malware.html (last visited Jan 17, 2017); *See also* Jai Vijayan, *Attack Uses Image Steganography For Stealthy Malware Ops On Instagram*, DARK READING (2016), http://www.darkreading.com/endpoint/attack-uses-image-steganography-for-stealthy-malware-ops-on-instagram/d/d-id/1327170 (last visited Apr 28, 2017).

feasibility of using steganography on a particular site - Instagram."[10] Under this scheme:

> once the remote system is compromised, encoded images can be posted from the command machine using Instagram's API. The remote system will download the image, decode it, execute the encoded commands, encode the results in another image, and post back to Instagram.[11]

Although Instegrogram was originally created for academic purposes,[12] its potential use as part of a malware attack poses the question of who would be liable for such an attack.

Under the Communications Decency Act (CDA), companies that offer web-hosting services are typically shielded from liability for most content that customers or malicious users place on the websites they host.[13] The CDA grants immunity to providers of interactive computer services from liability arising from content created by others.[14] The protections extend to individuals who operate websites and web forums to which other individuals can

---

[10] Rossseau, *supra* note 2.
[11] *Id.*
[12] *Id.*
[13] 47 U.S.C. § 230 (1998); *See also The Legal Implications of Social Networking: The Basics (Part One)*, INFOLAWGROUP LLP (2015), http://www.infolawgroup.com/2011/06/articles/social-networking/the-legal-implications-of-social-networking-the-basics-part-one/ (last visited Mar 3, 2017).
[14] Melissa Landau Steinman & Mikhia Hawkins, *When Marketing Through Social Media, Legal Risks Can Go Viral Venable*, VENABLE LLP (2010), https://www.venable.com/files/publication/b4f467b9-0666-4b36-b021-351540962d65/presentation/publicationattachment/019f4e5f-d6f8-4eeb-af43-40a4323b9ff1/social_media_white_paper.pdf (last visited Feb 17, 2017).

freely post content.[15] This encompasses almost any online service (*e.g.*, Google, Facebook, Instagram) that publishes information provided by a third-party or information content provider.[16] As such, commerce platforms and employers that provide or enable computer access for multiple users on their computer networks/servers to access the Internet may qualify for immunity.[17] Congress recognized that websites that display third-party content may have an infinite number of users generating an enormous amount of potentially harmful content,[18] and holding website operators liable for that content "would have an obvious chilling effect," in light of the difficulty of screening posts for potential issues.[19]

One crucial exception to CDA immunity is that no protection exists if the website controls the information content.[20] Thus, the CDA provides no immunity to an Internet service provider, like Yahoo, when it, rather than a third party, is the "Information Content Provider."[21] That is, if the service provider is "responsible, in whole or in part, for the creation or development of the offending content,"[22] its actions fall outside the CDA's protections. Consequently, courts have held that a service provider is not immune from

---

[15] *Donato v. Moldow*, 374 N.J.Super. 475, 865 A.2d 711 (N.J. Super. Ct. App. Div. 2005).
[16] *See Id.*; 47 U.S.C. § 230(c)(1) (1998).
[17] *Delfino v. Agilent Techs., Inc.*, 145 Cal. App. 4th 790, 52 Cal. Rptr. 3d 376 (Cal. App. Dep't Super. Ct. 2006); *Miller v. Fed. Express Corp.*, 6 N.E.3d 1006 (Ind. Ct. App. 2014).
[18] *Doe v. Backpage.com, LLC.*, 817 F.3d 12 (1st Cir. 2016).
[19] *Zeran v. America Online, Inc.*, 129 F.3d 327, 331 (4th Cir. 1997).
[20] *Malware Risks and Mitigation Report*, BITS (Jun. 2011), https://www.nist.gov/sites/default/files/documents/itl/BITS-Malware-Report-Jun2011.pdf.
[21] *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC.*, 521 F.3d, 1157, 1164 (9th Cir. 2008).
[22] 47 U.S.C. § 230(f)(3) (1998).

suit where the provider itself creates or helps to develop, rather than merely publishes, the unlawful content.[23] Arguably, sponsored ads, which are the advertiser's content posted by the respective networks, have no effect on immunity. Such features merely reflect choices about what content can appear on the website and in what form, and thus are editorial choices that fall within the purview of traditional publisher functions.[24] Likewise, a company that uses a social media network to create the picture, or develop information, "controls" that information and would not be immune. Even when a company is contractually permitted to advertise on a social network, only the social network remains immune.

Whether the CDA protections extend to damage caused by malware is still largely an open question of law.[25] However, a 2003 Third Circuit case supports its application to malware.[26] In *Green v. America Online*, the court held that a malicious program constituted "information" for purposes of the CDA, even though it was not communicated in the traditional sense.[27] The court concluded that the service provider, AOL, could not be held liable for the victim's computer receiving a signal from their service if it was sent by a third party with no role in the program.[28] Thus, the Court shielded web hosts if their hosted sites are a source of malware without the host's knowledge. Under the Court's

---

[23] *Roomates.com*, 521 F.3d at 1168-69; *See also Anthony v. Yahoo! Inc.*, 421 F.Supp.2d 1257, 1262-63 (N.D. Cal. 2006).
[24] *Reit v. Yelp! Inc.*, 29 Misc.3d 713 (N.Y. Sup. Ct. 2010); *See Obado v. Magedson*, 612 Fed.Appx. 90 (3d Cir. 2015).
[25] BITS, *supra* note 20.
[26] *Green v. America Online*, 318 F.3d 465 (3d. Cir. 2003) (holding that AOL not liable for user-posted virus placed into AOL chatroom).
[27] *Id.*
[28] *Id.*

interpretation in *Green*, a web service company cannot be held liable for third-party malware on a hosted website.

Thus, it is probable that companies would be liable for any third-party damage resulting from an Instegogram attack for which they did know or should have known the digital image was infected. As no statutory immunities exist to shield social media users, a company would be liable for any resulting damage caused by a criminal hacker's embedded C2 infrastructure. But is it even likely that a content creator could have known there was embedded malware? Digital image steganography rests on an employee's ability to notice minute differences in an image,[29] so Instegogram liability would rely on the limitations of the human eye to perceive minute changes in color and light intensity, small distortions that could reasonably go unnoticed.[30]

Of course, terms of service agreements may provide further protections. Among other things, a term of service agreement may allocate responsibility for an Instegogram attack with provisions waiving liability for viruses and any resulting third-party damage. Depending on the language, such a waiver may limit, prevent, or allocate any damages resulting from an Instegogram attack.

The increasing use of social media in the corporate environment poses new avenues for liability. As shown,

---

[29] *See* Rossseau, *supra* note 2 (describing digital image steganography's ability to be invisible to a person, "if Eve intercepts the image in transit, she is oblivious to the fact that the stego image contains any message at all since the image appears to be totally legitimate both digitally and to the human eye.").

[30] Joann Kennedy, *Use Offense to Inform Defense. Find Flaws Before the Bad Guys Do Sans Penetration Testing*, SANS (2004), https://cyber-defense.sans.org/resources/papers/gsec/steganography-corporate-environment-106511.

social media networks are generally immune from the consequences of an Instegogram attack. By contrast, the content creator is left exposed to potential liability for an Instegogram attack.

A Democracy of Users

John P. Dever & Captain James A. Dever*

"Well, Doctor, what have we got – a Republic or a Monarchy?"
"A Republic, if you can keep it."

Response attributed to Dr. Benjamin Franklin when queried as he left Independence Hall on the final day of the Constitutional Convention, September 17, 1787.[1]

INTRODUCTION

This article addresses how a Republic can thrive in a digital world. A number of Americans were first exposed to the Internet in the 1990s. In those years, the noise of Internet dial-up was the sound of progress, and AOL's treasured phrase "You've got mail!" linked users and communities in new and profound ways that only a short time before were the strict purview of science fiction. In 2017, individuals

* *James A. Dever* is an active duty Judge Advocate in the U.S. Army. He previously served at the Cyber Center of Excellence, Fort Gordon, GA. The views expressed in this article are solely those of the author and do not reflect the official policy or position of the United States Army, Department of Defense, or U.S. Government.
John P. Dever Jr. holds a L.L.M. in National Security Law from Georgetown University. He is currently the Leader of AML / Sanctions Program for Wholesale Banking, Wells Fargo. Prior to joining Wells Fargo he was the Finical Crimes Compliance Leader and Global Crisis Management Leader for GE Capital, Americas. Before joining the private sector, he served as an Assistant U.S. Attorney in the Northern District of Illinois and as an Assistant General Counsel in the Federal Bureau of Investigation's National Security Law Branch, Counterterrorism Division. He began his career on active duty in the U.S. Army as a Judge Advocate. He served multiple combat deployments and is the recipient of the Bronze Star and the Purple Heart Medals.
[1] 3 THE RECORDS OF THE FEDERAL CONVENTION OF 1787, 85 (Max Farrand ed. 1911).

navigate their world via digital devices. In a practical sense, analog maps are museum pieces, as many people get from A to B using a variety of smart phone apps. The use of this new technology is pervasive. Even a stop at a red light often entails a driver reaching for her smartphone to view a work text or Facebook news feed. Today's citizen lives an e-existence and therein lies a multitude of possibilities and pitfalls.

The article begins by discussing two of the issues that show both the incredible potential of the internet while simultaneously representing how the internet can also present very real danger, Big Data and the Internet of Things. Citizens must remain cognizant that privacy is constantly at stake in this electronic world. Perhaps not surprisingly, opinions differ regarding how best to protect privacy; although coding it appears to be a fruitful endeavor. As cybersecurity becomes the new arms race between hacker and system, illegitimate versus legitimate user, nations and private entities alike must develop resilient policies to account for a paucity of law. Most importantly, to secure the Republic for the next century, users must prize the responsibilities of citizenship. Democracy flourishes in the marketplace of ideas yet users are increasingly being drawn into digital echo chambers where faction is exorcised while accepted tropes are exalted. Systems and hardware must be better protected against hostile and unintended cyber events, but the ultimate safeguard of a Republic is the well-informed user-citizen.

I. THE FUTURE IS NOW

A. Big Data

Big Data refers to collecting and storing large

amounts of various granular data in real time and using data analytics to reveal insights from the aggregated information.[2] As the second decade of the twenty-first century draws to a close, people are becoming increasingly connected to the Internet in ways that sometimes obfuscate the relationship between human interaction and Big Data. The amount of information contained in Big Data is staggering. Much of the world's stored information today is digital, and existing mathematical terms struggle to quantify it.[3] The types of information that is now digitized include information that once existed in analog format (books, census records, customer information) as well as new kinds of information made possible by modern technologies.[4] In addition, digitization alters the nature of the information itself. "Information that can be digitized can also be collected, searched, quantified, compared, assessed, and endlessly repurposed."[5] This ability to manipulate data

---

[2] Swaroop Poudel, *Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security*, 31 BERKELEY TECH. L.J. 997 (2016); *see also* Charles McLellan, *The Internet of Things and Big Data: Unlocking the Power*, ZDNET (Mar. 2, 2016), http://www.zdnet.com/article/the-internet-of-things-and-big-data-unlocking-the-power.

[3] The largest current recognized number is a yottabyte: a digit with twenty-four zeros. *See* John Foley, *Extreme Big Data; Beyond Zettabytes and Yottabytes*, FORBES (Oct. 9, 2013), http://www.forbes.com/sites/oracle/2013/10/09/extreme-big-data-beyond-zettabytes-and-yottabytes.

[4] President's Council of Advisors on Science and Technology, *Big Data and Privacy: A Technological Perspective* (May 2014), https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf [http://perma.cc/87G9-HSCP] (distinguishing between data "born digital" and "born analog").

[5] Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 HARV. L. & POL'Y REV. 15, 20

allows it to be presented in any fashion the presenter wishes, with little regard to veracity.

Additionally, Big Data provides a different way of understanding and probing the world of information. Consider how Big Data has altered conventional research–if traditional scientific research begins with a question and then uses that hypothesis to identify and collect the appropriate data, Big Data upends that practice.[6] As near limitless information is being generated all of the time, researchers working with Big Data do not have to shape or limit their data collection. Nor are they restricted to beginning with a hypothesis. Indeed, the question can arise from the information itself. "This is why, for example, the constant stream of posted tweets on Twitter can generate data and insights for meteorologists, advertisers, and epidemiologists."[7]

B. Internet of Things

Billions of people are online. In the past decade, user demand drove a veritable explosion of smartphone sales and their applications. The next wave of information technology will likely be the Internet of Things (IoT).[8] The IoT comprises an evolving array of technologies that extend the idea of instantaneous connectivity beyond computers, smartphones, and tablets to everyday objects such as home

(2016).

[6] *Id.*

[7] *Id. See also* Victor Luckerson, *What the Library of Congress Plans to Do with All Your Tweets*, TIME (Feb. 25, 2013), http://business.time.com/2013/02/25/what-the- library-of-congress-plans- to-do- with-all- your-tweets [http://perma.cc/F5RN-UB5M].

[8] Poudel, *supra* note 2, at 997.

appliances, cars, and medical devices.[9] Market research indicates that 220 billion IoT devices will be in use by 2020.[10]

The goal of the IoT is to enable ubiquitous connection: a reality where the real, the digital, and the virtual are converging to create smart environments.[11] The underlying drivers of the IoT include massive increases in processing power, digitization of data, storage capacity, wireless communications and networking capabilities.[12]

The term IoT was first coined in 1998 by British technologist Kevin Ashton during a presentation to Procter and Gamble. He said "[a]dding radio-frequency identification and sensors to everyday objects will create an Internet of Things, and lay the foundations of a new age of machine perception."[13] The visionary concept was that radio-frequency identification devices could be used to order, track, and study manufacturing processes in an entirely innovative manner.[14] In 2009, Ashton reflected on the implications for the IoT:

---

[9] *Id.*

[10] Tim Bajarin, *The Next Big Thing for Tech: The Internet of Everything*, TIME (JAN. 13, 2014), http://time.com/539/the-next- big-thing- for-tech- the-internet- of-everything [http://perma.cc/7YCH-GY79].

[11] Meg Leta Jones, *Privacy Without Screens & the Internet of Other People's Things*, 51 IDAHO L. REV. 639, 641 (2015).

[12] Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J.L. & TECH. 6, 8 (2015).

[13] Kevin Ashton, *That 'Internet of Things' Thing*, RFID JOURNAL (June 22, 2009), http://www.rfidjournal.com/articles/view?4986 [https://perma.cc/X679-AWNF].

[14] Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CAL. L. REV. 805, 813 (2016).

> "If we had computers that knew everything there was to know about things using data they gathered without any help from us we would be able to track and count everything, and greatly reduce waste, loss, and cost. We would know when things needed replacing, repairing, or recalling and whether they were fresh or past their best. We need to empower computers with their own means of gathering information, so they can see, hear, and smell the world for themselves, in all its random glory."[15]

To be sure, the IoT offers vast possibilities to advance the myriad ways people connect, interact, and benefit from a digital world. And yet dangers aplenty lurk alongside the splendid technological possibilities.[16]

Certain innovators and technologists are making connections between the IoT and virtual/augmented reality. On March 25, 2014, Facebook founder Mark Zuckerberg announced in an online post that his company acquired Oculus Virtual Reality, the leader in virtual reality technology.[17] Zuckerberg stated that his "mission is to make the world more open and connected.… this has mostly meant building mobile apps … (but VR) is a new communication platform … you can share unbounded spaces and experiences (with) people."[18] Employing triumphal language, Zuckerberg expounded upon the possibilities of a future wherein people were connected to virtual reality – "(it) was once the dream of science fiction. But the internet

---

[15] Thierer *supra* note 12, at 10.

[16] Nikole Davenport, *Smart Washers May Clean Your Clothes, but Hacks Can Clean Out Your Privacy, and Underdeveloped Regulations Could Leave You Hanging on A Line*, 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 259, 268 (2016).

[17] Mark Zukerberg, Oculus VR Acquisition Announcement (Mar. 25, 2014), https://www.facebook.com/zuck/posts/10101319050523971.

[18] *Id.*

was also once a dream, and so were computers and smartphones. The future is coming…"[19]

II. PRIVACY FRONTIERS

A. Big Data and Privacy

Information privacy and data security are sometimes described as two sides of the same coin.[20] As people are often wary of new technology, advancements in communication techniques can be perceived as threats to privacy and lead to policymakers and consumers demanding additional safeguards against intrusion.[21] Certain experts

---

[19] *Id. See also* Ross Gerber, *Internet of Things, Virtual Reality And Smart Cars Driving Chips to the Next Level*, FORBES (Sept. 29, 2016, 4:32 PM), http://www.forbes.com/sites/greatspeculations/2016/09/29/internet-of-things-virtual-reality-and-smart-cars-driving-chips-to-the-next-level/#172a36ff451d.

[20] *Id.* Patrick Manzo, Executive Vice President, Global Customer Service and Chief Privacy Officer of Monster Worldwide, Inc., commented on the relationship between data and privacy: "Data security and data privacy are two sides of the same coin, and we trade that coin for consumer trust." He "defines data security as, simply, knowing where your data is located, and who may access the data. Data privacy is predicated on data security and requires further understanding how personal data is being collected, processed (and by whom), and transferred, and the consistency of these practices with applicable laws, regulations, and the reasonable expectations of the relevant consumers." Eileen Spear, *Data Privacy and Data Security: Two Sides of the Same Coin A Conversation with Patrick Manzo, Executive Vice President, Global Customer Service and Chief Privacy Officer of Monster Worldwide, Inc.*, NATIONAL LAW REVIEW (May 11, 2015), http://www.natlawreview.com/article/data-privacy-and-data-security-two-sides-same-coin-conversation-patrick-manzo-execut.

[21] Urs Gasser, *Recoding Privacy Law: Reflections on the Future Relationship Among Law, Technology, and Privacy*, 130 HARV. L. REV.

maintain that in 2026, up to one-third of Americans will be living with a digital device inside their bodies.[22] While "digital pills" may offer many potential benefits, a number of skeptics cite serious risks to privacy that must be addressed.[23] In a January 2015 report, the Federal Trade Commission (FTC) exhorted businesses to take concrete steps to help protect consumers' privacy.[24] The FTC report further noted that there are currently over 25 billion connected devices around the world and the number of these devices, including cars, is expected to rise exponentially.[25]

Most people know to guard their pin while accessing an ATM; it is common sense to protect a bank account from prying eyes. Yet what happens when connecting to the IoT or interacting with someone across the world through the medium of virtual reality becomes mundane? The issue of digital complacency arises when people are not adequately guarded against the new possibilities for intrusion they face in an increasingly electronic existence. The capacity to intrude on peoples' lives is increasing. Target's now-infamous use of Big Data helps illustrate the point.[26] The best time for retailers to get customers to commit to a new chain is at the moment of a major life change, such as a

F. 61, 63 (2016).

[22] Amelia R. Montgomery, *Just What the Doctor Ordered: Protecting Privacy Without Impeding Development of Digital Pills*, 19 VAND. J. ENT. & TECH. L. 147, 148 (2016).

[23] *Id.*

[24] Anthony Jones, *Autonomous Cars: Navigating the Patchwork of Data Privacy Laws That Could Impact the Industry*, 25 CATH. U.J.L. & TECH. 180, 195 (2016); FTC, *Internet of Things: Privacy and Sec. in a Connected World* 12-13 (2015).

[25] *Id.*

[26] Dennis D. Hirsch, *That's Unfair! Or Is It? Big Data, Discrimination and the FTC's Unfairness Authority*, 103 KY. L.J. 345, 350 (2015).

child's birth.[27] Several years ago, Target used Big Data to market baby goods to pregnant women. The tricky part was identifying which women were pregnant. Thanks to data analytics, Target was able to compare its massive database of customer purchases with public birth listings and in-store baby shower registries to identify about two dozen items that pregnant women often bought in the months before giving birth – items such as unscented body lotion, calcium supplements, and hand sanitizers.[28] Target then took this profile of a pregnant customer and applied it to its database of current customers. If a woman had recently purchased a number of items on the list, Target assigned her a high "pregnancy prediction score" and delivered baby-related advertisements and coupons.[29] Remarkably, Target's intrusive practices came to light when a father became aware that his high school aged daughter was pregnant when the retailer sent her numerous coupons for baby-related items.[30] As one Target statistician told the *New York Times*, data analytics is a powerful tool that must be wielded softly even in lawful arenas to avoid consumer backlash: "If we send someone a catalog and say, 'Congratulations on your first child!' and they've never told us they're pregnant, that's going to make some people uncomfortable…. We are very conservative about compliance with all privacy laws. But even if you're following the law, you can do things where people get queasy."[31]

---

[27] *Id.*
[28] *Id.* at 350-51.
[29] *Id.* at 351.
[30] Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?.
[31] *Id.*

B. Sacrificing Privacy

Privacy intrusions do not merely arise from the profit motive. Everyday consumers willingly engage in privacy-sacrificing behaviors.[32] For instance, whenever a user logs on to more than one Google service (e.g., Gmail, Google Maps, or YouTube), Google monitors and aggregates the user's searches and activity.[33] In regard to the IoT devices, consumers purchase them with little knowledge, or, perhaps more worrisome, with little care about to whom the devices may disclose data.[34]

Three problems may be exacerbated when consumers exchange their privacy rights for IoT device convenience. First, companies producing IoT devices could become like Google or Target and use customers' private data to create specialized advertisements.[35] Despite being lawful, Big Data analytics create an environment where companies have an almost unrestricted insight into customers' lives. Second, there are myriad data security risks whenever personal data is available on the internet. Hackers have repeatedly shown that they have the capability to compromise IoT devices and have broken into online video cameras and baby monitors.[36] Third, companies have shown

---

[32] Melissa W. Bailey, *Seduction by Technology: Why Consumers Opt Out of Privacy by Buying into the Internet of Things*, 94 TEX. L. REV. 1023, 1024 (2016).

[33] *Id.*

[34] Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEXAS L. REV. 85, 140-43 (2014) (explaining how difficult it is to locate the privacy policies of various IoT manufacturers).

[35] Bailey, *supra* note 32, at 1025.

[36] *Id. See generally Home, Hacked Home*, ECONOMIST (July 12, 2014), http://www.economist.com/news/special-report/21606420- perils-connected- devices-home-hacked-home [http://perma.cc/8MKC-

an eagerness to sell data to buyers. A particularly egregious example are "data brokers:" entities that aggregate consumer profiles that "may reveal where consumers live; how much they earn; and their race, health conditions, and interests."[37] Indeed, the FTC has already revealed that some mobile apps transmit information to third parties "about consumers' workouts, meals, or diets."[38] And the data exposures are not limited to third-party data brokers; for example, Fitbit has expanded its market to include sales to employers. While Fitbit insists that it does not sell individualized data to employers without the consumer's permission, its privacy terms allow it to sell "de-identified data" without consumer consent.[39]

C. Divergent Privacy Views

Broadly speaking, normative views of privacy fall

4QH9].

[37] Bailey, *supra* note 32, at 1025.

[38] Julie Brill, *The Internet of Things: Building Trust and Maximizing Benefits Through Consumer Control*, 83 FORDHAM L. REV. 205, 210-11 (2014).

[39] *See* Parmy Olson & Aaron Tilley, *The Quantified Other: Nest and Fitbit Chase a Lucrative Side Business*, FORBES (Apr. 17, 2014), http://www.forbes.com/sites/parmyolson/2014/04/17/the-quantified-other-nest- and-fitbit-chase-a- lucrative-side- business [http://perma.cc/4QFN-JLNC] ("Fitbit is selling companies the tracking bracelets and analytics services to better manage their health care budgets, and its rival Jawbone may be preparing to do the same."); Parmy Olson, *Wearable Tech Is Plugging into Health Insurance*, FORBES (June 19, 2014), http://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance [http://perma.cc/645Y-UCHJ] (detailing how "Fitbit's sales to employers are now one of the fastest growing parts of its business").

into two camps – behaviorist and consequentialist.[40] The behaviorist perspective looks to actors' actions rather than the consequences of those actions (i.e., a behaviorist might suggest that individuals have the right to engage in a specific type of data flow or to prevent that information flow from occurring).[41] The First Amendment provides an illustrative model: the press has the right to publish personal information without the subject's consent and regardless of the consequences.[42] On the other hand, the consequentialist model looks to the outcome of a given action and its effects on privacy rather than to the underlying actions. For example, certain police media guidelines prohibit the release of information about some sexual offenses or crimes involving children because it would tend to identify the victims.[43] Importantly, therefore, the consequentialist model factors unintended consequences into its assessment of whether information should be released. In short, conceiving of privacy as a set of consequences of information flows rather than a set of rights enjoyed by information subjects makes it easier to design policies that produce desirable privacy consequences.

If the consequentialist model is the best approach to protect privacy in the era of Big Data because it takes into account consequences, even those that are unintended, a complication is that statutory reform is slow compared to the rapid pace of technology. The Fourth Amendment protects citizens against unreasonable searches and seizures, a protection that includes warrantless searches of digital

---

[40] Roger Allan Ford, *Unilateral Invasions of Privacy*, 91 NOTRE DAME L. REV. 1075, 1104 (2016).
[41] *Id.*
[42] *Id.*
[43] *Id.*

data.[44] Although the Fourth Amendment has significant implications for the interplay between government and private entities that hold consumer data, it does not protect individuals from *voluntary* interactions with companies.[45] Congress has passed several sectoral statutes that protect discrete types of data that may be in the possession of private entities. For example, the Fair Credit Reporting Act protects consumer credit information, the Family Educational Rights and Privacy Act protects students' educational records, and the Health Information Portability and Accountability Act (HIPAA) protects patient medical information.[46] Overall, however, these laws cover limited types of information in certain situations. The medical information contained in a FitBit or Apple Watch is not covered by HIPAA because that statue only covers certain entities like hospitals or health insurance companies and not user-generated health information.

Given the realities of the digital age, the U.S. might benefit from adopting Britain's approach to privacy solutions. Indeed, Britain (and in large measure the European Union as well) has followed a consequentialist-omnibus approach to privacy wherein data is protected regardless of the type of entity holding the data or the precise type of data at issue.[47] This more holistic view of a "right to

---

[44] U.S. Const. amend. IV.

[45] Rebecca Lipman, *Online Privacy and the Invisible Market for Our Data*, 120 PENN ST. L. REV. 777, 787 (2016).

[46] *Id. See generally* Fair Credit Reporting Act, 15 U.S.C. §1681 (2012); Family Educational Rights and Privacy Act, 20 U.S.C. §1232g (2012); Health Information Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 26, 29, and 42 U.S.C.).

[47] Lipman, *supra* note 45, at 788; *See also* Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 Harv. L. Rev. 1966, 1975 (2013).

privacy" affects how entities view customer obligations. For its UK website, the giant data broker Acxiom has a privacy policy page that states in part "Acxiom Ltd respects the right of individuals to privacy."[48] The equivalent U.S. webpage begins with "Acxiom respects the privacy of every individual about whom we either process information or maintain information within Acxiom's information products."[49] Besides being much more legalistic and difficult to parse, the U.S. version does not contemplate any individual "right" to privacy, and it mirrors the U.S. sectoral approach by carefully defining whose privacy it will respect.[50]

D. Coding Privacy

1. Privacy by Design

For some researchers, the solution to digital privacy lies in code, taking privacy into account at the forefront of the engineering lifecycle by culturally perpetuating privacy at all levels of an organization.[51] In the Privacy by Design (PbD) framework, managers and creators are encouraged to think about the data and concomitant privacy interests at the start of the design process rather than being simply an

---

[48] Acxiom, *UK Privacy Policy*, http://www.acxiom.com/about-acxiom/privacy/uk-privacy-policy (last visited Mar. 1, 2017).
[49] Acxiom, *US Products Privacy Policy*, http://www.acxiom.com/About-Acxiom/Privacy/US-Products-Full-Privacy-Policy/ (last visited Mar. 1, 2017).
[50] Lipman, *supra* note 45, at 788.
[51] Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles*, IAB (2009), *https://www.iab.org/wp-content/IABuploads/2011/03/fred_carter.pdf.*

afterthought in the development lifecycle.[52] PbD is the notion that online platforms should be designed from the ground up with privacy in mind.[53] Refinement of PbD has yielded seven core tenets called the foundational principles: 1) proactive; 2) privacy as the default setting; 3) privacy embedded into design; 4) full functionality; 5) full lifecycle protection; 6) transparency; and 7) respect for user privacy.[54]

PbD enables creators to specially architect environments and systems with considerations of data use for implementation at the onset, which will directly tie to business or operational processes once the solution is promoted into a live production status.[55] In essence, PbD is a fluid and evolving framework with applicability to the continual advancement of data collection, storage, and use.[56] The design and implementation of privacy requirements in systems is a continually vexing problem and requires a multi-various approach to include the translation of complex social, legal, and ethical concerns into systems requirements.[57] Perhaps most significant, PbD is an opportunity to foster a privacy-first culture that extends from organizational governance and leadership to design concepts that over time will help define brand reputation.[58] After all, if PbD proves successful, it may assist the symbiotic relationship between privacy and the helpful aspects of Big Data: as former FTC chairwoman Edith Ramirez recently

---

[52] *Id.*
[53] Ari Ezra Waldman, *Privacy, Sharing, and Trust: The Facebook Study*, 67 CASE W. RES. L. REV. 193, 226 (2016).
[54] Cavoukian, *supra* note 75.
[55] Eric Everson, *Privacy by Design: Taking Ctrl of Big Data*, 65 CLEV. ST. L. REV. 27, 29 (2016).
[56] *Id.*
[57] *Id.*
[58] *Id.*

remarked, "[t]here is a risk we won't really be able to innovate, we won't really be able to make full use of big data … unless we really do make sure that consumers feel that they have control."[59]

2. Privacy Engineering

In 2017, the National Institute of Standards and Technology (NIST) developed An Introduction to Privacy Engineering and Risk Management in Federal Systems (PRM). The novel framework is a new approach to assessing and managing risks to privacy and is focused on achieving freedom from conditions that can create problems for individuals with unacceptable consequences that arise from the system as it processes personally identifiable information (PII).[60] Whereas PbD involves approaching the entire design of a system or product from a positive sum, proactive viewpoint, and using privacy as the default choice in system design, privacy engineering takes a more granular approach and recognizes the boundaries and overlap between privacy and security.[61]

---

[59] Anita L. Allen, *Protecting One's Own Privacy in A Big Data Economy*, 130 HARV. L. REV. F. 71, 78 (2016).

[60] Brooks et al., *NISTIR 8062 – An Introduction to Privacy Engineering and Risk Management in Federal Systems*, iv (Jan. 2017), http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf. Office of Management and Budget defines "personally identifiable information" as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual," in Circular A-130, "Managing Federal Information as a Strategic Resource" (2016), https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

[61] Janine S. Hiller, *Healthy Predictions? Questions for Data Analytics in Health Care*, 53 AM. BUS. L.J. 251, 303 (2016). *See also* Brooks et

As pertains to information security, the security objectives commonly known as the "CIA Triad" – Confidentiality; Integrity; and Availability are a means of categorizing capabilities and controls to achieve security outcomes.[62] Confidentiality is about how information is kept private; Integrity means neither systems nor data have been improperly altered or changed without authorization; and Availability means that systems function as anticipated, systems are prompt, and services are accessible when authorized users attempt to access them.[63] Significantly, the PRM realizes that privacy concerns may develop even when a system is properly adhering to CIA protocol. Accordingly, the PRM fashioned three privacy engineering objectives meant to compliment but in no way supplant the three traditional CIA security information objectives.

The first privacy engineering objective, Predictability, means designing systems so that stakeholders are not surprised by the handing of personally identifiable information (PII).[64] Put another way, Predictability is the foundation upon which stable, trusted relationships between systems and individuals can be built. The second objective, Manageability, is viewed as a system property that enables several of the Fair Information Practice Principles (FIPPs).[65] The FIPPS were first established by an advisory committee to the Secretary of Health, Education, and Welfare and were the basis of the Privacy Act of 1974, which governs federal

al., *supra* note 60, at 8.

[62] Brooks et al., *supra* note 60, at 10.

[63] Eric P. Roberson, *"Adequate" Cybersecurity: Flexibility and Balance for A Proposed Standard of Care and Liability for Government Contractors*, 25 FED. CIRCUIT B.J. 641, 652 (2016).

[64] Brooks et al., *supra* note 60, at 18.

[65] *Id.* at 19.

agencies' collection and use of personal information.[66] In 1980 the FIPPs were revised by the Organization for Economic Co-operation and Development and became an internationally recognized set of privacy principles.[67] The principles are laudable from an objective privacy standpoint and include collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.[68] Using the PRM model, if an entity cannot administer individuals' information with sufficient granularity, it cannot be confident that inaccurate information can be identified and corrected, obsolete information disposed of, only necessary information is collected or disclosed, and that individuals' privacy preferences about uses of their information are implemented and maintained.[69] Disassociability, the third PRM objective, captures an integral element of privacy-preserving systems – that the system actively protects or "blinds" an individual's identity or associated activities from exposure.[70]

Even more than PbD, privacy engineering has vast potential ramifications for the protection of PII because its Disassociability objective may prevent or forestall the effects of new technologies aimed at re-identifying "anonymized" data. For instance, the concept behind the smart grid is, among other things, to upgrade the existing national electrical grid to allow for the greater use of modern technologies that provide two-way communication between

---

[66] J. Frazee, M. Finley, JJ Rohack, *Mhealth and Unregulated Data: Is This Farewell to Patient Privacy?,* 13 IND. HEALTH L. REV. 384, 401 (2016).
[67] *Id.*
[68] *Id.*
[69] Brooks et al., *supra* note 60, at 19.
[70] *Id.* at 20.

energy producers and energy customers, eliminate vulnerabilities to cyberattacks, reduce power outages, promote the efficient use of electricity, and reduce customer costs.[71] Presently, in most areas of the country, utilities only learn of a power outage when a customer calls to report it.[72] The smart grid enables utilities to identify outages, their cause, and the customers affected as soon as they occur.[73] This allows utilities to employ resilient solutions such as quickly rerouting electricity to customers ti reduce the impact of an outage.[74] Advanced smart grid technology also allows utilities to monitor the health of the grid proactively, allowing them to repair pending faults in advance.[75] Traditionally, personal data is organized into three categories: (1) customer-specific data, (2) customer-specific de-identified data, and (3) aggregated data representing community level information.[76] To be sure, customer-specific data generate the greatest privacy concerns because that data set contains personal information that can be traced back to specific individuals and households and therefore should be afforded the most protection.[77] For this reason, in

---

[71] Robert B. McKinstry Jr., Thomas D. Peterson, Steven Chester, *Unlocking Willpower and Ambition to Meet the Goals of the Paris Climate Change Agreement (Part Two): The Potential for Legal Reform and Revision*, 47 ENVTL. L. REP. NEWS & ANALYSIS 10135, 10148 (2017).

[72] Samuel J. Harvey, *Smart Meters, Smarter Regulation: Balancing Privacy and Innovation in the Electric Grid*, 61 UCLA L. REV. 2068, 2072-73 (2014).

[73] *Id.*

[74] *Id.*

[75] *Id.*

[76] Megan McLean, *How Smart Is Too Smart?: How Privacy Concerns Threaten Modern Energy Infrastructure*, 18 VAND. J. ENT. & TECH. L. 879, 902 (2016).

[77] *Id.*

Colorado, a utility may not disclose customer data to third party entities, to include government agents, unless the customer first submits a signed "consent to disclose customer data form."[78] Accordingly, government agents cannot access consumer data without a warrant, subpoena, or court order.[79] The rationale behind the precautionary rule is because customer-specific de-identified data is customer-specific usage information that was stripped of PII yet still indicates single home usage. The problem is current limits of digital privacy protection make it impossible to discern whether a given piece of data was sufficiently de-identified to preclude the ability to re-identify it. Additionally, technological ability to manipulate data is constantly changing, which creates a genuine concern that data sufficiently de-identified today may be re-identifiable tomorrow.[80] Consequently, Colorado takes the sensible position that recognizes de-identified data presents the same threat to privacy as customer data and treats it identically.[81] The precautionary steps Colorado implements to prevent anonymized data from being re-identified could be helped by imbedding the PMR's Disassociability objective into the smart grid code.

III. DEVELOPMENTS IN CYBERSECURITY

A. Breaches

Computer networks constitute the nerve system of modern society. States, organizations, corporations, and

---

[78] 4 COLO. CODE REGS. § 723-3:3031.
[79] McLean, *supra* note 100, at 903.
[80] *Id.*
[81] *Id. See also* 4 Colo. Code Regs. § 723-3:3026(a).

individuals depend on information infrastructures for myriad uses to include commerce, communication, emergency services, energy production and distribution, mass transit, military defenses, and health services.[82] The centrality of digital technology in all facets of modern life coupled with the vulnerability of the selfsame technologies and infrastructures to threats and damage necessitates close attention to issues of cybersecurity broadly understood. As a recent study observed, cybersecurity incidents intentional or accidental, are increasing at an alarming pace and could disrupt the supply of essential services people take for granted such as water, healthcare, electricity or mobile services.[83] Threats are diverse and can have different origins including criminal, politically motivated, terrorist or state-sponsored attacks, as well as natural disasters and unintentional mistakes.[84]

It is no surprise that the number and magnitude of data breaches continue to rise.[85] The Global State of Information Security Survey reports that the compound annual growth rate of detected breaches increased by 66% in the six years prior to 2015.[86] While the public may find an occasional data breach understandable, the actual prevalence

---

[82] Oren Gross, *Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents*, 48 CORNELL INT'L L.J. 481, 482 (2015).
[83] *Id.*
[84] *Id.*
[85] Open Security Foundation, *Data Loss Statistics*, DataLossDB, http://datalossdb.org/statistics (last visited Mar. 1, 2017) (data begins from 2007).
[86] *Security Incidents Continue to Rise in Cost and Frequency While Budgets Decrease, according to PwC, CIO and CSO's The Global State of Information Security® Survey 2015*, PWC, http://www.pwc.com/us/en/press-releases/2014/global-state-of-information-security-survey-2015.html (last visited March 1, 2017).

is surprisingly high and approximately one of five organizations will likely succumb to a material data breach in the next two years.[87] A brief survey of recent hacking events is eye-raising as hackers compromised the confidential account and financial information of 145 million eBay records; 130 million Heartland records; 76 million JPMorgan Chase client records; 80 million Anthem records; 77 million Sony records; 70 million Target records; and 56 million Home Depot records.[88]

The Federal Information Security Management Act of 2002 (FISMA) created a cybersecurity framework for federal information systems, with an emphasis on risk management, and required implementation of agency-wide information security programs.[89] Pursuant to FISMA, the National Institute of Standards and Technology (NIST) is responsible for developing security standards for federal computer systems (aside from national security systems).[90] Each federal agency is responsible for complying with those standards and they report annually on the status of their information security to the Office of Management and Budget, which then reports to Congress.[91]

Given splashy news headlines about hacking results, it is perhaps not surprising that many consumers believe companies are not taking sufficient measures to prevent data breaches. By one estimate, 90% of the data breaches that happened in 2014 could have been prevented had the compromised entity followed industry "best practices."[92]

---

[87] Marian K. Riedy & Bartlomiej Hanus, *Yes, Your Personal Data Is at Risk: Get over It!*, 19 SMU SCI. & TECH. L. REV. 3, 12 (2016).
[88] *Id.*
[89] 40 U.S.C. §11331 (2012).
[90] *Id.*
[91] 44 U.S.C. §§3544-3545.
[92] *Id.*

And yet the tremendous increase in data breaches is coexistent with the fact that the amount of money spent protecting and securing data has consistently increased over the years.[93] In fact, global expenditure on information security is projected to reach over $100 billion by 2018.[94] Despite the spending increases, however, industry experts almost universally concede that throwing money at information security will not cure the pandemic because "data security systems are complex beasts, with multiple vulnerabilities and points of attack."[95]

B. Protecting Critical Infrastructure

Cyberattacks are occurring at a furious pace; from Sony to JP Morgan and the U.S. Office of Personnel Management, Saudi Aramco to the Ukraine crisis, cybersecurity is increasingly taking center stage in the diverse arenas of geopolitics, international economics, security, and law.[96] Yet despite the increasing proliferation of cyber events, the field of international cybersecurity law and policy remains relatively immature. For example, although there has been a relative abundance of scholarship exploring the contours of the law of cyberwarfare, less attention is paid to defining a law of cyber peace applicable

---

[93] *Id.*

[94] *Id.*

[95] *Id. See generally* Robert W. Hahn & Anne Layne-Farrar, *THE LAW AND ECONOMICS OF SOFTWARE SECURITY*, 30 HARV. J.L. & PUB. POL'Y 283, 288 (2006) (discussing the many different routes for attacking computers or networks).

[96] Scott J. Shackelford, J.D., Scott Russell, J.D., Andreas Kuehn, *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, 17 CHI. J. INT'L L. 1, 3 (2016).

below the armed attack threshold at which point the law of armed conflict is activated.[97] As underscored by the International Court of Justice in the oft-cited *Nicaragua* case, "[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations."[98] Accordingly, cyber hostilities directed against

---

[97] *Id. See e.g.*, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICATION TO CYBER WARFARE 17 (Michael N. Schmitt ed., 2013) (discussing when a cyberattack could trigger the right of self-defense); TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 127 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009); David Turns, *Cyber Warfare and the Notion of Direct Participation in Hostilities*, 17 J. CONFLICT & SECURITY L. 279 (2012); Emily Crawford, *VIRTUAL BATTLEGROUNDS: DIRECT PARTICIPATION IN CYBER WARFARE*, 9 J.L. & POL'Y FOR INFO. SOC'Y 1 (2012); Michael N. Schmitt & Sean Wattset, *The Decline of International Humanitarian Law* Opinio Juris *and the Law of Cyber Warfare*, 50 TEX. INT'L. L.J. 189 (2015); LTC Dean L. Whitford et al., JUDGE ADVOCATE GENERAL'S LEGAL CTR. & SCH., U.S. ARMY, LAW OF ARMED CONFLICT DESKBOOK 29 (LTC William J. Johnson & LCDR David H. Lee eds., 2016); Michael N. Schmitt, *Cyber Operations and the* Jus Ad Bellum *Revisited*, 56 VILL. L. REV. 569 (2011); Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533 (2010); Eric Talbot Jensen, *Future War and the War Powers Resolution*, 29 EMORY INT'L L. REV. 499 (2015).

[98] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgement, 1986 I.C.J. Rep.14, ¶ 202 (June 27)The case involved U.S. assistance to Nicaraguan guerrillas known as the Contras and the mining of Nicaraguan harbors. The case provided helpful jurisprudence on the scope of the prohibition on the use of force. The court reasoned "[t]here appears now to be general agreement on the nature of the acts which can be treated as constituting armed attacks. In particular, it may be considered to be agreed that an armed attack must be understood as including not merely action by regular armed forces across an international border, but also "the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to

cyber infrastructure located on another state's territory, whether government owned or not, constitute a violation of that state's sovereignty.[99] Yet a critical unanswered question with respect to these sovereign rights and responsibilities is whether cyber operations that do not cause damage nor amount to an intervention nevertheless violate the targeted state's sovereignty.[100] Given the paucity of guidance in this critical arena, the U.S. has turned to strengthening its cyber defenses for critical infrastructure.

In 2009, President Obama declared Critical Infrastructure (CI) to be a "strategic national asset," though a fully integrated U.S. cybersecurity policy has yet to be established.[101] In 2013, Executive Order 13636 (EO), "Improving Critical Infrastructure Cybersecurity" provided for the creation of the NIST Cyber Security Framework, a voluntary set of standards in best security practices for critical infrastructure.[102] CI is defined in the EO as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[103] In Framework Draft Version 1.1, released in January 2017, the authors explain

---

amount to" (*inter alia*) an actual armed attack conducted by regular forces, "or its substantial involvement therein." This description, contained in Article 3, paragraph g), of the Definition of Aggression annexed to General Assembly resolution 3314 (XXIX), may be taken to reflect customary international law. *Id.* at 14, ¶ 195.

[99] Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?*, 25 STAN. L. & POL'Y REV. 269, 274-75 (2014).

[100] *Id.* at 275.

[101] President Obama, *Remarks by the President on Securing our Nation's Cyber Infrastructure (*May 29, 2009).

[102] Exec. Order No. 13,681, 79 Fed. Reg. 63,491 (2014).

[103] *Id.*

that cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems and thus place the Nation's security, economy, public safety and health vectors at risk.[104] Extending the Framework's viability beyond CI, the authors posit that similar to financial and reputational risk, cybersecurity risk affects a company's bottom line as it can drive up costs, impact revenue, harm an organization's ability to innovate and to gain and maintain customers.[105]

C. Toward a Standard of Care

The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of an organization's risk management processes.[106] The Framework consists of three components: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles.[107] Through use of the Profiles, the Framework will help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources.[108] The Tiers provide a mechanism for organizations to view and understand the characteristics

---

[104] Cybersecurity Framework, Draft Version 1.1, NAT. INST. OF STAND. & TECH., https://www.nist.gov/sites/default/files/documents/2017/01/30/draft-cybersecurity-framework-v1.1.pdf
[105] *Id.*
[106] *Id.*
[107] *Id.*
[108] *Id.*

of their approach to managing cybersecurity risk.[109]

The NIST Framework is important, in part, because even though its critics argue that it helps solidify a reactive stance to the nation's cybersecurity challenges, it is in fact spurring the development of a standard of cybersecurity care in the U.S. that plays into discussions of due diligence.[110] The NIST Framework harmonizes industry best practices to provide a flexible and cost-effective approach to enhancing cybersecurity that assists owners and operators of CI in assessing and managing cyber risk. Although the NIST Framework is still relatively new, some private-sector clients are already receiving advice that if their "cybersecurity practices were ever questioned during litigation or a regulatory investigation, the 'standard' for 'due diligence' was now the NIST Cybersecurity Framework."[111] In the relative near future, the NIST Framework has the potential not only to shape a standard of care for domestic critical infrastructure organizations but also to harmonize global cybersecurity best practices for the private sector writ large, given active NIST collaborations with a number of nations, including the U.K., Japan, Korea, Estonia, Israel, and Germany.[112]

---

[109] *Id.*

[110] Shackelford, *supra* note 120, at 27. *See* Scott J. Shackelford et al., *Toward a Global Standard of Cybersecurity Care?: Exploring the Implications of the 2014 Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. J. INT'L L. 287 (2015).

[111] Shackelford, *supra* note 120, at 27. *See also Why the NIST Cybersecurity Framework Isn't Really Voluntary*, Info. Sec. Blog (Feb. 25, 2014), http://www.pivotpointsecurity.com/risky-business/nist-cybersecurity-framework.

[112] Shackelford, *supra* note 120, at 27.

D. The Plight of Corporations

Corporations that are victims of cyberattacks perpetuated by a state actor have little options under domestic law. A state actor conducting hostile cyber operations against a corporation indeed violates the sovereignty of the host nation.[113] It matters not whether these activities were physically destructive as long as they were unlawful and detrimental.[114] A host state has multifarious options to respond to the aggressor state depending on whether the activity is an armed attack or something that falls beneath the level of an armed attack.[115] Yet, if states have options, what options might private entities possess? A state reacting to cyber hostilities will look to international law to regulate its response; in contrast, a corporation can only rely upon domestic law to justify its actions.[116] In addressing the immediate hostile cyber event, a corporation may only use protective measures that do not cause destruction or death to a hostile state actor's cyber agents or

---

[113] Daniel Garrie & Shane R. Reeves, *An Unsatisfactory State of the Law: The Limited Options for A Corporation Dealing with Cyber Hostilities by State Actors*, 37 CARDOZO L. REV. 1827, 1849 (2016). *See also* Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?*, 25 STAN. L. & POL'Y REV. 269, 274-75 (2014) ("[H]ostile cyber operations directed against cyber infrastructure located on another state's territory, whether government owned or not, constitute, *inter alia*, a violation of that state's sovereignty...."); *see also* Michael Schmitt, *International Law and Cyber Attacks: Sony v. North Korea*, Just Security (Dec. 17, 2014, 9:29 AM), http://justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea. For example, North Korea's cyber hostilities directed at Sony violated the sovereignty of the United States.

[114] Garrie, *supra* note 137, at 1850-51.

[115] *See generally* Schmitt, *supra* note 137.

[116] Garrie, *supra* note 137, at 1851.

infrastructure.[117] Further, the corporation must exercise caution and not pierce the sovereignty of the hostile state, an exercise in precision which can prove difficult in the borderless nature of cyberspace, since this would also be a violation of international law.[118] In other words, a state has the latitude to even preempt a cyberattack and has internationally-recognized authority to engage the hostile state in self-defense. On the other hand, a private entity's actions must be limited to the defensive rather than anticipatory or preemptive spheres and its response is capped at stopping the hostile state's cyber hostilities without violating international law.[119] In the end, private entities have few legal options that are consistently effective against

---

[117] *Id. See* U.S. DEP'T OF DEF., QUADRENNIAL DEFENSE REVIEW REPORT, at 4 (2010) (discussing the difficulties of cyberspace); Stephen W. Korns & Joshua E. Kastenberg, *Georgia's Cyber Left Hook*, PARAMETERS, WINTER 2008-09, AT 60, 70 ("[I]nternational laws of war are...fundamentally weak in addressing borderless, nonstate actor participation in cyber conflict where individuals organize their own cyber campaigns.").

[118] Garrie, *supra* note 132, at 1851. Interestingly, the lack of meaningful national borders in cyberspace could lead to the theoretical situation where a private entity acts in self-defense against a hostile state actor's agents in cyberspace and the result is death or destruction in the host nation. As the use of force in self-defense is an exclusive right of state actors, the corporation would be in violation of the U.N. Charter's general prohibition on the use of force. *See* U.N. Charter art 2, ¶ 4. As a perverse result, under the law of state responsibility, the United States would be responsible for the corporation's violation of the hostile state's sovereignty. *See* G.A. Res. 56/83 (Jan. 28, 2002) (Responsibility of States for Internationally Wrongful Acts) This is the same result if a corporation is acting in self-defense and their response damages a third nation's cyber infrastructure or personnel. *Id.*

[119] *See generally* Dever & Dever, *Making Waves: Refitting the Caroline Doctrine for the Twenty-First Century*, 31 QUINNIPIAC L. REV. 165 (2013) (historical investigation into the norms of anticipatory self-defense of nations).

the variety of threats that they face.[120] Criminal enforcement is complicated by the lack of a consistently enforced international paradigm, complex jurisdictional issues, and the vexing problem of identifying an attacker in a manner specific enough to support criminal prosecution.[121] Civil litigation is similarly of questionable utility for two reasons: (1) the problem of anonymity in cyberspace and (2) the low likelihood of holding third parties liable in tort.[122]

IV. E-REPUBLIC

A. A Lively Past

In 1815 John Adams said to Thomas Jefferson, "What do we mean by the Revolution? The war? That was no part of the Revolution; it was only an effect and consequence of it. The Revolution was in the minds of the people . . . before a drop of blood was shed at Lexington."[123] If the Revolution had ideological origins when the original patriot Crispus Attucks fell during the Boston Massacre, the question of who has the right to vote continues to be a painful chapter in the history of the American experiment.[124] When surveyed about what rights are most valued under the Constitution, Americans invariably include the right to

---

[120] Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 Harv. J.L. & Tech. 429, 442 (2012).
[121] *Id.*
[122] *Id.*
[123] BERNARD BAILYN, THE IDEOLOGICAL ORIGINS OF THE AMERICAN REVOLUTION 1 (KNOPF 1967).
[124] Kevin Brown, Foreword: President Barack Obama Law & Policy Symposium, 35 T. MARSHALL L. REV. 1, 7 (2009).

vote.[125] As the Founders understood, an advantage of federalism is its parochial qualities because state and local governments draw voters into the political process.[126] Local, accessible government allows individuals to participate actively in governmental decision making and trains citizens in the techniques of democracy, fosters accountability among elected officials and enhances voter confidence in the democratic process.[127]

History can sometimes be a comfort because 2016 was not the first bruising, contentious American presidential election. Consider the election of 1800 between Thomas Jefferson and John Adams; the outcome of the contest was so bizarre that America had to amend its Constitution to make sense of new political realities.[128] Prior to ratification of the 12th Amendment, electoral college members each had two votes for president and whoever garnered the most votes was president while second place took the vice presidency.[129] When Jefferson and his Democratic-Republican running mate, Aaron Burr, tied with 73 votes, Federalist Party founder Alexander Hamilton famously sneered, "Mr. Burr loves nothing but himself –thinks of nothing but his own aggrandizement," which ultimately turned favor against Burr in the House and Representatives and led Jefferson to become president.[130] As fans of the

---

[125] Joshua A. Douglas, *Is the Right to Vote Really Fundamental?*,18 CORNELL J.L. & PUB. POL'Y 143, 145 (2008)
[126] Deborah Jones Merritt, *The Guarantee Clause and State Autonomy: Federalism for A Third Century*, 88 COLUM. L. REV. 1, 7 (1988).
[127] *Id.*
[128] Eliott C. McLaughlin, *10 of the Most Bizarre Elections in American History*, CNN Politics (March 4, 2016 8:26 AM), http://www.cnn.com/2015/10/30/politics/interesting-u-s-elections/).
[129] *Id.*
[130] *Id.*

smash hip-hop Broadway musical "Hamilton" know all too well, the antipathy between Hamilton and Burr continued for three more years until Burr killed Hamilton in a duel.[131]

Or consider the 1876 presidential campaign when Rutherford B. Hayes defeated his Democrat opponent Samuel J. Tilden by one electoral vote.[132] In a manner that presaged our modern salacious-driven news cycle, Hayes scorched Tilden with a series of broadsides calling him everything from a briber to a thief and drunken syphilitic.[133] Suspicion of voter fraud in Republican-controlled states was rampant while Jim Crowe-era marauders suppressed voter turnout in the South.[134] Consequently, Florida, Louisiana and South Carolina were deemed too close to call, and Tilden remained one electoral vote short of the 185 required to win. With 165 electoral votes tallied for Hayes, all he needed to do was capture the combined 20 electoral votes from those three contested states to win the presidency.[135] An ensuing crisis unfolded, starting with threats of a second civil war and ending with a backroom deal, the Compromise of 1877, that delivered the presidency to Hayes in exchange for the removal of federal troops from the South and the effective end of Reconstruction.[136]

---

[131] Chris Isidore, 'Hamilton' has best week ever for a Broadway show, CNN (November 30, 2016 1:12 AM), http://money.cnn.com/2016/11/29/media/hamilton-box-office-record/.
[132] John Copeland Nagle, *How Not to Count Votes*, 104 COLUM. L. REV. 1732 (2004).
[133] Gilbert Kin, *The Ugliest, Most Contentious Presidential Election Ever*, Smithsonian.com (September 7, 2012), http://www.smithsonianmag.com/history/the-ugliest-most-contentious-presidential-election-ever-28429530/.
[134] *Id.*
[135] *Id.*
[136] *Id. See generally* Nathan L. Colvin & Edward B. Foley, *Lost Opportunity: Learning the Wrong Lesson from the Hayes-Tilden*

In recent memory, the contest between George W. Bush and Al Gore in 2000 was a source of bitterness and anguish for many. As two scholars succinctly summarized in 2001, "[w]e live in extraordinary times. In the past year the Supreme Court of the United States has decided an election and installed a president."[137] On election night every major broadcast and cable news channel – ABC, NBC, CBS, CNN, MSNBC, and Fox News – all made and withdrew projections of Florida for both Bush and Gore.[138] At 3 a.m. on November 8, Gore conceded when Bush pulled 50,000 votes ahead and broadcasters put Florida's 25 electoral votes into Bush's win column.[139] But within two hours of Gore's concession, Bush's Florida lead had shrunk and the small margin triggered an automatic recount under Florida law.[140] Almost immediately, concerns about voting irregularities emerged in places like Palm Beach County, where a punch-card ballot with a format that was easily misread resulted in many disqualified votes.[141] A scant few days after the election, The New York Times ran a piece that explained what "chads" were to an anxious electorate:

Dispute, 79 FORDHAM L. REV. 1043, 1045 (2010).

[137] Jack M. Balkin & Sanford Levinson, *Understanding the Constitutional Revolution*, 87 VA. L. REV. 1045 (2001).

[138] Peter Marks & Bill Carter, The 2000 Elections: The Network Predictions; Media Rethink an Urge to Say Who's First, N.Y. TIMES (November 9, 2000), http://www.nytimes.com/2000/11/09/us/2000-elections-network-predictions-media-rethink-urge-say-who-s-first.html.

[139] Samantha Levine, Hanging Chads: As the Florida Recount Implodes, the Supreme Court Decides Bush v. Gore, US NEWS (January 17, 2008 5:00 PM), https://www.usnews.com/news/articles/2008/01/17/the-legacy-of-hanging-chads.

[140] *Id.*

[141] *Id.*

> The leadership of the free world may be decided by chads[,] . . . tiny bits of cellulose that, under the pressure of a citizen wielding his voting franchise and a metal stylus, are supposed to detach sharply from a punch-card ballot. The rectangular hole is interpreted as a vote by an electronic reader, while all unpunched holes are considered nonvotes. The problem with chads is that they often do not fully detach . . . Then they're called 'hanging chads,' and the computers can interpret them in various ways each time they are run through. The issue is significant in Florida because thousands of ballots were read by voting machines as having no vote in the presidential column. Democrats hope that when the paper cards are reviewed one by one, many will be seen to have partly punched holes next to Mr. Gore's name.[142]

For 36 days, who won the presidency was in limbo, as Bush and Gore were separated by a razor-thin margin, complicated by the "hanging chad" difficulties in Florida. On November 26, Florida Secretary of State Katherine Harris, who doubled as Bush's state campaign co-chair, certified voting results that gave Bush a minute 537-vote lead.[143] On December 12, the United States Supreme Court rendered its decision in a 5-to-4 vote which allowed the Harris vote certification to stand and delivered the presidency to Bush.[144] As one scholar noted, a delicious irony that surely John Marshall would have enjoyed emerged from the Court's decision in *Bush v. Gore*: we moved from a world in which the interpretive authority of the political

---

[142] Ford Fessenden, *Counting The Vote: The Ballots; After Cards are Poked, The Confetti Can Count*, N.Y. TIMES (Nov. 12, 2000), http://www.nytimes.com/2000/11/12/us/counting-the-vote-the-ballots-after-cards-are-poked-the-confetti-can-count.html.

[143] Levine, *supra* note 193.

[144] *Bush v. Gore*, 531 U.S. 98 (2000).

branches was clear and that of the Supreme Court questionable and uncertain, to one in which the Court's authority stood relatively unchallenged while that of everyone else is under siege.[145] Even years after the election, people were still dumbfounded with what to do with the punch cards [t]he contested . . . election has largely faded into people's hazy memories of pre-9/11 America. But the Florida ballots are still there, nearly six million punch cards and their chads, stowed in boxes, stacked on pallets, wrapped in plastic."[146]

B. E-Voters

In 1955, Isaac Asimov penned a short story that turned out to be less fantastic than his usual fare; in the not-so-distant-future, an advanced computer holding "trillions of items" of information determined the outcome of the 2008 presidential election.[147] In 2002, after the debacle of the "hanging chad," and with growing awareness of the limitations of digital technology to disrupt or upend an election, Congress passed the Help America Vote Act (HAVA), which was designed to help overhaul the nation's

---

[145] Larry D. Kramer, *The Supreme Court 2000 Term Foreword: We the Court*, 115 HARV. L. REV. 4, 15 (2001).

[146] Dana Canedy, *Florida Ponders Fate of Historic 2000 Ballots*, N.Y. TIMES (February 16, 2003), http://www.nytimes.com/2003/02/16/us/florida-ponders-fate-of-historic-2000-ballots.html?rref=collection%2Ftimestopic%2FPresidential%20Election%20of%202000&action=click&contentCollection=timestopics&region=stream&module=stream_unit&version=latest&contentPlacement=287&pgtype=collection.

[147] Ira S. Rubinstein, *Voter Privacy in the Age of Big Data*, 2014 WIS. L. REV. 861, 862 (2014).

election system in the wake of the 2000 election.[148] The HAVA seeks to promote the efficiency and accuracy of federal elections.[149] It establishes minimum standards for "voting systems" for federal elections and mandates that those systems generate a paper record of each vote that may be used in case of a recount.[150] Lastly, HAVA also requires each state to establish a central "computerized statewide voter registration list" to "serve as the official voter registration list" for all "elections for Federal office.

Perhaps because voting is essential to American democracy, many people have a false sense of security when it comes to the purported infallibility of e-voting. In truth, the technologists who designed the current generation of e-voting computers "weren't thinking about … system security . . . [Most machines] are a decade or older. Most . . . [run] Windows XP, for which Microsoft hasn't realized a security patch since April 2014 . . . [M]any of them are susceptible to malware, or equally if not more alarming, a well-timed denial of service attack."[151] When people think

---

[148] Tom Zeller, *Ready or Not, Electronic Voting Goes National*, N.Y. TIMES, September 19, 2004, http://www.nytimes.com/2004/09/19/politics/campaign/ready-or-not-electronic-voting-goes-national.html?_r=0. *See also* Help America Vote Act of 2002, Pub. L. No. 107-252, 116 Stat. 1666 (2002) (codified as amended at 52 U.S.C. §§ 20901-21145).

[149] Michael T. Corely, *Dismantling the Unitary Electoral System? Uncooperative Federalism in State and Local Elections*, 111 NW. U. L. Rev. 103, 111 (2017).

[150] *Id.*

[151] Brian Barret, *America's Electronic Voting Machines are Scarily Easy Targets*, WIRED (August 2, 2016, 9:17 AM), https://www.wired.com/2016/08/americas-voting-machines-arent-ready-election.

about hacking and e-voting, they usually imagine a switching results scenario, but hackers can do far less and still cause havoc; if machines are not working, or working slowly, that could create a host of problems and prevent individuals from casting a ballot.[152] To be clear, there is a host of new, more secure e-voting computers available than the machines most states bought in bulk a decade or more ago, but only a handful of states and municipalities such as Rhode Island, Washington D.C. and parts of Wisconsin upgraded their equipment in the year prior to the current election.[153] One e-voting expert explained why the states have failed to upgrade their machines: "[t]he money's not there right now. . . . [E]lection officials told us what they are hearing from their state legislators [who will not] be funding this type of equipment . . . they say come back to us after there's some kind of crisis. Perhaps this latest election cycle pushed the state of equipoise in favor of purchasing more secure equipment to protect the integrity of American democracy.

Yet no matter whether e-voting security measures are improved, nothing can guarantee a hack-free election. For this reason, it is important to consider what national policy should be in the face of international hacking. In the weeks after the 2016 election, a declassified report authored by the CIA, FBI, and NSA declared that the president of Russia, Vladimir V. Putin, personally "ordered an influence campaign in 2016 aimed at the U.S. presidential election," and turned from seeking to "denigrate" Hillary Clinton to developing "a clear preference for President-elect Trump."[154] Furthermore, the report did not back up claims

---

[152] *Id.*
[153] *Id.*
[154] David Sanger, *Putin Ordered 'Influence Campaign' Aimed at U.S.*

by the Trump campaign that the Russian-sponsored hacking activity had no effect on the election because "[w]e did not make an assessment of the impact that Russian activities had on the outcome of the 2016 election," the report concluded, saying it was beyond its responsibility to analyze American "political processes" or public opinion.[155] The intelligence agencies did conclude "with high confidence" that Russia's primary military intelligence unit, the GRU, created a "persona" called Guccifer 2.0 and a website, DCLeaks.com, to release the e-mails of the Democratic National Committee and of the chairman of the Clinton campaign, John D. Podesta.[156]

By November 23, 2016, the Clinton campaign was urged by a number of premier computer scientists to call for a recount of vote totals in Wisconsin, Michigan and Pennsylvania.[157] The scientists thought they discovered evidence that vote totals in three states may have been manipulated or hacked.[158] Essentially, the researchers believed they a questionable trend of Clinton performing worse in counties that relied on electronic voting machines compared to paper ballots and optical scanners.[159] And while the group had not found any evidence of hacking, the unusual voter pattern warranted an independent review.[160]

Election, Report Says, N.Y. TIMES (January 6, 2017), https://www.nytimes.com/2017/01/06/us/politics/russia-hack-report.html.

[155] *Id.*

[156] *Id.*

[157] Dan Merica, *Computer Scientists Urge Clinton Campaign to Challenge Election Results*, CNN politics (November 23, 2016, 4:43 PM), http://www.cnn.com/2016/11/22/politics/hillary-clinton-challenge-results/.

[158] *Id.*

[159] *Id.*

[160] *Id.*

On January 7, 2017, President-elect Trump conceded that Russia and other countries were in fact trying to meddle in the election:

> "While Russia, China, other countries, outside groups and people are consistently trying to break through the cyber infrastructure of our governmental institutions, businesses and organizations including the Democrat [sic] National Committee, there was absolutely no effect on the outcome of the election including the fact that there was no tampering whatsoever with voting machines. There were attempts to hack the Republican National Committee, but the RNC had strong hacking defenses and the hackers were unsuccessful."[161]

Ultimately, Russian interference in the 2016 election may set the stage for a "new normal" of international interference. As the Intelligence community recently warned, "[w]e assess Moscow will apply lessons learned from its campaign aimed at the U.S. presidential election to future influence efforts in the United States and worldwide, including against U.S. allies and their election processes."[162] In a similar vein, the German government warned "there might be a Russian cyberattack on the federal election in Germany" this upcoming fall, based on the U.S. 2016 campaign troubles, and cautioned that the Bundestag itself

---

[161] *2016 Presidential Campaign Fast Facts*, CNN, January 9, 2017 1:52 PM, http://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/.

[162] David Ignatius, *Russia's Assault on America's Elections Is Just One Example Of A Global Threat*, WASHINGTON POST (February 23, 2016), https://www.washingtonpost.com/opinions/global-opinions/russias-assault-on-americas-elections-is-just-one-example-of-a-global-threat/2017/02/23/3a3dca7e-fa16-11e6-9845-576c69081518_story.html.

was "the focus of Russian intelligence interest."[163]

C. New Challenges

On February 27, 1968 renowned CBS news anchor Walter Cronkite, recently back from witnessing the destruction caused by the Tet Offensive in Vietnam, predicted on national television that the war would continue for years and end not in victory but rather a bloody stalemate.[164] President Johnson was stunned by Cronkite's pronouncement and declared "If I've lost Walter, I've lost middle America."[165] Putting aside the often cantankerous relationship between the current administration and large segments of the media, it is improbable, given the explosion of digital media in the past two decades, that a sitting president will ever again divine policy through the medium of a single albeit respected journalist.

The digital age has flattened communication; today the "Twitter in Chief" bypasses traditional news outlets and speaks out directly via his Twitter account.[166] Yet flattened communication is no panacea for a republic that requires well-informed citizens. Approximately 88% of Millennials get their news from Facebook, and due to the methodology of the Facebook newsfeed algorithm, users tend to receive more new stories similar to ones they clicked on in the

---

[163] *Id.*

[164] Peter W. Morgan, *The Undefined Crime of Lying to Congress: Ethics Reform and the Rule of Law*, 86 NW. U. L. REV. 177, 232 (1992).

[165] *Id.*

[166] See generally Amanda Wills and Alysha Love, *All the President's tweets*, CNN (February 26, 2017 6:42 AM), http://www.cnn.com/interactive/2017/politics/trump-tweets/.

past.[167] Unfortunately, this limited algorithm is built to please users; individuals only encounter biased "news" with which they are predisposed to agree. Ultimately, greater numbers of Millennials are consuming news in an "echo chamber," and that does not bode well for democracy. Many of the Founders – Jefferson, Madison, and Adams – believed a well-informed citizenry was essential for perpetuation of the American experiment.[168] In today's world, *Federalist 10* would appear on some newsfeeds but not others; Millennials, and indeed all generations, deserve better. A study of digital news consumers before the 2016 election revealed Democrats were more likely to visit left-leaning outlets like Daily Kos and The Huffington Post while Republicans visited conservative-aligned outlets like Fox News and Breitbart far more often than Democrats.[169]

The global village that was once the Internet has been replaced by digital islands of isolation that are grouping certain users while driving other users farther apart.[170] From parochial newsfeeds to tailored experiences on Google Search, the user experience is becoming increasingly personalized and the Internet a community of self-segregators.

---

[167] Anna Johansson, *5 Ways Millennial Social Media Habits Will Change In 2017*, FORBES, (November 29, 2016 2:36 PM), https://www.forbes.com/sites/under30network/2016/11/29/5-ways-millennial-social-media-habits-will-change-in-2017/#5f7f43be3219.
[168] Sandra Day O'Connor, *The Rule of Law and Civic Education Foreword* 67 SMU L. REV. 693, 699 (2014).
[169] Brendan Nyhan, Relatively Few Americans Live in Partisan Media Bubble, but They're Influential, N.Y. TIMES September 7, 2016, https://www.nytimes.com/2016/09/08/upshot/relatively-few-people-are-partisan-news-consumers-but-theyre-influential.html.
[170] Mostafa M. El-Bermawy, *Your Filter Bubble Is Destroying Democracy*, WIRED, (November 18, 2916 5:45 AM), https://www.wired.com/2016/11/filter-bubble-destroying-democracy.

V. CONCLUSION

There is a certain irony to be found in the fact that the internet, which allows almost unlimited access to information, has in practicality come to be utilized in a fashion where the users very often simply inhabit echo chambers of like-minded thought. In some ways, this may be because the sheer amount of information available is overwhelming and therefor unwieldy. Effectively sifting through the internet to correctly identify reputable sources representing diverse points of view is very difficult and requires time and a certain level of sophistication.

The 2000 and 2016 elections are apt bookends for an investigation into how the digital world has changed what it means to be an informed citizen. For all the concern about "Y2K," the world of the 2000 election was largely analog. Put differently, 2000 was as much ancient regime as it was a harbinger of things to come. From the perspective of 2017, technology offers so much to both the nation and the peoples of the world. It is no mere platitude to say the future is here but it is not equally distributed. How long would dictators remain enthroned in North Korea if the average inhabitant had unfettered access to the Internet? How might the Grameen Bank become widely digitized and help millions escape the bonds of poverty? Closer to home, citizens should not be blithely unaware of the dramatic changes technology has brought to their lives. It is unfortunate to see a family at a restaurant, together but not communing, the head of each member bent over a device and thumbs busily tapping out work e-mails or clicking on the latest viral YouTube video. Technology can sometimes be too ever-present. Most importantly, citizens must remember that the connected world has definite currents that tend to bind some groups and isolate others. For the Republic to stand, users must

reorganize the Internet to some degree according to principles of responsible citizenship. It is insufficient to protect e-votes from hacking; ballots must be cast from an informed position.

Is Uncle Sam Stalking You? Abandoning Warrantless Electronic Surveillance to Preclude Intrusive Government Searches

J. Alexandra Bruce*

ABSTRACT

The Founders drafted the Fourth Amendment foreseeing immense governmental abuse likely to stem from intrusive, unlimited searches. The Fourth Amendment bars any government investigative efforts absent a warrant grounded in a showing of probable cause. Further, the Fourth Amendment specifically protects the "papers" of U.S. citizens. This is interpreted to extend to all private communication whether conducted through traditional or electronic channels.

This article argues the Fourth Amendment mandates oversight in all surveillance conducted by the intelligence community. Administrations have made continuous efforts to conduct massive collections of electronic data—including private communications of U.S. citizens—without obtaining a warrant. The foreign surveillance exception was recognized to provide the Executive with an exception to the Fourth Amendment's warrant requirement where the investigation was centered on national security. The numerous abuses stemming from the recognition of an

* *J. Alexandra Bruce* author graduated *summa cum laude* from The University of Mississippi School of Law in 2017 and serves as a judicial law clerk to the Honorable Rhesa H. Barkesdale of the United States Fifth Circuit Court of Appeals for the 2017-2018 term. The author wishes to thank Professor Ronald Rychlak for his integral role in developing this Article. Additionally, the author would like to thank her mother, Elisa Bruce, for her continued support and encouragement in academic endeavors.

exception, led Congress to draft the Federal Intelligence Surveillance Act. This statute mandated judiciary and legislative oversight of the Executive's previously unchecked power to conduct intelligence surveillance.

This article is the first to consider completely abandoning the foreign intelligence exception, to maintain all national security electronic surveillance with the oversight of the Federal International Surveillance Court.

The Federal International Surveillance Court, organized through FISA, provides a tribunal for an independent judiciary to consider the constitutionality of the intelligence community's electronic surveillance procedures. The court scrutinizes the particular intelligence purpose; the reasonableness of the surveillance; and maintains minimization procedures.

This article scrutinizes the constitutionally problematic investigations rendered through warrantless searches. Lastly, the article provides evidence to demonstrate vulnerable privacy rights best preserved by foregoing the problematic "foreign intelligence exception" to subject all searches—even those centered on the security of the nation— to the oversight of a neutral judiciary.

INTRODUCTION

There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time.[1]

George Orwell

[1] George Orwell, *1984,* 1 (1949).

For decades the courts and legislature have grappled over the appropriate balance of the preservation of constitutionally protected privacy rights and national security intelligence surveillance.[2] Despite the Fourth Amendment's clear preference for warrants,[3] administrations have repeatedly employed electronic surveillance—absent a warrant— for the purported goal of obtaining national security intelligence.[4] Conflicts in the Government's right to protect the security of the nation and citizens' rights to privacy continue to frustrate the legal system.[5]

Insufficient standards for constitutional intelligence gathering and immense opportunity for unreasonable investigatory searches generated by the "foreign intelligence

---

[2] *See generally*, *U.S. v. U.S. Dist. Court for the Eastern Dist. of Mich. (Keith),* 407 U.S 297, 314–15 (1972) (holding "As the Fourth Amendment is not absolute in its terms, our task is to examine and balance the basic values at stake in this case: the duty of Government to protect the domestic security, and the potential danger posed by unreasonable surveillance to individual privacy and free expression.").

[3] State v. Edman, 281 Conn. 444, 454 (Conn. Feb. 27, 2007) (discussing "both the state and federal constitution evince a preference for obtaining search warrants to protect the individual rights of our citizens. '[I]t is a cardinal principle that searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable . . . subject only to a few specifically established and well-delineated exceptions.'") (citing *Mincey* v. *Arizona*, 437 U.S. 385, 390 (1978); *Katz* v. *United States*, 389 U.S. 347, 357 (1967)).

[4] *Keith*, 407 U.S. at 311 n.10. (citing Br. for Pet'r at 16-18; Br. for Resp't at 51-56; 117 Cong. Rec. 14056.).

[5] *See generally*, *Keith,* 407 U.S. at 297; *see also* James E. Meason, *The Foreign Intelligence Surveillance Act: Time for Reappraisal*, 24 Int'l Law. 1043 (1990) (hereafter "24 Int'l Law"); *see also* 50 U.S.C.A. § 1801 (West 2015); *see also* ACLU v. NSA, 438 F. Supp. 2d 754 (E.D. Mich. 2006); In re. Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1006 (FISA Ct. Rev. 2008).

exception"[6] encouraged the passing of the 1978 Foreign Surveillance Act (FISA).[7] Centered on facilitating efficient intelligence gathering and preserving citizens' constitutional privacy rights,[8] FISA designed a court to administer warrants in the unique circumstances of foreign intelligence surveillance.[9] The Foreign Intelligence Surveillance Court (FISC), provides a judicial oversight procedure sufficient to satisfy the Fourth Amendment's reasonableness mandate — the process is considered a "warrant within the meaning of the Fourth Amendment"[10]—the court administers these "warrants" for the majority of the Government's FISA surveillance efforts.[11] The FISA was drafted with the intention of structuring a procedure to enforce judicial

[6] *Keith*, 407 U.S. 297; *see also* Nola K. Breglio, *Leaving Fisa Behind: The Need to Return to Warrantless Foreign Intelligence Surveillance*, 113 Yale L.J. 179 (2003) (stating "The foreign intelligence exception [] remained a large window for *totally unsupervised* government surveillance.").
[7] Rep. No. 604, 95th Cong., 1st Sess. at 7 (1977); *see also* S. REP. 95-604(I).
[8] Alan Butler, *Standing Up to Clapper: How to Increase Transparency and Oversight of Fisa Surveillance*, 48 New Eng. L. Rev. 55 (2013).
[9] S. REP. 95-604(I).
[10] United States v. Megahey, 553 F. Supp. 1180, 1190 (E.D.N.Y. Dec. 1, 1982) ("[T]he FISA warrant is a warrant within the meaning of the Fourth Amendment, since it provides for the interposition of independent judicial magistrates between the executive and the subject of the surveillance which the warrant requirement was designed to assure.").
[11] Butler, *supra* note 8 at 55.

oversight and maintain the limitations of the Fourth Amendment.[12]

The Supreme Court holds "warrantless electronic surveillance" proves unreasonably intrusive, and extends beyond what is constitutionally permitted by the Fourth Amendment.[13] Though the Court's holding was clear that criminal investigations employing warrantless electronic surveillance proved unconstitutionally intrusive, the Court left open the question of whether or not an exception existed for investigations centered on national security threats.[14]

This article argues that the FISC should not only be maintained, but continue as the sole remedy for the Government to obtain approval of electronic national security surveillance. The prevailing constitutional validity provided through FISC-approved investigations is conveyed through both Court precedent— holding warrantless searches unreasonable even where conducted for national security[15]— and the overwhelming post FISA opinions

---

[12] United States v. Duggan, 743 F.2d 59, 73 (2d Cir. N.Y. Aug. 8, 1984) ("The procedural safeguards laid out in the Act 'are necessary to insure that electronic surveillance by the U.S. Government within this country conforms to the fundamental principles of the Fourth Amendment.'") (citing S. Rep. No. 701, 95th Cong., 2d Sess. 13, *reprinted in* 1978 U.S. Code Cong. & Ad. News 3973, 3982 ("Senate Report 95-701")).

[13] *Katz*, 389 U.S. at 347 (1967).

[14] "Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case." *Id.* at 358 n.23.

[15] *See generally*, *Katz*, 389 U.S. at 347 (1967); *see also Keith*, 407 U.S. at 297, 314–15 (1972); *but see Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980).

holding the FISC and FISA procedures constitutionally sound.[16]

Previous articles have argued "warrant-free" intelligence procedures prove more effective, and more protective of the target's Fourth Amendment rights.[17] Similarly, articles find that the targets of these warrantless investigations are better suited to challenge the searches' reasonableness "after the fact in normal Article III courts."[18]

This article argues completely foregoing constitutionally prohibited warrantless searches—even within the delicate climate of national security threats—to rely solely on FISC approved electronic surveillance and

---

[16] *See generally,* United States v. Abu-Jihaad, 630 F.3d 102, 120 (2d Cir. 2010); *see also* United States v. Ning Wen, 477 F.3d 896, 898 (7th Cir. 2007); *see also* United States v. Damrah, 412 F.3d 618, 625 (6th Cir. 2005); *see also* In re Sealed Case, 310 F.3d at 742–46; United States v. Johnson, 952 F.2d 565, 573 (1st Cir. 1991); United States v. Pelton, 835 F.2d 1067, 1075 (4th Cir. 1987); United States v. Cavanagh, 807 F.2d 787, 790–92 (9th Cir. 1987); United States v. Kashmiri, No. 09 Cr. 830–4, 2010 WL 4705159, at 3–5 (N.D. Ill. Nov.10, 2010); United States v. Warsame, 547 F.Supp.2d 982, 993 (D. Minn. 2008); United States v. Mubayyid, 521 F.Supp.2d 125, 135–41 (D. Mass. 2007); United States v. Holy Land Found. for Relief & Dev., No. 04 Cr. 240, 2007 WL 2011319, at 5–6 (N.D. Tex. July 11, 2007); United States v. Jayyousi, No. 04 Cr. 60001, 2007 WL 851278, at 1 (S.D. Fla. Mar.15, 2007); United States v. Benkahla, 437 F.Supp.2d 541, 554 (E.D. Va. 2006); United States v. Marzook, 435 F.Supp.2d 778, 786 (N.D. Ill. 2006); United States v. Nicholson, 955 F.Supp. 588, 590–91 (E.D. Va. 1997); In re Kevork, 634 F.Supp. 1002, 1014 (C.D. Cal. 1985); United States v. Falvey, 540 F.Supp. 1306, 1312 (E.D.N.Y. 1982).

[17] Breglio, *supra* note 6 (arguing to "revive the constitutional viability of foreign intelligence surveillance [by] forego[ing] the FISA warrant procedure entirely"); *see also* Carol M. Bast (FNd1) & Cynthia A. Brown, *A Contagion of Fear: Post-9/11 Alarm Expands Executive Branch Authority and Sanctions Prosecutorial Exploitation of America's Privacy*, 13 Cardozo Pub. L. Pol'y & Ethics J. 361 (2015) (arguing, "under FISA and the contagion of fear of terrorism is a lethal combination leading to an almost necessary loss of protection for civil liberties.").

[18] Breglio, *supra* note 6.

intelligence gathering procedures. The first section considers the FISC's efficiency through scrutiny of the court's ability to preserve both the Fourth Amendment's clear prohibition of warrantless searches, and encourage efficient foreign intelligence gathering procedures. The second section argues the FISC proves sound public policy by serving to better preserve civil liberties, vulnerable to increased security threats. The third section considers the Executive overreach procured through the FISC's oversight and scrutiny of intelligence operations.

In conclusion, the FISC is demonstrated to serve as the most effective to combat the constitutionally problematic nature of balancing the Government's right to protect the nation, and citizens' constitutionally protected privacy rights.[19] Additionally, modifications to the court's structure to increase judicial oversight, and a complete abandonment of the foreign intelligence exception will be explored as the most effective mode for the preservation of civil liberties.

I. BACKGROUND OF THE FISA COURT

Prior to the drafting of the Federal Intelligence Surveillance Act (FISA), the Executive's constitutional authority to protect the nation was interpreted to accord an "inherent power" to conduct warrantless searches

[19] *Duggan*, 743 F.2d at 74 (finding that FISA procedures "provide an appropriate balance between the individual's interest in privacy and the government's need to obtain foreign intelligence information"); *see also Pelton*, 835 F.2d at 1075 ("FISA's numerous safeguards provide sufficient protection for the rights guaranteed by the Fourth Amendment").

purportedly sustained for national security purposes.[20] These Government-orchestrated intelligence gathering efforts were argued as "reasonable" under the theory the President and Attorney General sustain an exemption to the Fourth Amendment when working to protect the nation's security.[21] The abuse inherent to this exemption is conveyed through the "sixty-five thousand *domestic* intelligence investigations" that were conducted by the FBI —absent obtaining a warrant or judicial oversight— within just one year.[22]

These Government actions offend the intention of the Fourth Amendment's limitations on intrusive Executive power obtained through unreasonable searches.[23] A regimen of unchecked Executive actions to carry out warrantless

---

[20] Br. for Resp't at 30, *Keith*, 407 U.S. at 297 (1972) (No.135521); *see also Duggan*, 743 F.2d at 72; *See also Truong*, 629 F.2d at 912-14, *cert. denied*, 454 U.S. 1144 (1982); *see also* United States v. Buck, 548 F.2d 871, 875 (9th Cir.), *cert. denied*, 434 U.S. 890 (1977); United States v. Butenko, 494 F.2d 593, 605 (3d Cir.) (*en banc), cert. denied*, 419 U.S. 881 (1974); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974); *but see* Zweibon v. Mitchell, 516 F.2d 594, 633-651 (D.C. Cir. 1975), (dictum), *cert. denied*, 425 U.S. 944 (1976).

[21] *Duggan*, 743 F.2d at 59, 72 ("Prior to the enactment of FISA, virtually every court that had addressed the issue had concluded that the President had the inherent power to conduct warrantless electronic surveillance to collect foreign intelligence information, and that such surveillances constituted an exception to the warrant requirement of the Fourth Amendment."); *see also Keith,* 407 U.S. at 301 ("the Government argued the warrantless electronic surveillance was lawful as a "reasonable exercise of Presidential power."); *see also Truong*, 629 F.2d at 908.

[22] SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, BOOK II: INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755 at IV, V (1976), available at https://www.intelligence.senate.gov/sites/default/files/94755_II.pdf.

[23] *See* Br. for Resp't, *supra* note 4 at 12 (citing Boyd v. United States, 116 U.S. 616, 635 (1885)); Marcus v. Search Warrant, 367 U.S. 717 (1961); Stanford v. Texas, 379 U.S. 476 (1965).

searches amounts to the "hallmark of a police state."[24] Watergate exposed the nation to the abuse possible where the Executive is left unchecked.[25] This led to judicial and legislative action reigning in, previously unrestrained, Executive intelligence efforts.[26]

In 1972, the Supreme Court considered the constitutionality of domestic intelligence gathering methods.[27] Writing for the majority, Justice Powell held that warrantless *domestic* surveillance, absent prior judicial approval, failed to maintain the reasonableness standard mandated by the Fourth Amendment.[28] The decision narrowly considered solely "internal security matters," avoiding any determination of the Executive's power to investigate the "activities of foreign powers or their agents" absent a warrant.[29] Consequentially, the Executive remained uncertain of the constitutionality of its efforts to obtain foreign intelligence.[30]

The legislature's drafting of FISA was in response to Congressional awareness of the Intelligence Community's increased encroachment on Americans' civil liberties.[31] The Church Committee—a Senate committee organized to investigate unconstitutional intelligence gathering schemes—discovered abuses including "warrantless break-

---

[24] *See* Br. for Resp't, *supra* note 16 at 12 (citing Shuttlesworth v. Birmingham, 382 U.S. 87 (1969)).
[25] *See* 24 Int'l Law. at 1043.
[26] *See generally*, Breglio, *supra* note 5 at 7; *see also* 24 Int'l Law. at1043.
[27] *Keith,* 407 U.S. at 310.
[28] *See Id.* (holding the "Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive.").
[29] *See Id.*, at 322.
[30] *See generally*, Breglio, *supra* note 6 at 7; *see also* 24 Int'l Law. 1043.
[31] Assistant Attorney General John P. Carlin Delivers Opening Remarks at the National Security Division 10 Year Anniversary Conference, JUSTICE NEWS (Dep't of Just.), Sep. 14, 2016.

ins, excessive surveillance of politically "subversive" groups, and indiscriminate opening of citizens' mail."[32] The Committees findings led Congress to draft FISA, reigning in the Executive's broad intelligence gathering powers and mandating legislative and judicial oversight of the Executive's investigative schemes.[33] American's civil liberties remain vulnerable today as warrantless searches remain valid under the "foreign intelligence exception."[34] Reasonable, constitutionally valid search efforts demand judicial oversight to properly protect American's constitutional privacy rights.

A. The FISC Proves Necessary to Prevent Unreasonably Intrusive Electronic Surveillance

The Supreme Court holds "individual freedoms" most effectively preserved through judicially administered warrants.[35] Further, intelligence gathering efforts' require balancing "the legitimate need to safeguard domestic security" and the harm of impeding on "individual privacy and free expression."[36] The fear of the "erosion of our sense of privacy and independence" was held to far outweigh the fear that "upheaval will modify our form of government."[37]

Prior to the passing of FISA, warrantless investigations were employed by numerous administrations

---

[32] *Id.*
[33] *Id.*; *see also* 24 Int'l Law. at 1043.
[34] *In re Directives*, 551 F.3d at 1013.
[35] Redacted, 2011 WL 10945618 at 26 (Foreign Intel. Surv. Ct. Oct. 3, 2011).
[36] *Keith,* 407 U.S. at 314.
[37] *Id*.

for the purported purpose of protecting national security.[38] Since the 1940s, administrations have exploited the preservation of national security to conduct intrusive surveillance efforts, void of judicial oversight.[39] Administrations employing these "warrantless wiretapping activities" did not consider the failure to obtain a warrant a bar to the pursuit of criminal prosecution.[40] The targets of these constitutionally invalid searches were prosecuted with evidence obtained through the warrantless investigations.[41]

Through the passing of FISA, Congress orchestrated the Federal Intelligence Surveillance Court.[42] This Article III court is composed of 11 U.S. district judges, maintaining the power to grant approval for particular electronic surveillance efforts where the government maintains "probable cause to believe" the targets of their surveillance efforts are "foreign power[s] or agent[s] of a foreign power."[43]

FISA's specific inclusion of an "agent of a foreign power" affords opportunity for the oversight of electronic surveillance, targeted at U.S. citizens.[44] An "agent of a

---

[38] *See Keith,* 407 U.S. at 314*; see also Katz*, 389 U.S. at 364 (Justice White concurring) ("Wiretapping to protect the security of the Nation has been authorized by successive Presidents…We should not require the warrant procedure and the magistrate's judgment if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable.").

[39] *Keith*, 407 U.S. at 311 n.10 (Past administrations have employed electronic surveillance in cases concerning organized crime and other various "domestic security cases" since at least 1946.) (citing Br. for Pet'r 16-18; Br. for Resp't 51-56; 117 Cong. Rec. 14056.).

[40] Br. for Resp't, *supra* note 15 at 100.

[41] *Id*.

[42] 50 U.S.C.A. § 1801 (West).

[43] *See* Br. for Pet'r at n.1*,* Wikimedia Foundation v. NSA (2015) (No. 5025551) (citing 50 U.S.C. § 1803(a); In re Motion for Release of Court Records, 526 F. Supp. 2d 484, 486 (F.I.S.C. 2007)); *see also In re Sealed*, 310 F.3d at 722 (citing 50 U.S.C. § 1805(a)(3)).

[44] *See* Br. for Pet'r, *supra* note 35 (citing 50 U.S.C. § 1805(e)(1)).

foreign power" includes U.S. citizens who "knowingly engage in clandestine intelligence gathering activities" or "knowingly engages in sabotage or international terrorism, or activities that are in preparation thereof."[45] Though the FISC presents an opportunity for the government to obtain judicial approval to conduct investigations with a less stringent standard of probable cause,[46] judicial approval remains necessary.[47]

1. The Foreign Intelligence Exception is Insufficient to Constitutionally Maintain Electronic Foreign Intelligence Surveillance

The Court has acknowledged the "legitimate need" for intelligence gathering through electronic surveillance,[48] yet failed to expressly determine what foreign surveillance actions maintain constitutional validity.[49] The lack of Court precedent led various circuit courts to find a "foreign intelligence exception" rendering the recognition of the Government exemption from the Fourth Amendment's Warrant Clause.[50]

---

[45] *See Id*. (citing 50 U.S.C. § 1805(b)(2)(A)).
[46] 50 U.S.C. § 1805(a)(3)(A)(2000).
[47] *Id*.
[48] *See generally, Katz,* 389 U.S. at 347.
[49] *Keith,* 407 U.S. at 297, 314. (Holding that "prior judicial approval" was necessary for the type of surveillance in the particular case and that the mandate on warrants for searches applies solely to domestic investigations and intelligence gathering); *see also Katz*, 389 U.S. at 347.
[50] *See* United States v. Butenko, 494 F.2d 593, 608 (3d Cir. 1974); *see also Truong*, 629 F.2d at 913-16; *see also* United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973); *see also* United States v. Buck, 548 F.2d 871, 875 (9th Cir. 1977).

Courts recognizing the foreign surveillance exception to the general warrant requirement cited the "procedural hurdle" that could potentially hinder vital national security investigations.[51] Additionally, the opinions convey an overall concern that the judiciary lacks the necessary knowledge to make determinations regarding appropriate foreign intelligence measures.[52] This exception is considered appropriate only where the executive conveys the particular surveillance is administered "'primarily for foreign intelligence reasons."[53] This presents both procedural and prosecutorial burdens, as should it be determined the particular investigation was "primarily a criminal investigation," all evidence discovered through the warrantless procedure will be appropriately excluded.[54]

2. The FISC Approved Foreign Surveillance Efforts are Sustained within the Limitations of the Fourth Amendment

The judiciary considers the "totality of the circumstances" in order to determine whether or not a particular search effort maintains the reasonableness mandated by the Fourth Amendment.[55] When employing this analysis, the judiciary considers the "nature of the government intrusion and how the intrusion is

---

[51] *Truong*, 629 F.2d at 913.
[52] *See Id.* (arguing, "the judiciary is largely inexperienced in making the delicate and complex decisions that lie behind foreign intelligence surveillance.").
[53] *See Id.*
[54] *Truong*, 629 F.2d at 913.
[55] *See In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1012 (Foreign Int. Surv. Ct. Rev. 2008) (citing Samson v. California, 547 U.S. 843, 848, 126 S.Ct. 2193, 165 L.Ed.2d 250 (2006); Tennessee v. Garner, 471 U.S. 1, 8–9, 105 S.Ct. 1694, 85 L.Ed.2d 1 (1985)).

implemented."[56] This is particularly influential in intelligence gathering efforts targeted at national security. Courts have consistently struggled to balance the constitutional limitations and the necessity of national security, as more intrusive search efforts are permitted where the government's interest in conducting a search holds greater importance and preserving national security is of "the highest order of magnitude."[57]

The lacking specificity of the foreign surveillance exception resulted in sizable opportunities for unrestrained surveillance.[58] Concerned for the lacking standards in foreign surveillance and opportunity for intrusive, constitutionally invalid searches, Congress considered statutory procedures to procure constitutionally invalid surveillance, while securing foreign intelligence.[59]

Recognizing the constitutional abuses inherent to unchecked Executive surveillance capability, Congress extended the Fourth Amendment's protection against unreasonable searches to intelligence gathering.[60] With the passing of FISA, Congress took an active role in scrutinizing the Executive's national security investigation techniques.[61] Additionally, when considering the "inconvenience" judicial approval imposes on the Attorney General's ability to investigate national security matters, the Court has held it "justified in a free society to protect constitutional values."[62]

---

[56] *See In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d at 1012.
[57] *See In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d at 1012.
[58] *See* Breglio, *supra* note 6 at 7.
[59] S. REP. 95-604(I).
[60] 24 Int'l Law. at 1043.
[61] *See Id.*
[62] *Keith,* 407 U.S. at 301.

B. FISA Provides for Efficient Foreign Surveillance While Preserving Civil Liberties

In 1978, Congress passed FISA with the intention of "provid[ing] further safeguards for individuals subjected to electronic surveillance."[63] This Act served to maintain a level of judicial oversight of foreign intelligence gathering in order to preserve vulnerable civil liberties, while maintaining the flexibility necessary in these particular investigations.[64] The Act provided for the designation of judges to consider these specific foreign intelligence surveillance efforts.[65] These judges make up the Foreign Intelligence Surveillance Court (FISC), which serves to authorize a majority of the government's FISA surveillance efforts.[66]

The FISC considers the government's methods for foreign intelligence gathering, and determines whether or not the actions comply with the Fourth Amendment.[67] FISA explicitly forbids "contents of any communication to which a United States person is a party . . . be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person."[68] The legislation is centered on facilitating effective gathering of crucial intelligence while

---

[63] S. REP. NO. 95-604(I).
[64] *See* Breglio, *supra* note 6 at 7.
[65] *See generally*, S. REP. NO. 95-604(I).
[66] *See* Butler, *supra* note 8 at 55.
[67] *See* 50 U.S.C.A. § 1881(a) (West).
[68] 50 U.S.C.A. § 1801(h)(4) (West).

protecting Americans' privacy rights.[69] Additionally, FISA has proven successful in prosecuting individuals discovered to be actively involved in carrying out acts of terrorism against the United States.[70]

The FISC is criticized as insufficiently balancing the privacy rights of U.S. citizens and the vital need for homeland security surveillance,[71] yet this court serves as the only government body with power to administer any judicial oversight. Arguments for the abolition of the FISC largely ignore the immense lack of protections available to defendants subjected to warrantless searches that are conducted absent any judicial oversight.[72]

C. Judicial Approval through FISC Accords the Government Certainty that their Efforts Maintain Constitutionality and Evidence Obtained Will Not be Subject to Exclusion

FISA created a judicial procedure to oversee surveillance efforts and reign in unreasonable investigations utilized by the intelligence community.[73] The court, organized within FISA, acts independently "to review requests from intelligence professionals about tools or

---

[69] Senate leaders clarify the intentions of the legislation as creating a "more explicit…statutory intent, as well as to provide further safeguards for individuals subjected to electronic surveillance." S. REP. NO. 95-604(I).
[70] *See generally*, United States v. Rahman, 861 F. Supp. 247, 250 (S.D.N.Y. 1994), *aff'd*, 189 F.3d 88 (2d Cir. 1999).
[71] Breglio, *supra* note 6 at 185.
[72] Breglio, *supra* note 6 at 186 (noting the opportunity for "*totally unsupervised* government surveillance" under the foreign surveillance exception) (emphasis added).
[73] 50 U.S.C.A. § 1801 (West).

tactics that they intend to employ."[74] The intelligence community is subject to additional congressional oversight under FISA mandates.[75]

Following the September 11, 2001 terrorist attacks, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("PATRIOT ACT") to expand and improve the nation's homeland security endeavors.[76] The Act expanded FISA and its function in monitoring foreign surveillance.[77] Specifically, the PATRIOT ACT altered the standard for obtaining a FISA warrant from demonstrating "the purpose" of the investigation to be the procurement of foreign intelligence, to only a government showing that the "significant purpose" of the investigation is collecting foreign intelligence.[78]

The mere addition of the word "significant" provided the government with greater liberty to use information obtained through a FISA warrant in criminal prosecutions.[79] These changes have been heavily criticized as leaving defendants "virtually powerless to challenge the legitimacy of any such evidence."[80] Additionally, those parties who are investigated through FISA approved intelligence gathering

---

[74] PRESS BRIEFING BY PRESS SECRETARY JOSH EARNEST, 2016 WL 5844916, at 3, 120 (Oct. 5, 2016).
[75] *Id.*; *see* 50 U.S.C. § 1801; *see also Attorney General Loretta E. Lynch Delivers Keynote Address on Counterterrorism and International Cooperation*, JUSTICE NEWS (Dep't of Just.) Dec. 19, 2015; Butler, *supra* note 8 at 55.
[76] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272. (2001).
[77] *Id.*
[78] *Id.* (striking the Foreign Intelligence Surveillance Act of 1978's language, "'the purpose' and inserting 'a significant purpose'").
[79] Breglio, *supra* note 6 at 15.
[80] *Id.*

procedures are able to challenge these searches in the FISC.[81]

II. THE FISC IS ESSENTIAL FOR ELECTRONIC INTELLIGENCE GATHERING METHODS TO MAINTAIN CONSTITUTIONALITY

Courts have struggled with the constitutionality of electronic surveillance for nearly a century. In the early 1900s, the United States Supreme Court analyzed the Fourth Amendment's limitations on the Government's ability to conduct investigations through wiretapping.[82] In his dissent, Justice Brandeis recognized the harmful reality of unreasonable searches stemming from validation of Government efforts to intercept private citizens' communications.[83] Justice Brandeis' ominous dissent considers the probability that intrusive investigations would "not likely [] stop with wiretapping" to eventually lead to government intrusion into multiple facets of Americans' personal lives.[84]

Over eighty years after Justice Brandeis' *Olmstead* dissent, a National Security Agency (NSA) electronic data collection procedure was challenged as effectively allowing a "government agent [to] open every letter that comes

---

[81] *See In re Directives Pursuant to Sec. 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1006 (FISA Ct. Rev. 2008).
[82] Olmstead v. United States, 277 U.S. 438, 474 (1928).
[83] *Id.*
[84] In his dissent, Brandeis predicts the current difficulties surrounding the constitutionality of foreign surveillance efforts through interceptions of internet data. Brandeis states, "[w]ays may someday be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home." *Id.* at 473.

through a mail processing center to read its contents before determining which letters to keep."[85] The constitutional obstructions extending from unchecked Executive power to employ electronic investigations is congruent with America's ever expanding dependence on electronic communication.

A. Increased Electronic Communication and National Security Threats Proves FISA a Sound Public Policy

The digital economy and Americans' economic and societal dependence on electronic communication continues to rapidly expand.[86] Increases in electronic communications have perpetuated the NSA's elaborate schemes, using the newest technologies to intercept communications and gather intelligence worldwide.[87] With every aspect of American life currently touched by electronic communication,[88] there is an even greater need for judicial oversight in these intelligence-gathering efforts.[89]

Arguing that the necessity to "protect the country" promulgates a presidential power to conduct warrantless investigations of both "agents of foreign powers" and

---

[85] Brief for Petitioner at 1–2, Wikimedia Found. v. Nat'l Sec. Agency (2016) (No. 703452).
[86] *See generally*, J. Alexandra Bruce, *A Billion Dollar Investment: The Profitability of Modifying the Current Energy Regulations to Secure the Nation's Energy Supply*, 17 Appalachian J.L. (2017).
[87] Meason, *supra* note 6.
[88] Bruce, *supra* note 82.
[89] Though Silicon Valley innovators did not create technologies "so that people who want to harm innocent people can be more violent," but rather because of their commitment to "making people freer to communicate or express their views," terrorist organizations have employed social media to "propagate their hateful ideology." Earnest, *supra* note 74 at 3.

"domestic organization[s],"[90] the Government contends warrantless searches, orchestrated by the Executive, prove reasonable when undergone to protect the security of the nation.[91] Considering the government's efforts to secure unchecked power for gathering intelligence through electronic surveillance, and Americans' increased use of electronic communications, it is vital that judicial oversight into these intrusive searches be maintained and strengthened.[92]

FISA, and the government actors working to implement FISA, have continued to generate "effective and civil liberties-protective foreign intelligence collection in the digital age."[93] Modifications to FISA and its regulatory agents have coincided with the immense evolution of communication and modes of organizing terrorist activity.[94]

Increasingly innovative forms of communication within the United States induced the intelligence and tech communities to coordinate efforts.[95] While maintaining both "statutory and constitutional limits," these newly created entities facilitate "intelligence collection authorities that enable critical FBI counterintelligence and counterterrorism investigations."[96] Nonetheless, these

---

[90] *Id*.
[91] Brief for Petitioner at 2, *U.S. Dist. Court for the Eastern Dist. of Mich.* (*Keith*), 407 U.S. 297 (1972) (No. 135522).
[92] Brief for Petitioner at 2, *U.S. Dist. Court for the Eastern Dist. of Mich.* (*Keith*), 407 U.S. 297 (1972) (No. 135522).
[93] Assistant Attorney General John P. Carlin Delivers Opening Remarks at the National Security Division 10 Year Anniversary Conference, JUSTICE NEWS (Dep't of Just.), Sep. 14, 2016.
[94] *Id*.
[95] Earnest, *supra* note 70 at 3.
[96] Carlin, *supra* note 93.

innovative communications prove to be both constitutionally protected free speech and private speech.[97]

In 2016, the Government worked with Twitter to shut down extremists employing the channel to propagate their message and "radicalize people."[98] The continued cooperation of these entities, with competing interests, is vital to the future of intelligence gathering. The tech community is committed to innovation that increases the freedom of expression and ideas, whereas the Government is committed to protecting the nation from increased vulnerability to foreign terrorist organizations.[99]

The balance of national security and free communication is effectively considered where these two communities cooperate.[100] Continuing oversight of electronic investigations, while including necessary private-sector parties, is essential to protecting vulnerable privacy rights and national security.

1. FISA's Internal Review Process Provides Accountability

Protection of civil liberties, and the continued intelligence efforts necessary to homeland security, proved

---

[97] "The First Amendment protects anonymous online speech, which can be as necessary to democratic self-governance as the anonymous pamphlets our Founders wrote." Brief for Petitioner, *supra* note 87, at 5 (citing Reno v. American Civil Liberties Union, 521 U.S. 844, 870 (1997); Taylor v. John Does, 1-10, 2014 WL 1870733, at 2 (E.D.N.C. May 8, 2014).
[98] Earnest, *supra* note 70, at 3.
[99] *Id*.
[100] *Id*.

the central purpose for FISA.[101] The NSA has utilized the FISC to aide in their efforts to internally police their practices, and remain within constitutional limits.[102] Additionally, the FISC has conveyed a direct effort to be a greater force than merely a "rubber stamp" for any surveillance sought by the government.[103] The court has determined various government practices to be illegally conducted outside the limits of the Fourth Amendment.[104]

The Department of Justice (DOJ) reports that the average time necessary to maintain FISA approval for gathering business records is 115 days.[105] FBI Agents, disproportionately those orchestrating cyber investigations, describe the FISC approval process as "lengthy," and criticized the procedural burdens as having a "negative impact on their investigations."[106] In particular, those agents conducting cyber investigations have found the process to be burdensome.[107] Though these procedural limitations may

---

[101] S. REP. NO. 95-604(I) (quoting Attorney General Bell while noting "for the first time in our society the clandestine intelligence activities of our government shall be subject to the regulation and receive the positive authority of a public law for all to inspect").
[102] *In re* Prod. of Tangible Things from [Redacted], No. BR 08–13, 2009 WL 9150913, at 3 (FISA Ct. Mar. 2, 2009).
[103] *See generally*, Michael T. Francel, *Rubber-Stamping: Legislative, Executive, and Judicial Responses to Critiques of the Foreign Intelligence Surveillance Court One Year After the 2013 NSA Leaks*, 66 Admin. L. Rev. 409 (2014); *see also* Conor Clarke, *Is the Foreign Intelligence Surveillance Court Really A Rubber Stamp? Ex Parte Proceedings and the FISC Win Rate*, 66 Stan. L. Rev. Online 125 (2014).
[104] *See First Direct Evidence of Illegal Surveillance Found by the FISA Court*, WASH. POST (Oct. 12, 2011), http://apps.washingtonpost.com/g/page/national/first-direct-evidence-of-illegal-surveillance-found-by-the-fisa-court/393.
[105] *See generally*, *OJ OIG Releases Report on the FBI's Use of Section 215 of the Patriot Act*, DEP'T OF JUSTICE (September 29, 2016), https://oig.justice.gov/press/2016/2016-09-29.pdf.
[106] *Id.*
[107] *Id*.

occasionally prove burdensome to the intelligence community, these safeguards are vital as innovative technologies are employed.[108] The agents, conducting electronic surveillance, perceiving the process as burdensome, further demonstrates the procedural safeguards employed to protect the privacy rights impacted by electronic communications.

Dissimilar from pre-FISA administrations, the Obama administration pledged to center the intelligence communities' determination of proper use of new technologies on the balancing of privacy rights, while effectively avoiding attacks on the nation.[109] This continued Executive focus on the balancing of privacy rights and effective intelligence gathering, whether or not effectively carried out, further conveys the more conservative approach maintained post-FISA.

2. The FISC Provides Judicial Oversight to Prevent Prosecutorial Abuses and Executive Overreach

Prior to the passing of FISA, Congress "deferred to presidential authority" for decisions related to intelligence,[110] and the legislature avoided maintaining any active role in intelligence for more than a century.[111] Without any clear limitations, the government orchestrated lawful, warrantless intelligence gathering methods for the purported endeavor of "protect[ing] national security."[112] Challenges to the admission of evidence obtained through these warrant-

---

[108] *See* Earnest, *supra* note 74, at 3.
[109] *See Id*.
[110] *See* Meason, *supra* note 83.
[111] *Id.*
[112] *Keith,* 407 U.S. at 300.

free searches, forced Government criticism of the lacking standards "to authorize national security intelligence wiretaps," and any "meaningful or appropriate guideline[s]" for constitutional surveillance.[113]

Under FISA, Executive surveillance schemes are subject to judicial and legislative oversight.[114] FISA stemmed reform of the Executive's approach to maintaining both foreign and domestic electronic surveillance. Dissimilar from previous administrations' interpretation of an Executive exemption to the Fourth Amendment,[115] the Obama administration supported intelligence subject to "rigorous oversight by all three branches."[116]

B. Utilizing the Significant Purpose Test to Determine the Appropriateness of a FISA Warrant Proves Consistent with the Fourth Amendment

Overwhelmingly, the controversy surrounding the FISC, and the court's decisions are centered on recent FISA provisions expanding the legally permitted aggregate of intelligence surveillance conducted within the United States.[117] Though much criticism centers on the FISC, one of the most challenged portions of FISA is the FISA Amendments Act of 2008 (FAA), which effectively expands

---

[113] Brief for Respondent, *supra* note 16, at 3-4.
[114] 50 U.S.C.A. § 1801 (West).
[115] *See generally* Brief for Respondent, *supra* note 16.
[116] Earnest, *supra* note 70, at 3.
[117] *See* Butler, supra note 7, at 55 (citing USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. §§ 1861-62 (2006)) (citing FISA Amends. Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436, 2438 (2008) (codified as amended at 50 U.S.C. § 1881a (2006 & Supp. III 2010)).

the power of the intelligence community by suppressing the oversight power of FISA and the FISC.[118]

Though controversial, the PATRIOT Act's addition of a "significant purpose" test has been considered and determined to be within the limits of the Fourth Amendment.[119] The 3rd Circuit holds the "significant purpose" renders the government unable to obtain foreign surveillance for the "sole objective of criminal prosecution."[120] Additionally, the court determined that the government must convey a "broader objective than criminal prosecution—such as stopping an ongoing conspiracy—and includes other potential non-prosecutorial responses" in order to maintain the "significant purpose" necessary to obtain a FISA warrant.[121]

FISA's implementation of the "significant purpose" test proves more protective of individual rights than an unchecked foreign intelligence exception. Prior to the creation of the FISC, the Government maintained evidence procured through warrantless foreign surveillance, appropriately excluded only where "the purpose of the particular surveillance was not intelligence gathering but obtaining evidence of crime."[122] The amended FISA statute, by modifying the standard of the "primary purpose" for conducting foreign intelligence to the "significant purpose,"[123] mandates the "government have a measurable foreign intelligence purpose, other than just criminal

---

[118] Butler, supra note 7, at 55 (citing 50 U.S.C. § 1881a(a)).
[119] *See In re* Sealed Case, 310 F.3d 717, 735 (2002); *see also* United States v. Duka, 671 F.3d 329, 344 (3d Cir. 2011) ("FISA's 'significant purpose' standard is reasonable in light of the government's legitimate national security goals.").
[120] 310 F.3d 717, 735.
[121] *Id.*
[122] *Id.*
[123] 50 U.S.C.A. § 1804(a)(6)(B) (West).

prosecution of even foreign intelligence crimes."[124] Though criminal prosecution cannot amount to the primary objective of the investigation, evidence uncovered through a legally sound foreign intelligence investigatory search is admissible in criminal prosecutions.

Where a law enforcement officer is legally on the premises conducting a lawful search, any violations of law discovered are appropriately considered permissible evidence.[125] Courts are consistent in upholding the "significant purpose test" as constitutionally within the limits of the Fourth Amendment.[126] This renders evidence, acquired through an appropriately conducted FISA search, admissible in domestic criminal prosecutions.[127]

Conveying the "probable cause to believe that a foreign agent is communicating with his controllers outside our borders makes an interception reasonable" under the constitutionally valid FISA requirements.[128] Therefore, should an agent uncover evidence related to a domestic crime, while conducting a FISA investigation, this evidence

---

[124] United States v. Abu-Jihaad, 630 F.3d 102, 128 (quoting *Sealed Case*, 310 F.3d at 735); *see also* United States v. Duka, 671 F.3d 329, 344 (3d Cir. 2011).

[125] "Inspectors lawfully on the premises under such warrants may report any violations of law that they find; evidence in plain view need not be overlooked, even if that evidence concerns a different statute." United States v. Ning Wen, 477 F.3d 896, 898 (7th Cir. 2007); *see also* United States v. Hartwell, 436 F.3d 174, 181 n.13 (3d Cir. 2006) ("[T]he fruits of the search need not be suppressed so long as the search itself was permissible.").

[126] *Abu–Jihaad*, 630 F.3d at 128; *see also Sealed Case*, 310 F.3d at 735; *Duka*, 671 F.3d at 344 (3d Cir. 2011); *Hartwell*, 436 F.3d at 181.

[127] *Ning Wen*, 477 F.3d at 898 (holding that the principles alloying "[i]nspectors lawfully on the premises under such warrants [to] report any violations of law that they find" appropriately extend to FISA, and under this context "evidence in plain view need not be overlooked, even if that evidence concerns a different statute"); *see also Sealed Case*, 310 F.3d 717 (FISA Ct. Rev. 2002).

[128] *Id.*

may be appropriately considered "in plain view" and admissible in a domestic criminal prosecution.[129]

The process of maintaining FISA warrant procedures, and the FISC serves to protect prosecutors who may otherwise be forced to exclude evidence determined to have been unlawfully discovered. Dissimilar from the vulnerability to exclusion that evidence— procured in warrantless investigations failing to maintain a consistent intent of intelligence gathering— is subject to, all evidence procured through these FISA approved investigations will not be subject to exclusion.[130]

C. National Security Investigations Demand a Warrant Process and the Judiciary is Qualified to Administer Oversight

Constitutionally protected privacy rights are extremely vulnerable to the government's collection of the "personal communications of U.S. persons."[131] The Fourth Amendment specifically protects "papers" of U.S. citizens from "unreasonable search and seizure."[132] Because a person's private communication is "akin to personal papers," this protection extends to letters "transmitted by letter, telephone or e-mail."[133] It follows that judicial oversight and Fourth Amendment limitations appropriately reach all government data-collection initiatives.

---

[129] *Id.*
[130] Evidence uncovered through a reasonable intercept "may be used in a domestic prosecution whether or not the agents expected to learn about the domestic offense." *Id*.
[131] Redacted, 2011 WL 10945618, at 26 (FISA Ct. Oct. 3, 2011)
[132] *Id.*; *see also Truong Dinh Hung*, 629 F.2d at 915 (discussing how "individual privacy interests are severely compromised any time the government conducts surveillance without prior judicial approval").
[133] *Id.*

Previous courts have held the Executive maintains the power to execute warrantless *foreign* intelligence gathering under its "Article II authority over foreign affairs."[134] The constitutional vulnerability rendered through the recognition of this narrow exception is conveyed through the Government's purported interpretation of the exception to extend to permit even warrantless domestic surveillance.[135]

Unsurprisingly, government intrusion into the private lives of Americans, even under judicial governance, renders angst amongst the citizenry.[136] Determining the appropriate balance between the government's responsibility to maintain domestic security, and the constitutional rights of its citizens, proves increasingly difficult in the hostile climate of foreign terrorist threats.[137]

The FISC and Title III courts each serve to authorize electronic surveillance.[138] The courts differ on the standards of probable cause necessary to obtain an authorization for electronic surveillance.[139] Title III mandates a showing of "probable cause for belief that an individual is committing, has committed, or is about to commit" a particular crime.[140]

---

[134] *Abu-Jihaad*, 630 F.3d at 121 (citing *Truong*, 629 F.2d at 908).
[135] What is defined as an "agent of a foreign power" may include U.S. citizens who are determined to be "knowingly engag[ing] in clandestine intelligence gathering activities" or "knowingly engages in sabotage or international terrorism, or activities that are in preparation thereof." Brief for Petitioner at 29–34, United States v. U.S. District Court (*Keith*), 444 F.2d 651, 653 (6th Cir. 1971), *aff'd*, 407 U.S. 297 (1972) (citing 50 U.S.C. § 1805(b)(2)(A)).
[136] *Keith*, 407 U.S. at 312.
[137] *See id.*; *see also* Francel, *supra* note 30; Clarke, *supra* note 30; *Sealed Case*, 310 F.3d 717; Earnest, *supra* note 70, at 12 (discussing the balancing of "the need to protect our basic constitutional rights and the need to protect the United States of America").
[138] *Sealed Case*, 310 F.3d at 738.
[139] *Id.*
[140] 18 U.S.C.A. § 2518(3)(a) (West).

Dissimilarly, FISA mandates the government demonstrate "probable cause that the target is a foreign power or an agent of a foreign power."[141]

Judicial oversight is vital, as the Government acknowledges evidence procured through foreign surveillance efforts are appropriately utilized in "prosecuting the crime thus disclosed."[142] Preservation of individual liberties, vulnerable to intrusive government search initiatives, are best protected through judicially administered warrants.[143]

A court specifically designed to scrutinize the constitutionality of intelligence surveillance proves necessary as the technology employed by the intelligence sphere is "extremely complex."[144] To grasp the complexity of various intelligence surveillance methods, the FISC is briefed by various parties in the intelligence community.[145]

The necessity of a warrant process within the intelligence community is conveyed through recent intelligence surveillance methods that fail to maintain FISC approval. One of the most controversial intelligence surveillance programs—upstream surveillance— maintains very little FISC oversight.[146] The NSA employs this procedure, absent a FISC warrant,[147] "to seize[] Americans'

---

[141] 50 U.S.C.A. § 1805(a)(3) (West).
[142] *See generally* Brief for Petitioner at 1–2, Wikimedia Found. v. Nat'l Sec. Agency (2016) (No. 703452).
[143] *Keith*, 407 U.S. at 311, *but see Truong Dinh Hung*, 629 F.2d at 913 (finding "the judiciary [] largely inexperienced in making the delicate and complex decisions that lie behind foreign intelligence surveillance") (citing New York Times Co. v. United States, 403 U.S. 713, 727–30 (1971) (Stewart, J., concurring); United States v. Belmont, 301 U.S. 324, 330 (1937).
[144] United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2014 WL 2866749, at *11 (D. Or. June 24, 2014)
[145] *Id*.
[146] Reply Brief for Petitioner, *supra* note 87, at 11–12.
[147] *Megahey*, 553 F. Supp. at 1190 (determining the FISC process is a

communications in bulk and review the contents of substantially all international text-based communications--and many domestic communications as well."[148]

III. UTILIZING FISC AND PROHIBITING WARRANTLESS SEARCHES IMPROVES PUBLIC TRUST AND ACCOUNTABILITY OF GOVERNMENT INTELLIGENCE

Since the passing of FISA, the legislature has continued efforts to regulate and oversee intelligence. In 2006, the National Security Division was created to generate "information sharing, coordination and unity of purpose" within the national security sector.[149] This division facilitates information sharing amongst "prosecutors, law enforcement agencies, and the Intelligence Community" in order to more efficiently respond to threats.[150]

A. Investigations Maintained Through FISA Warrants Sustain Better Transparency and Accountability than Warrantless Methods

FISA, and the PATRIOT ACT's modifications to the FISC, regulate and encourage law enforcement agencies in the investigation and prosecution of persons involved in criminal acts of terrorism.[151] The methods employed by the

warrant within the context of the fourth amendment).
[148] *Id.*
[149] Assistant Att'y Gen. John P. Carlin Delivers Opening Remarks at the Nat'l Sec. Div. 10 Year Anniversary Conf., (Sept. 14, 2016), 2016 WL 4773001
[150] *Id.*
[151] In Re: **** Applicant for Sec. Clearance, ISCR Case No. 04-00540 (Jan. 5, 2007).

intelligence sphere, to ensure our safety, are subject to various FISA mandated oversights.[152]

The PATRIOT ACT's modifications to FISA further support the role of the court to provide judicial oversight for the increased foreign intelligence efforts stemming from the September 11 terrorist attacks.[153] Nonetheless, American civil liberties remain vulnerable to expanding innovative intelligence gathering schemes.[154] Warrantless searches have proven constitutionally problematic,[155] therefore maintaining the judicial and legislative oversight currently in place and encouraging continued reform— targeted at protecting vital privacy rights— is of the utmost importance.

The court scrutinizes intelligence surveillance efforts' consistency with the Fourth Amendment.[156] Safeguards, maintained by the FISC, to preserve constitutionally protected privacy rights include: scrutinizing the permissibility of the particular intelligence purpose; scrutinizing the procedures' reasonableness under the limitations of the Fourth Amendment; mandating a "significant purpose" for any collection of electronic communications; and minimization procedures which serve to "minimize the acquisition, retention, and dissemination of

---

[152] Earnest, *supra* note 70, at 3.
[153] *See In re* Sealed Case, 310 F.3d 717, 735 (FISA Ct. Rev. 2002) (holding section 1804 and section 1805 to provide the FISA court with the authority "to review the government's purpose in seeking the information").
[154] *See id.*; *see also* Sudha Setty, *Surveillance, Secrecy, and the Search for Meaningful Accountability*, 51 Stan. J. Int'l L. 69 (2015).
[155] *See generally* Meason, *supra* note 21); *see generally United States v. U.S. Dist. Court*, 407 U.S. 297 (1972) (holding the government's warrantless electronic surveillance procedures, purportedly for national security, amounted to an unreasonable, constitutionally invalid search).
[156] Brief for Petitioner, Wikimedia Foundation v. NSA (2015) (No. 5025551).

U.S.-person information."[157] Proper implementation and consistency of minimization requirements is overseen by the FISC.[158]

Through its efforts to prosecute citizens with evidence obtained in warrantless electronic investigations, the Government has clearly conveyed a desire to secure unchecked electronic surveillance.[159] The FISC's review of these surveillance methods "provides prior review by a neutral and detached magistrate" strengthening the preservation of civil liberties and the Fourth Amendment.[160] The FISC additionally enforces implementation of procedures to maintain constitutional practices within the intelligence sphere.[161] Where it is determined that data has been gathered from "an identifiable U.S. person or a person reasonably believed to be located in the U.S." the court is notified.[162]

An overwhelming amount of FISC criticism stems from recent modifications to the court's structure that weaken its ability to oversee and scrutinize surveillance techniques.[163] The FISA Amendments Act of 2008 (FAA) forced substantial changes to the role of the FISC in

---

[157] Answering Br. for Pl. Appellee at 38, United States v. Mohamud, 843 F.3d 420 (9th Cir. 2016) (No. 14-30217), 2015 WL 8988426; *see also* Br. for Pet'r, *supra* note 132..
[158] Brief for Petitioner, *supra* note 131.
[159] *See generally* Reply Brief for Petitioner, *supra* note 81, at 2. (emphasis added).
[160] United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2014 WL 2866749, at *11 (D. Or. June 24, 2014).
[161] Redacted, 2011 WL 10947772, at *4 (FISA Ct. Nov. 30, 2011)
[162] *Id.* (citing Amended NSA Minimization Procedures at 6 (§ 3(b)(5)(b)(2)(c)).
[163] "The basic framework established by FISA remains in effect today, but it has been gravely weakened by the FAA to permit the acquisition of U.S. persons' international communications without probable cause or individualized suspicion." Br. for Pet'r, *supra* note 81, at 5.

approving intelligence efforts.[164] The court's authority is narrowed within the statute to expand legally permitted surveillance[165] and permit the court to merely "review[] the general procedures the government proposes to use in carrying ... surveillance."[166] The lacking oversight, though problematic, fails to persuade the need to absolve the court entirely.

Government efforts to increase transparency and accountability have coincided with the implementation of FISA. Both Deputy Attorney General James Cole, and Attorney General Loretta Lynch addressed the Obama administration's efforts to "promote greater transparency" of the intelligence community.[167] Additionally, the administration mandated the Director of National Intelligence's release of reports centered on the "effectiveness of implementing reforms that balance our civil liberties with our national security needs."[168] Consequentially, public knowledge of intelligence practices, and avocation for modifying various procedures has stemmed from this increased transparency.[169]

Transparency stemming from FISA and the FISC is further conveyed from the visibility of FISC litigation.[170] In

---

[164] Br. for Pet'r, *supra* note 79, at 5.
[165] *Id*., at 5. (citing *In re* Proceedings Required by § 702(i) of the FAA, No. 08-01, 2008 WL 9487946, at *2 (FISC Aug. 27, 2008),
[166] *Id*. (citing 50 U.S.C. § 1881a(i).
[167] *See* Lynch *supra* note 71; *see also* Deputy Att'y Gen. James M. Cole Testifies Before The U.S. House Judiciary Comm.,(Feb. 4, 2014), 2014 WL 408411.
[168] Earnest, *supra* note 70, at 3.
[169] *See* Lee Ferran, *NSA Can Access More Phone Data Than Ever*, (Oct 20, 2016), http://abcnews.go.com/US/nsa-potentially-access-phone-data/story?id=42892417; *see also* Charlie Savage, *N.S.A. Said to Search Content of Messages to and from U.S.,* N.Y. TIMES, (Aug. 8, 2013), http://nyti.ms/1E1nlsi
[170] Statement By Dir. Of Nat'l Intelligence On The Declassification Of Doc. Related To The Protect America Litig., DOJ 14-971.

a previous court opinion, upholding controversial NSA directives to Yahoo!, the Executive Branch released both the court's opinion and the briefs related to the litigation to the public.[171] The documents were made available on the Office of the Director of National Intelligence (ODNI) website.[172] The public is aware of the FISC procedures and their opinions.[173]

Increased awareness invites criticisms. Though public criticism may decrease with the unitization of warrantless, unchecked Executive searches for national security investigations, constitutional violations are likely to increase.

B. FISC Properly Operates as a Necessary Check on the Executive

Prior to the passing of FISA, the Executive routinely fought for unlimited power to investigation citizens without a warrant, absent judicial oversight.[174] The Government argued the President's "need for intelligence information with respect to threats to national security posed by so-called domestic organizations is *no less than* his need for such information with respect to threats posed by foreign ones."[175]

The necessity of judicial oversight is demonstrated through Government attempts to present evidence, obtained

---

[171] *Id.*
[172] *Id*.
[173] *Mohamud*, 2014 WL 2866749, at *11, (Declassifying FISC opinions has led to public awareness "that the court meets with senior officials at the Department of Justice to discuss information provided in the submissions.")
[174] *See generally* Reply Br. for Pet'r, *supra* note 83, at 2.(emphasis added). (note 83 is 24 Int'l Law. 1043)
[175] *Id*. (emphasis added)).

through warrantless "national security surveillance," to criminally prosecute U.S. citizens.[176] The Government cites the Executive's power to protect the nation to justify the broad exception to the Fourth Amendment's warrant requirement.[177] Determining "no sharp and clear distinction can be drawn between 'foreign' and 'domestic' information" the Government interpretation of the recognized foreign intelligence exception is to exempt surveillance targeted at American citizens domiciled in the U.S. from Fourth Amendment limitations.[178] This rendered all electronic surveillance efforts, purportedly orchestrated for the purpose of "national security" exempt from any "prior judicial authorization."[179]

Congress sought to abate constitutional concerns promulgating from the Executive's recognition of a "presidential authority to conduct warrantless foreign intelligence surveillance" with the drafting of FISA.[180] FISA mandates electronic investigations, even where aimed towards the collection of evidence related to national security, "be authorized by a warrant from a federal district judge."[181]

FISA mandates the FISC to provide "prior judicial scrutiny" of authorizations of electronic surveillance.[182] The

---

[176] *See Keith*, 407 U.S. 297, 303.
[177] *See generally* Reply Brief for Petitioner at 2, U.S. v. U.S. Dist. Court for the Eastern Dist. of 66 Mich, 407 U.S. 297 (1972)(No. 135522) .
[178] Br. for Pet'r at *5, United States v. U. S. Dist. Court, 444 F.2d 651 (6th Cir. 1971) (No. 70-153), 1972 WL 135522, *aff'd*, 407 U.S. 297 (1972).
[179] *See generally* Reply Br. for Pet'r, *supra* note 83, at 2 (citing Article IV, Section 4). (cites to 24 Int'l Law 1043)
[180] United States v.Abu-Jihaad, 630 F.3d 102, at 121 (2d Cir. 2010).
[181] United States v. Ning Wen, 477 F.3d 896, at 897 (7th Cir. 2007) (citing 50 U.S.C. § 1803(a) (2012)).
[182] 50 U.S.C. § 1805; 18 U.S.C. § 2518; *see also In re* Sealed Case, 310 F.3d 717, 738.

constitutional validity of the FISC is most accurately conveyed through the numerous court decisions upholding the FISA requirements as constitutionally sound, and valid under the Fourth Amendment.[183]

Though the FISC is continually attacked as protecting unreasonable investigatory schemes, it serves to limit the "broad authority…to gather intelligence information through electronic surveillance in dealing with domestic organizations" sought by the Executive.[184] The FISC serves as a check on the Executive and further provides the judicial oversight necessary for intelligence procedures to comply with the Fourth Amendment.[185] Further, the FISC has even served as a judicial check on warrantless foreign intelligence schemes, maintained post FISA, under the "foreign intelligence exception."[186]

---

[183] *See Abu-Jihaad*, 630 F.3d 102, at 120 (stating "all other courts that have considered the issue, both before and after enactment of the PATRIOT Act, have rejected constitutional challenges to FISA") (citing *Ning Wen,* 477 F.3d at 898; United States v. Damrah, 412 F.3d 618, 625 (6th Cir.2005); *In* Sealed Case, 310 F.3d 717, 742–46 (FISA Ct. Rev. 2002); United States v. Johnson, 952 F.2d 565, 573 (1st Cir.1991); United States v. Pelton, 835 F.2d 1067, 1075 (4th Cir.1987) United States v. Cavanagh, 807 F.2d 787, 790–92 (9th Cir.1987); *United States v. Kashmiri, No. 09 Cr. 830–4, 2010 WL 4705159, at *3–5 (N.D.Ill. Nov.10, 2010)*; United States v. Warsame, 547 F.Supp.2d 982, 993; United States v. Mubayyid, 521 F.Supp.2d 125, 135–44; United States v. Holy Land Found. for Relief & Dev., No. 04 Cr. 240, 2007 WL 2011319, at *5–6 (N.D.Tex. July 11, 2007); United States v. Jayyousi, No. 04 Cr. 60001, 2007 WL 851278, at *1 (S.D.Fla. Mar.15, 2007); United States v. Benkahla, 437 F.Supp.2d 541, 554 (E.D.Va.2006); United States v. Marzook, 435 F.Supp.2d 778, 786 (N.D.Ill.2006); States v. Nicholson, 955 F.Supp. 588, 590–91 (E.D.Va.1997); *In re* Kevork*,* 634 F.Supp. 1002,1014; United States v. Falvey, 540 F.Supp. 1306, 1312 (E.D.N.Y.1982).

[184] *See generally* Reply Br. for Pet'r, *supra* note 172, at 2.

[185] 50 U.S.C.A. § 1881a (West 2015)

[186] *In re.* Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008).

The court continues to hold—even where the FISA procedure is available to secure a warrant— particular circumstances render warrantless intelligence surveillance constitutionally valid.[187] This was conveyed through repeated challenges to the NSA efforts to maintain electronic internet surveillance in order to "target certain non-U.S. persons reasonably believed to be located outside the United States in order to acquire foreign-intelligence information."[188] In considering these warrantless government investigations, "probable cause and necessity" were scrutinized, and the methods were determined to "resemble[] those associated with traditional warrant requirements."[189]

In 2007 the NSA issued directives to Yahoo! mandating the corporation to provide information believed to be effective in securing foreign intelligence.[190] The NSA maintained this "upstream collection" of internet communications was centered on "targets reasonably believed to be located outside the United States."[191] Yahoo! refused to honor the directives, and the U.S. Government initiated proceedings in the FISC to compel Yahoo!'s compliance.[192] The FISC held these surveillance schemes reasonable under the Fourth Amendment, and Yahoo! was compelled to comply with the directives.[193] Though

---

[187] *See Id.* at 1009.
[188] Br. for Pet'r, *supra* note 132; *see also In re Directives*, 551 F.3d at 1013; *see also* Redacted, 2011 WL 10945618, at *1 (FISA Ct. Oct. 3, 2011).
[189] Br. for Pet'r, *supra* note 132.
[190] *See* Statement By Dir. Of Nat'l Intelligence On The Declassification Of Doc. Related To The Protect America Litig., DOJ 14-971.
[191] *In re Directives* , 551 F.3d at 1013; *see also* Redacted, 2011 WL 10945618, at *1 (FISA Ct. Oct. 3, 2011)*; see also Statement By Dir. Of Nat'l*, DOJ 14-971
[192] *In re Directives*, 551 F.3d at 1013.
[193] *Id.*

controversial, this decision conveys the vitality of promulgating efficient tribunals to both preserve Fourth Amendment limitations, and provide parties with the opportunity to challenge any intrusive intelligence efforts.[194]

Though these warrantless searches remain subject to some form of judicial scrutiny, the failure to secure a warrant, even in limited circumstances, proves increasingly problematic. Just four years following the court's approval of the intelligence gathering scheme, the court reconsidered this particular government request for electronic communication purportedly centered on foreign intelligence.[195] In this subsequent case, the FISC considered the reality of the NSA's "upstream collection" of multi-communication transactions (MCTs).[196] The Government originally maintained the constitutionality of this NSA program arguing that a "relatively small" amount of protected communication would be unintentionally acquired through the expansive data collection.[197]

Considering "the totality of the circumstances" the court scrutinized both the "ratio of non-target, Fourth Amendment-protected communications to the total number of communications" and the amount of protected communication collected in "absolute terms" to hold the data collection inconsistent with the Fourth Amendment.[198]

With concrete evidence of the data collected, the court determined the ratio of protected communication collected proved small in comparison to all communication intercepted by the NSA program, but the "tens of thousands of non-target, protected communications" in absolute terms

---

[194] *See Statement By Dir. Of Nat'l*, DOJ 14-971
[195] *See* Redacted, 2011 WL 10945618, at *1 (FISA Ct. Oct. 3, 2011)
[196] *See Id*., at 26.
[197] *Id.*
[198] *Id.*

proved problematic.[199] The court found the collection of "a very large number of Fourth Amendment-protected communications that have no direct connection to any targeted facility and thus do not serve the national security needs" amounted to an unreasonable search.[200]

C. Completely Foregoing Warrantless Searches Promotes Constitutionally Valid Intelligence Gathering Procedures

Unreasonable Executive surveillance endeavors motivated the drafting of legislation to limit the Executive's power and enforce oversight in intelligence procedures.[201] It follows, efforts to maintain the constitutionality of intelligence gathering have increased as recent security threats perpetuate a demand for expanded surveillance.[202] Dissimilar from earlier administrations' endeavors to avoid the Fourth Amendment's limitations,[203] the passing of FISA brought a continued Executive attempt to implement a "rigorous oversight regime to "maintain national security."[204]

The Court's majority opinion in *Katz* failed to address the constitutionality of foregoing warrants to conducted electronic surveillance where national security

---

[199] *Id.*
[200] *Id.* at 26.
[201] *See* Meason, *supra* note 21.
[202] Setty, *supra* note 149, at 101 & n.186 ("Establishing the Privacy and Civil Liberties Oversight Board (PCLOB) was a recommendation of the 9/11 Commission Report.")
[203] *See supra*, note 10.
[204] Deputy Att'y Gen. James M. Cole Testifies Before The U.S. House Judiciary Comm., *supra* note 162; *see also* Lynch *supra* note 71 (stating the administration made "protection of civil liberties and privacy a priority in the fight against terrorism.")

was at issue.[205] Nonetheless Justices Douglas and Brennan recognized the potential abuses inherent to an unchecked Executive power to employ warrantless investigations.[206] Additionally the Justices stressed the need for judicial oversight, as it is unlikely Fourth Amendment rights maintain appropriate protection where "the President and Attorney General assume both the position of adversary-and-prosecutor and disinterested, neutral magistrate."[207]

The implementation of FISA and further creation of the FISC, convey the overwhelming need to abandon the "foreign intelligence exception" to the Fourth Amendment's warrant clause.[208] Despite previous legislative and judicial efforts to procure constitutionally abusive surveillance methods though the passing of FISA and creation of the FISC, the "foreign intelligence exception" continues to be recognized as a reasonable "special needs" search excused from compliance with the Fourth Amendment.[209]

The oversight implemented through FISA has continued to effect reform to intelligence gathering methods employed by the Executive. Dissimilar from past administration's continued efforts to advocate for Executive exemptions to the Fourth Amendment, post FISA administrations' have conveyed an approach to intelligence gathering centered on "balanc[ing] our civil liberties with

---

[205] Katz v. United States, 389 U.S. 347, at 359–60.
[206] *Id*.
[207] *Id* at 360. (Justices Brennan and Douglas Concurring)("Neither the President nor the Attorney General is a magistrate. In matters where they believe national security may be involved they are not detached, disinterested, and neutral as a court or magistrate must be.")).
[208] *See* 50 U.S.C.A. § 1801 (West 2015); *see also* Earnest, *supra* note 70, at 3 (discussing the FISC procedure of "review[ing] requests from intelligence professionals about tools or tactics that they intend to employ."
[209] *In re.* Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1009 (FISA Ct. Rev. 2008).

our national security needs."[210] The sharp deviation from earlier practices is demonstrated through the numerous Executive undertakings to increase accountability within the intelligence sphere.[211] The Privacy and Civil Liberties Oversight Board (PCLOB)—created by the Obama Administration— is sustained for the sole purpose of protecting the security of the nation, while concurrently "upholding the liberties" protected by the Constitution.[212]

The FISC needs to be altered to avoid any mere "rubber stamp" approvals, allow for advocacy of "privacy concerns" and generate a more "genuinely adversarial" procedure.[213] Implementing stricter scrutiny in the decisions to issue warrants for the gathering of foreign intelligence, or excluding all information obtained with a FISA "warrant" that fails to pertain to national security threats may prove beneficial to better protect civil liberties. The court continues to uphold the "foreign intelligence exception" though the abuses stemming from this exception prove the very reason for the court's creation.[214]

Following the September 11 attacks, President George W. Bush authorized the NSA's implementation of

---

[210] Earnest, *supra* note 70, at 3.
[211] *See* Lynch *supra* note 71. (discussing the creation of the Privacy and Civil Liberties Oversight Board), *see also* Deputy Att'y Gen. James M. Cole Testifies Before The U.S. House Judiciary Comm., 2014 WL 408411 (recognizing the "potential misuse" of data collected for intelligence).
[212] See Garrett Hatch, CONG. RESEARCH SERV., RL34385, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD: NEW INDEP AGENCY STATUS (2012) ("The PCLOB was statutorily authorized in 2007, but only became operational and fully staffed in late 2013 and early 2014, months after the Snowden disclosures."); *see also* Setty, *supra* note 149, at n.186.
[213] Setty, *supra* note 149.
[214] *See* Meason, *supra* note 21; *see also* 50 U.S.C.A. § 1801 (West 2015)

warrantless national security surveillance.[215] The government sought approval from the FISC, following a federal district court's determination the program was unconstitutional because it exceeded the limits of the Fourth Amendment.[216] The FISC considered an additional warrantless search exception in 2007 when scrutinizing the constitutional validity of the FISA expansion that allowed for "warrantless foreign intelligence surveillance" on persons "'reasonably believed" to be located outside the United States."[217] These particular intelligence methods were conducted for the purposes of obtaining "foreign intelligence information" and maintained the "minimization procedures" mandated by FISA.[218] This "upstream collection" of internet communications was argued by the NSA as "critical to Government efforts to combat international terrorism and other threats to the United States and its interests."[219]

The FISC decision holding these warrantless investigations constitutionally reasonable where the intent was to protect the security of the nation proves problematic.[220] Though the FISC's creation centers on the constitutionally problematic "foreign intelligence exemption," the court upheld the exception to protect warrantless investigations lacking FISC oversight.[221] The FISC determined the particular intelligence gathering efforts within what the Court has previously defined as "special

---

[215] *See* Br. for Pet'r, *supra* note 81, at *6.
[216] *See Id*. (citing ACLU v. NSA, 438 F. Supp. 2d 754 (E.D. Mich. 2006).
[217] *In re.* Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1006 (FISA Ct. Rev. 2008).
[218] *Id*., at 1010.
[219] Br. for Pet'r, *supra* note 131.
[220] *In re Directives*, 551 F.3d at 1006.
[221] *Id*.

needs" case that maintains an exemption from Forth Amendment limitations.[222]

The FISC's upholding of warrantless surveillance and further the "foreign intelligence exception" stands in direct contrast to the Court's previous rulings. Currently, the Supreme Court has never recognized "special needs" cases to include intelligence gathering efforts, maintained absent judicial oversight.[223] Previous Court opinions holding the fear of the "erosion of our sense of privacy and independence" to far outweigh the fear that "upheaval will modify our form of government" suggest that the Court would not consider judicial oversight to "materially interfere" with these national security surveillance efforts,[224] but rather that the court would consider these particular investigations to warrant the necessity of judicial oversight.[225]

Investigations, orchestrated through solely warrantless searches, absent judicial oversight, remain unreasonably intrusive searches under the Fourth

---

[222] *Id.*

[223] *Id,* at 1006. (citing Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995) (holding the warrant and probable-cause requirement impracticable for the employment of procedures to drug test high-school athletes. Considering these actions "special needs, beyond the normal need for law enforcement")(quoting Griffin v. Wisconsin, 483 U.S. 868, 873(1987)); Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 620, (1989) (upholding the mandate for drug and alcohol testing of railroad employees for the purposes of safety as constitutional); 1011 cf. Terry v. Ohio, 392 U.S. 1, 23–24, (1968) (holding the frisk for weapons in the intent of securing the safety of law enforcement officers proved reasonable, and constitutionally valid absent a warrant).

[224] *In re Directives*, 551 F.3d at 1006.

[225] *Id., but see* United States v. Truong Dinh Hung, 629 F.2d 908, 913 (4th Cir. 1980) (holding "the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would, following *Keith*, 'unduly frustrate' the President in carrying out his foreign affairs responsibilities."

Amendment. Following the establishment of the FISC—to administer specialized judicial oversight for unique foreign intelligence procedures— the continued recognition of a constitutional exception for foreign intelligence gathering is unwarranted.

IV. CONCLUSION

Pre FISA administrations' abuse of Constitutional privacy rights conveys the vital need for judicial oversight in the intelligence sphere. An Executive exemption to the Fourth Amendment, absent any judicial oversight leaves Americans' civil liberties vulnerable. The FISC oversight, maintained through FISA warrants, provides both judicial oversight and transparency to the electronic surveillance programs employed by the intelligence sphere.

Dissimilar from previous, unchecked national security surveillance, search powers are properly narrowed through the limitations promulgated by congressional and judicial oversight of the Executive's intelligence gathering procedures. Acquisitions of communications under FISA are scrutinized by the judiciary and challengeable in the FISC.

It is vital that the FISC be maintained and that courts abandon the unreasonably intrusive, warrantless surveillance facilitated through the foreign surveillance exception. A multitude of constitutional safeguards exist to prohibit any government body's exercise of unchecked power. These safeguards convey immense doubt the Framers foresaw an exemption to the Fourth Amendment's limitations, protecting the citizenry from abusive government searches, as constitutionally valid.

Cyber Enhanced Sanction Strategies: Do Options Exist?

Mark Peters*

ABSTRACT

Today's financial sanction practices need immediate updates to generate sufficient impact in modern crisis resolution and should consider cyber-based strategies. Globally, some erected, economic sanctions have existed for decades without achieving, or making significant progress towards, their desired effects. Cyber means could enhance sanction strategies to more effectively achieve national ends. The strategy suggested here designates a potential methodology as Cyber Enhanced Sanctions (CES) and advocates digital techniques to more effectively influence national decision-makers while allowing reversibility, secured communications, and humanitarian relief through digital channels. Examining current cyber means establishes a baseline for strategists to develop implementation strategies. Once a baseline strategy is proposed, this article further suggests a potential application case in U.S. sanctions against Russia concerning the Ukrainian conflict. Overall, CES could offer expanded options for the U.S. national power toolkit.

* *Lt. Col. Mark Peters* is the Operations Division Chief for the 625th Operations Center at JBSA-Lackland, Tex. Previously, he served as the Commander, 18th Intelligence Squadron, Wright-Patterson AFB, OH. He holds a Doctorate Degree in Strategic Security from Henley-Putnam University and has a forthcoming text from Potomac Books researching how states use cyber means to achieve economic ends.

INTRODUCTION

In 2014, Russia first invaded Crimea, promising help and solidarity to oppressed ethnic minorities. Ukraine followed on Putin's hit list with a separate invasion when the nation failed to fall in line with Russia's desired European Union trade guidelines. The United States and EU responded quickly with news conferences, stern démarches, and eventually, governmental actions generating economic sanctions. Current financial sanction practices sometimes fail to achieve desired timelines, missing targeted bank accounts or actors, and failing to create the desired response and influence decision makers. A cyber-based strategy may offer improvements to purely diplomatic financial sanctions in achieving national ends.

Sanctions, supported by national diplomatic and economic influences, are a traditional state answer to foreign crises with the most recent change being the use of targeted actions against individual actors. Some sanctions, such as those levied against Iran, required years before any actions were realized, implemented, and resolved, and even longer before any results could possibly be tracked to those effects.[1] Even if imposed sanctions start effectively, their actions may fail to impact intended targets. During recent U.S. sanctions against Russia relating to the Ukrainian crisis, several Russian leaders including Vladislav Surkov, a Putin advisor,

[1] In Iran's case, since 1979, eleven separate legislative acts describing economic sanctions and seventeen different Executive Orders have been applied to Iran to attempt to curb their behavior regarding Weapons of Mass Destruction proliferation and terrorist support. Dianne E. Remmack, *Iran: U.S. Economic Sanctions and the Authority to Lift Restrictions*, Congressional Research Service (15 Jul 2016) R43311.

and Dmitri Rogozin, a deputy prime minister, joked with national media about the United States' ineffectiveness in enforcing sanctions.[2] If traditional sanctions falter, the choices available to senior leaders rapidly narrow and may lead to deciding between costly, military action and perceived national ineffectiveness. Cyber means offer an approach to augment U.S. economic sanction effectiveness without a boots on the ground commitment.

Current financial sanction strategies delay national ends through time-consuming methods and frequently fail to significantly change the sanctioned state's decision calculus. The lack of effective alternatives, unreachable targets due to conventional economic structures, and minimized communication channels to those harbored by hostile governments, can prevent sanctions from reaching their full potential in a timely manner. Cyber technology offers some alternatives through combining cyber means with economic sanction employment to target selected financial targets. Strategies emphasizing cyberspace tools may enhance economic sanctions and improve effectiveness through: increased enforcement opportunities, targeted economic denial and disruption, immediate reversibility upon success through ceasing cyber effects, increasing communication channels to threatened populations, and finding alternatives for improved humanitarian relief. Herein, a Cyber Enhanced Sanction (CES) is defined as employing active cyber techniques to support state-established economic sanctions guidelines. CES cyber techniques would seek to target vulnerabilities in digital financial transactions to delay or disrupt their execution, while coordinating with political decision-makers to achieve sanction goals.

---

[2] Stephen Lee Mylers & Peter Baker, *Putin Recognizes Crimea Secession, Defying the West,* N.Y. TIMES, March 18, 2014.

The CES strategy exploration builds through four areas. The first two are theoretical; examining current sanction practice shortfalls, and then discussing strategies underlying sanction enhancement through cyber. The next two areas focus on proposed CES means: examining publicly available CES techniques and limitations, and next evaluating a proposed CES framework, which could have been employed during the current Ukrainian conflict by the U.S. against Russia. Modifying publicly available cyber techniques would support the proposed effect categories and increase influence on sanction outcomes from a foreign leader's decision calculus, to increasing public unrest, or even cause a head of states outright removal. The modifications suggested are theoretical in this paper, strategies are outlined, but individual techniques would have to be developed for each sanction event. Cyber means still face limitations including escalation fears, legal constraints, and technical challenges in access and tool availability. Each limitation creates potential challenges for both policy and operational implementation even if they are successfully mitigated. After weighing the generic options, one can move to consider currently published U.S. guidance and standards as they could apply to cyber technique applications in the Ukrainian crisis and potential effectiveness metrics.

I. WHAT'S WRONG WITH CURRENT SANCTION PRACTICES?

Sanctions employ national power means, usually economic, to create effects. Current practices simply take too long to work but evaluating current practices first requires obtaining common definitions. In policy, power is, "the ability to affect other people to get the outcomes one

wants."[3] Sanctions are the, "deliberate, government-inspired withdrawal, or threat of withdrawal, of customary trade or financial relations."[4] An economic sanction definition specifies, "[o]rganized actions governments take to change the external environment in general or the policies and actions of other states in particular to achieve the objectives . . . set by policy makers."[5] All three explanations drive discussion on sanction ways and ends without considering means. The term cyber means suggests using a cyber-based technique to link overall objectives to lower level effects. For example, preventing a bank from issuing funds to purchase nuclear fuel by denying access to servers containing financial accounts. Multiple commonly accepted cyberspace definitions appear within academic and operational literature. One of the broadest refers to cyberspace as a "man-made environment for the creation, transmittal, and use of information in a variety of formats."[6] A more technical definition cites cyberspace as, "an agglomeration of individual computing devices that are networked to one another . . . and the outside world."[7] Nye cites cyber power as, "the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power."[8] In the national power spectrum, cyber uses microforce compared

---

[3] JOSEPH S. NYE, CYBER POWER at 2 (2010).
[4] Yitan Li, *US Economic Sanctions Against China: A Cultural Explanation of Sanction Effectiveness, in* 38-2 ASIAN PERSP. 311, 312 (2014).
[5] *Id.*
[6] GREGORY J. RATTRAY, STRATEGIC WARFARE IN CYBERSPACE (2001).
[7] MARTIN C. LIBICKI, CYBERDETERRENCE AND CYBERWAR 6 (2009).
[8] JOSEPH S. NYE, CYBER POWER 4 (Belfer Ctr. for Sci. & Int'l Affairs, Harvard Kennedy School 2010).

to the megaforce reserved for nuclear weapons.[9] CES offers these microforce means as an enhancement after an initial sanctioning decision to help create timely change.

Microforce theory emerged from Gregory Rattray's information warfare discussions. In addressing interstate cyberpower strategically, Gregory Rattray used cyber as his primary action showing how states achieve ends with information. He delineates cyberpower as when, "state and nonstate actors [use cyber means] to achieve objectives through digital attacks on an adversary's centers of gravity"[10] He avoids using cyberspace regularly, preferring its interpretation as a domain rather than a separate construct. Rattray also avoids discussing economic centers of gravity as information vulnerabilities. His theory's military cyberpower concentration likely explains why he ignores addressing diplomatic and economic vulnerabilities.

One of Rattray's main contributions to cyber applications occurs in categorization. He establishes the term "microforce" for digital attacks as a function other than a conventional kinetic weapon, or the nuclear megaforce examined in deterrence discussions.[11] Later discussion here links these terms with qualitative categories for evaluation. Rattray frames information warfare requirements as complex interconnections, civilian technological leadership, a fast change rate, and global interconnection between operations and production. As important, he details what conflict characteristics define where a state could seek cyberpower advantages, such as when an offensive advantage exists, a significant vulnerability is present,

[9] RATTRAY, STRATEGIC WARFARE IN CYBER SPACE 20 (2001).
[10] *Id.* at 14.
[11] *Id.* at 12.

minimal opportunity exists for retaliation, and effects are observable.[12]

Understanding the basic definitions above allows returning to why sanctions sometimes fall short in application. Economic sanctions present the primary means for international organizations like the United Nations (UN) to manage crisis. In the late 1990's, practices shifted from broad economic sanctions denying all financial activity to specific commodities, and then to targeting individuals. Individuals do not always appear relevant to national policy impacts although post-crisis link analysis frequently uncovers connections. CES theory suggests exposing sanctioned individuals through cyber techniques, as previously highlighted by established UN practices, may influence their decision-making and create desired government changes without collateral population impacts.[13] CES goes beyond merely naming individuals in diplomatic documents to influence multiple economic vulnerabilities across the global cyber commons.

Economic sanctions historically work based on the intended receiver's threat perception. Ang and Peksen's study traced sanction effectiveness to asymmetric perceptions, issue salience and outcome.[14] These elements tie foreign policy makers' perceptions on international conflicts, whether issues are personally relevant, and how domestic policies drive international outcomes. The applied

---

[12] *Id.*

[13] Peter Wallensteen & Helena Grusell, *Targeting the Right Targets? The UN Use of Individual Sanctions*, *in* 18-2 GLOBAL GOVERNANCE 208-09 (2012).

[14] Adrian U-Jin Ang & Dursun Peksen, *When Do Economic Sanctions Work? Asymmetric Perceptions, Issue Salience, and Outcomes*, 60 POL. SANCTIONS Q. 142 (2007).

Russian sanctions did not pose either a national or personal threat to Russian leaders. CES options help shift from broad-based applications to the financial influences linked to Russian oligarchs through identifying and selecting digital options tied to the individual. Disconnects between the Russian people and their leaders' exploitations have emerged over recent crises, and CES options could help expand those gaps.[15] Modern attempts to sanction Iran demonstrated where financial sanctions proved to be neither timely nor effective.[16]

A. Sanction Theories

In a broad-based discussion, theoretical applications provide a knowledge base while specific strategies and techniques appear in the next section. Sanctions are sometimes considered a blockade option in denying or disrupting trade.[17] World War I associated efforts used blockades to deny entire ports or prevent trade goods from shipment. As a denial and disruption means, financial sanctions serve three general purposes: denying individual

---

[15] FIONA HILL & CLIFFORD G. GRADDY, MR. PUTIN: OPERATIVE IN THE KREMLIN (2013).

[16] This Congressional report provides a detailed review of all sanctions associated with Iran and a quick look at their effectiveness. Obviously, Iranian sanctions have not succeeded as expected but a full effectiveness discussion is beyond the scope of this paper. KENNETH KATZMAN, RS20871, IRAN SANCTIONS (2017).

[17] The US Navy defines blockade as, "a belligerent operation to prevent vessels and/or aircraft of all nations, enemy as well as neutral, from enter or exiting specified ports, airfields, or coastal areas belonging to, occupied by, or under the control of the enemy nation." U.S. NAVY, MARINE CORPS & COAST GUARD, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS, Ch. 7.7, (Dep't of the Navy 1995).

finances, disrupting government functions, and ensuring humanitarian relief.[18] Rabkin and Rabkin show a clear comparison exists between cyber means and blockade usage in influencing economic outcomes without physical harm.[19] This CES theory attempts to expand national options through access, breach, disruption and denial techniques. Traditional sanctions can manipulate economic impacts by changing names and accounts on documents before global distribution to banks and merchants. Most sanctions only create effects in implementing countries, for example, preventing Russian oligarchs from reaching their U.S. bank accounts. Altering digital code could create global pressure through influencing selected individuals in their home countries while white-list techniques allow humanitarian relief to pass through enacted controls.[20]

Wallensteen suggests targeted sanction employment improves through gradually escalating pressure.[21] Gradual escalation only applies if the desired pressure influences decision-making calculus manageably. For instance, it is difficult to control cooking temperatures with a blowtorch, but easier with an electric oven. Escalation is critical in scaling effects to desired results. Managing sanction pressure requires being able to increase a tool's breadth, such as an imposed sanction denying several Russian leaders their

---

[18] Joy Gordon, *Smart Sanctions Revisited*, *in* 25-3 ETHICS & INT'L AFF. 315, 327 (2011).

[19] Jeremy Rabkin & Ariel Rabkin, *Navigating Conflicts in Cyberspace: Legal Lessons from the War at Sea*, 14 CHI. J. INT'L L. 197, 215 (2013).

[20] White lists describe actions where particular named activities are allowed to pass through a digital or physical barricade. Only the activity identified on the white list designations can cross the barriers. All other actions are diverted away or denied by the enforcing agent, whether digital or physical security.

[21] Wallensteen & Grusell, *supra* note 15, at 216.

U.S. bank account access that could be enhanced by adding additional leaders or restricting access to more commercial and financial institutions. CES options would move past denying only U.S. bank account activity to deny additional transactions to sanctioned entities in their own state. Rapidly changing a selected individual from government approved sanction lists in an implemented cyber technique allows CES options to increase sanction efficiencies. CES enforcement would not require multiple rounds of diplomacy and coordination, only implanting the tools within the desired financial networks. Global CES applications complement interdependence theory and also support realist and liberal international relations approaches.[22]

Targeted sanctions seek three basic outcomes: to bring leaders to the bargaining table, deprive resources to create regional power shifts, and threatening increased sanctions.[23] Cyber enhancement impacts all outcomes through increased sanction possibilities. Network means potentially deny individual's access to not just local resources, but to any digitally accessed finances worldwide. Although their legality may be questionable in any one state, actions could be authorized under broader multinational options such as the U.N. Security Council or NATO. Digitally manipulating accounts allows one to shift resources from a sanctioned account to provide congressionally approved funding to local opposition groups. Sanctioning activities that occur through cyber could be done with or without the support of organizations in the

[22] ROBERT KEOHANE & JOSEPH NYE, POWER AND INTERDEPENDENCE 252 (2012). ALISON LAWLOR RUSSELL, CYBER BLOCKADES 24-26 (2014).
[23] Wallensteen & Grusell, *supra* note 16, at 210.

offending state. Of course, offensive cyber actions against another state, even if justified by international agreements fall in a less defined area of international policy. U.S. Executive Orders (EO) sanctioning Russia over Ukrainian involvement only block properties within the United States' possession.[24] Cyber offers global power expansion within sanction planning, without committing local troops or the national resources required for traditional enforcement while increasing effectiveness. Cyber techniques can move past older means to disrupt or deny any digital system, worldwide.

CES techniques will demonstrably enhance sanction effectiveness. Historical sanction evaluation metrics measured whether sanctions affected target states' decision-making calculus.[25] CES effectiveness should also not be tool-centric, but evaluate sanction efficiency. For instance, with a Stuxnet-like example, effectiveness would not measure individual centrifuge operations but the overall effect on the Iranian nuclear development program. One study examining eight-targeted UN sanctions without cyber enhancements estimates sanctions achieving national goals at a 20-34% rate.[26] Sanctioned activities are frequently complex, and continuing data analysis will hopefully provide more comparative data. Wallensteen's study's biggest shortfall is the original data's age, at 20–30 years old, which coincides with the beginning of Iranian sanctions. Modern sanction effectiveness studies are rare, with most using qualitative case studies rather than quantitative

[24] Exec. Order No. 13660, *Blocking Property of Additional Persons Contributing to the Situation in Ukraine*, 79 Fed. Reg. 53, THE AMERICAN PRESIDENCY PROJECT (2014)
[25] Gordon, *supra* note 20, at 315-335.
[26] Wallensteen & Grusell, *supra* note 16, at 225.

assessments. Kozhanov, studying U.S. sanctions on Iran, highlights how policy loopholes can delay successful sanction employment.[27] Most loopholes consist of newly emerging activities or unreachable financial transactions. Cyber-enhancement would allow altering sanctions based on Treasury approved lists and close loopholes between financial means in one country and industrial production in another. CES means could highlight individuals, corporations, and products for explicit effects while traditional sanctions may persist for years without significant impacts. U.S. sanctions on Iran have generated only minimal behavior changes since their 1984 inception.[28] Modern resource constraints mean even small behavioral improvements in an adversary may be worthwhile investments in new means.

B. Sanction Legality

National power employment always depends on international perceptions. Effective sanction enhancement should enforce justice while remaining within national and international legal boundaries. CES should function with declared sanctions, through reaching other global cyber commons areas to disrupt and deny channels. Evaluating overall sanction legality is also left for other discussions. Some CES actions affecting foreign institutions may move from a typical sanction action to a cyber-attack, although short of physical harm. A starting point for CES legality

---

[27] Nikolay A. Kozhanov, *U.S. Economic Sanctions Against Iran: Undermined by External Factors*, *in* 18-3 MIDDLE EAST POLICY 144, 144-160 (2011).

[28] Jeffrey J. Schott, *Economic Sanctions Against Iran: Is the Third Decade the Charm?* Vol. 47 NAT'L ASS'N FOR BUS. ECON. (2012).

should be applicable international standards and UN due process considerations. Specific correlation to international law is essential to ethical cyber employment, and this will likely be the sanctioning power's responsibility during implementation.[29]

CES actions could be undertaken covertly. Many consider covert action statutes and regulations sufficient oversight for covert cyber actions. A post-1947 U.S. covert actions review refers to them as an option between overt military intervention and diplomacy.[30] American constitutional doctrine calls for power separation between legislative and executive branches when authorizing specific Presidential powers. Covert action requirements currently state that congressional committees should be informed with written findings prior to initiation.[31] CES implementation approvals outside the public purview would most likely occur here. Covert actions fall outside typical Title 10 (Military) and Title 50 (Intelligence) authorities, although internal oversight does exist.[32] Working within these guidelines could create oversight for digital actions generating physical effects.

CES employment will likely follow an implementing power's initial sanction declaration and delivery. LOAC questions emerge as some cyber tools are currently

---

[29] Although unethical tool use has been a human possibility since first picking up a stone, one hopes that individuals and nations prefer legal and ethical approaches.

[30] L.K. Johnson, *Intelligence Analysis and Planning for Paramilitary Operations*, 5 J. NAT'L SEC. L. & POLICY 481 (2012).

[31] Aaron P. Brecher, *Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations*, 111 MICH. L. REV. 423, 428 (2012).

[32] U.S. Government. "Armed Forces." Title 10, United States Code. Mar 1, 2012. U.S. Government "War and national defense." Title 50, United States Code. Mar 1, 2012.

positioned within military inventory and under acting commanders. While some scenarios may be considered cyber-attacks, CES does not advocate attacks on sovereign states, instead seeking to enhance existing unilateral or multilateral sanctions. The dividing line remains narrow, but sufficient enough to provide potential national power opportunities. When nations consider actions, which may be regarded as attacks, the Law of Armed Conflict (LOAC) should always be a primary reference. Academic writings have considered legality associated with cyber-attacks in some depth, so only a short overview is presented here.

Four areas are routinely considered as LOAC guidelines: proportionality, necessity, distinction, and chivalry. The best examination emerges from using concrete examples. During later discussion, the current U.S. EO 13660 series describing sanction employment against Russia in the current Ukrainian crisis provides relevant examples.[33] Proportionality prevents force use exceeding those necessary to attain military objectives; so here, cyber microforce should be the minimal force required to deny resources to declared individuals. Force must also be in proportion to the current conflict, for example, nuclear responses are not authorized for an attack involving automatic weapons. Theorized CES employment should not create overtly physically damaging effects, even if secondary or tertiary effects may occur. Necessity means utilizing minimal force to achieve objectives. Executive guidance will help to determine specific objectives. EO 13660 allows the Department of Treasury (DoT) and the Office of Foreign Asset Control (OFAC) to designate sanctioned individuals.[34] Distinction involves

[33] Exec. Order No. 13660, *supra* note 26.
[34] *Id.*

discriminating between combatants and non-combatants to engage with only valid targets. The Geneva and Hague conventions require all combatants to have a commander, fixed insignia, carry arms openly, and conduct operations in accordance with law.[35] Since most EO-identified, sanctioned individuals are non-military, and are not being attacked by physical force, distinction should be waived.[36] Finally, chivalry involves recognizing traditional emblems such as white flags and red crosses. Although they are not traditionally employed during cyber engagements; cyber tools could be constructed to allow humanitarian donations recognized by 50 U.S.C 1702(b)(2) and listed within EOs to avoid sanctioning, and in effect, create a digital Red Cross on network transactions.[37] Thus, any LOAC concerns regarding CES would appear to be initially satisfied.

Recent law of war changes treat cyber as an information weapon. No U.S. congressional limitations restrict cyber separately under LOAC, but a potential for perceived misuse emerges from civilian damages inflicted through indirect effects.[38] The Geneva Convention, Additional Protocol I (API), Article 58 requires military forces to attempt to remove civilian populations from affected areas and avoid locating military objectives near

---

[35] Ingrid Detter, THE LAW OF WAR at 136 (2000).

[36] Cyberattack is commonly defined as, "[a] cyber-attack consist[ing] of any action taken to undermine the function of a computer network for a political or national security purpose[s] . . . . [T]he best test of whether a cyberattack is properly considered cyber-warfare is whether the attack results in physical destruction, sometimes called a 'kinetic effect,' comparable to a conventional attack. Oona Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 826, 841 (2012).

[37] Exec. Order No. 13660, *supra* note 26.

[38] Detter, *supra* note 37, at 273.

densely populated areas.[39] Both sections pose issues if CES strategies involve attacks, which incorrectly identify individuals. Ninety-eight percent of all government communications pass over civilian networks and increase separation difficulties for targeting cyber techniques.[40] Cyber will increase implementation speeds and may cause some selection errors, but also increases correction speeds. The United States is an API signatory, although this particular section still lacks senatorial advice and consent. Further, cyberspace restrictions may require reevaluation of CES strategies if they occur in conjunction with international operations. UN due process standards may be a more beneficial lens to derive future regulations.

UN due process methods include notification, an individual's right to be heard, and actions prior to enforcement.[41] Past UN reports show no existing process fully validates submissions, as any member state may submit nominations at any time. Current U.S. sanctions concerning Russia delivered public notification of their intent through the DoT's website.[42] The UN right to be heard prefers considering individual challenges prior to when nation's implement sanctions. Governments using CES will likely react to an emerging crisis, and individuals would present delisting claims to the UN only after formal sanctions are in place. Finally, no prior due process examples for CES cases exist. Methods could likely follow restricted notification

---

[39] Eric T. Jensen, *Cyberwarfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1549 (2010).
[40] *Id.* at 1533.
[41] Kuho Cha et al., *United Nations Security Council Sanctions and the Rule of Law: Ensuring Fairness in the Listing and De-listing Process of Individuals and Entities subject to Sanctions*, [13 No. 2] THE WHITEHEAD J. DIPLOMACY & INT'L REL., 133-52 (2012).
[42] Exec. Order No. 13660, *supra* note 26.

procedures similar to the US Foreign Intelligence Surveillance Act (FISA) court. Arguments suggest public activities, like Russia's Crimean annexation, self-select certain individuals for retaliation while some persons may remain unaware of their own roles in their nation's actions. Publicly identified individuals could, theoretically, judicially challenge enacted sanctions at any time from declaration through employment. The current U.S. EO 13660 series sanctioning Russia identifies, in section 7, a Presidential determination stating sanction effectiveness depends on no prior notices before initial publications.[43]

Current sanctions have problems, which cyber means could solve. Developing cyber definitions allows a common framework to coordinate activities. Sanctions have been used before in international relations and years of examples demonstrate how and when certain techniques may be applied. Most importantly, studies illustrate where sanctions have success. Reviewing legality and process constraints illustrates where current sanctions are limited in application and a broader CES strategy involving cyber-attacks creates opportunity for policy makers. Using CES strategies to mitigate current sanctions shortfalls requires explaining the interdependence lens underlying cyber means.

II. WHAT STRATEGIES SUPPORT CYBER MEANS?

Interdependence theories state military power's importance decreases as international communication increases, but military cyber means allow for continued influences. Traditional Clausewitzian strategy envisions war as the extension of politics by other means, while modern theorists propose hard, soft, and smart national power

[43] *Id.*

applications. Many nations already employ a mixed power palette to influence international opinions. Cyber must become another brush within the U.S. national toolkit to paint the desired picture for tomorrow's world. The single brush used for traditional sanctions is insufficient, although CES offers a variety of brush sizes.

Cyberspace revolves on information manipulation. Static and dynamic information changes can drastically alter functionality and user impacts. Original functionality studies are too narrow to appreciate cyber usages, as global interdependence trends increasingly gain velocity through new developments. One can see globalism trends in economic, military, environmental and cultural tendencies. These trends are not uniform practices and vary by operational canvasses across the world. Cyberspace elements link functionally through interconnected information, to allow unique channels between individuals. Increased institutional velocities across networks adjusts not only message speeds, but how quickly an organization's structure may change to adapt to incoming information. Complex interdependence theory, while historically focused on softer applications, like monetary policy, allows coercive cyber teeth within sanctioning strategies.[44]

In the past, theorists relied on older strategies to drive cyber implementation without grasping strategic impacts.[45] These shortfalls limited vision and failed to spur creative power employment. Developing cyber means to accentuate cyberpower applications remains theoretically

---

[44] ROBERT O. KEOHANE & JOSEPH S. NYE, JR. POWER AND INTERDEPENDENCE (4th ed. 2012).

[45] Joseph S. Nye & William A. Owen, *America's Information Edge*, FOREIGN AFFAIRS: BLOG (Mar./Apr. 1996), https://www.foreignaffairs.com/articles/united-states/1996-03-01/americas-information-edge.

similar to the advantage gained when air forces improved from ballistic bombs to GPS-guided weaponry. Cyber techniques offer the opportunity to target specific resources, deny access to terrorists and adversary nations, and control global economic channels. Creative approaches ensure policy makers leverage new techniques and domains effectively.

A standard national power toolbox contains Diplomatic, Information, Military, and Economic (DIME) options. Power can be employed creatively anywhere, although targeted trade and financial sanctions are a frequent choice. Targeted trade sanctions disrupt particular commodities, while financial sanctions may blacklist persons and companies, categories of individuals, or target states and wide groups.[46] Blacklists identify individuals with whom the sanctioning entity forbids contact through freezing foreign financial assets.[47] Cyber enhancement allows denying sanctioned individuals, organizations, or assets within non-U.S. locations. The policy maker's only challenge may be deciding whether to characterize cyber-enhanced financial disruption as a hard, soft, or smart power application.

Typically, power uses are divided between hard and soft applications. While power remains the ability to make one act, hard power entails coercive methods like military force, while soft power addresses attractive elements like persuasion. Soft power is often viewed as a kinder, gentler approach to achieve desired end-states. Any targeted

[46] Gordon, *supra* note 20, at 327.

[47] Blacklists describe where a full list of all prohibited individuals is maintained by the controlling entity. In most network security, a blacklist would comprise the IP addresses of known malicious actors or sites the security function did not wish users' visiting.

sanction not including kinetic military force could employ soft power.[48] Cyber enhancement allows military cyber experts to contribute fully to soft power employment. The information revolution creates the illusion all nations possess similar soft power. Soft power influences require transmission mediums and, despite cyber's low entry costs, entry barriers for produced visual media, such as movies, which remains high. If measuring international influence, U.S. targeted sanctions employing soft power in Iran, Egypt, and Syria have been relatively ineffective.[49] Some nations have integrated soft power to negate smaller countries' information gains, although U.S. public successes employing softer, cyber means appears limited.[50] Blending military cyber expertise to CES strategies may regain some international, U.S. advantages.

Channels existing in an interdependent world-view allow smart power means to create effects. Power theories describe behavioral effects as coercion or attraction, while smart power combines hard and soft techniques through contextual intelligence applications. Nye defines contextual intelligence as understanding both the strengths and shortfalls of national, and specifically U.S. power.[51] Smart power through sanctions first appeared in the late 1990's when the United Nation's shifted to targeting financial sanctions against individuals and organizations, rather than

---

[48] Christopher A. Ford, *Soft on "Soft Power"*, *in* 32-1 SAIS REVIEW 90 (2012).
[49] *Id.* at 95.
[50] Nye, *supra* note 10.
[51] Joseph S. Nye, *Get Smart: Combining Hard & Soft Power*, FOREIGN AFFAIRS: BLOG (July/Aug. 2009), https://www.foreignaffairs.com/articles/2009-07-01/get-smart.

entire nations to limit negative humanitarian impacts.[52] Smart power theory describes the U.S. military power as unipolar, because economic relations are multipolar, and transnational relationships as inherently chaotic. While interdependent aspects lend stability to transnational relationships, that stability will be limited physically and temporally. Utilizing contextual intelligence to describe selected power relationships within a narrow scope allows tool development to match desired outcomes.[53] CES strategies are perfectly placed to enhance smart power options.

Cyberspace techniques are as varied as their kinetic cousins with the two most common categories being attack and exploitation. Planning CES strategies requires understanding what constitutes exploitation, when it becomes an attack, and when continuing actions cross state redlines. Experienced cyber theorists still frequently debate where lines between the three definitions emerge. Means labeled as cyber-attack may be necessary to achieve CES objectives. Targeting individuals, just like UN methods, allows CES methods to remain below cyber-conflict standards and redlines while still accomplishing national objectives.

Cyber-exploitation differs from cyber-attack by not fully depriving users of the system value. Martin Libicki provides three exploitation factors; no consequential harm, difficult to detect, and not recognized as *casus belli* by law of war.[54] CES-associated actions may appear as exploitation or attack forms through impacts. Those actions which

---

[52] Wallensteen & Grusell, *supra* note 15, at 208.
[53] Nye & Owen. *supra* note 47.
[54] MARTIN C. LIBICKI CYBERDETERRANCE AND CYBERWAR, at 23 (2009).

become attack may create legal concerns; the strategy should follow similar approaches to drone conflicts, focusing on where a CES cyber-attack creates no physical harm, and prevents an imminent threat. When policy makers plan CES during various international crisis events, financial or resource denial effects without physical damage will likely be a preferred U.S. option. Some attacks will first require exploitation and all exploitation requires prior access. Cyber methods could include denial of service on institutional websites, accessing and changing individual account information, or using realigning previously state funds to support congressionally approved opposition activities either publicly or covertly. Categorizing techniques as attack or exploitation will likely be less relevant to planners than overall sanction effectiveness.

Cyber-attack, from the State Department legal advisor, Harold Koh in a September 2012, US Cyber Command conference, and cited in Rabkin and Rabkin, must cause, "death, injury, or significant destruction [which] would likely be viewed as a use of force".[55] Academic cyber-attack definitions are more loosely structured like Hathaway et al.'s cyber-attack definition as, "any action taken to undermine the functions of a computer network for a political or national security purpose"[56] CES strategies including attack means should center on depriving an individual or organization of an information asset's economic value. Cyber-attacks meeting Koh's definition are usually considered cyber-warfare and may trigger self-defense rights under the UN Charter's Article 51. However,

[55] Rabkin & Rabkin, *Navigating Conflicts in Cyberspace: Legal Lessons from the War at Sea*, [14 No. 1] CHI. J. OF INT'L L. 197 at 200 (2013).
[56] Hathaway, et. al. *The Law of Cyber-Attack*, [100 No. 4] Cal. L. Rev. 817, 826 (2012).

Hathaway et. al. also makes the same differentiation as Koh regarding physical destruction when discussing triggered self-defense rights. CES methods may be considered illegal by the sanctioned country but should not cross any redlines or invite retaliatory attack.

Policy makers remain unconvinced cyber solutions offer valid international alternatives. Libicki in, "Brandishing Cyberattack Capabilities" explains how once a capability emerges, nations will be credited with those capabilities, regardless of actual employment.[57] Cyber-tools will be credited both when adversary systems work correctly and when they fail. Crediting cyber means with attack regardless of employment techniques allows planning to use their full potential. Properly placed messaging could affect one's decision calculus through suggesting unaligned effects actually connect to CES. Messaging resource costs, especially through social media, could be relatively small. Comparatively, the U.S. Department of Homeland Security has spent millions, if not billions of dollars, preparing to defend Critical Infrastructure and Key Resources (CIKR) vulnerabilities from attack. For planners, cyberspace defenses will remain critical and network vulnerability assessments are central within those discussions.

In cyberspace operations, access is paramount. Vulnerability and threat are often paired elements. Conducting cyberspace operations requires developing both a tool and access vector. Multiple versions of both will be needed during any extended sanction efforts. Implementing actors will likely see cyber-sanctioned networks rapidly striving to fix vulnerabilities even if the network intrusions

[57] MARTIN C. LIBICKI, BRANDISHING CYBERATTACK CAPABILITIES, at 12 (2013).

are undetected.[58] Original sanctions tell a bank to deny certain actors their services, CES methods merely tell the network to deny services to digital customers. Closing vulnerabilities will harden the target and require additional resources committed to redesigning networked tools for continued use. Once a vulnerability is closed, new access may be required to reach the same effect. CES techniques will likely need constant development, alteration, and adjustment to reach desired effects.

III. WHAT EMPLOYMENT TECHNIQUES SUPPORT CES?

A key to CES employment is determining which tools generate desired effects. Cyber-enabled actions seek to deny network accesses from targeted actors through multiple means. Several well publicized cyber-attack and exploitation techniques are evaluated here for potential usefulness as a baseline model while the overall employment focus remains on the Ukrainian case. Discussed cyber techniques to complement sanction activities include breach, disruption, functional denial, and global denial. Political and technical limitations are also considered. These CES options provide primarily for targeted potential means in an international conflict. A theoretical Ukrainian CES employment plan, based on current U.S. policy, would identify government websites associated with targeted individuals, public-facing email, or corporate websites. U.S. targets for sanction appear within DoT lists, Executive Orders, and current law. Most nations and cyber-operators guard cyber-attack techniques zealously so using publicized attacks as potential CES foundations avoids wandering into unsupportable debates

[58] Martin C. Libicki, *Cyberspace Is Not a Warfighting Domain*, [8 No. 2] I/S: A J. OF L. AND POLICY FOR THE INFO. SOC'Y 331, (2012).

about how an option could be employed. CES means may vary greatly between nations depending on covert capabilities and accesses.

A. Technique

Modifying public techniques to create unique cyber effects enables wider CES planning without revealing access techniques or zero-days. The first suggested option, breach, evolves from the 2014 Target data breach and DigiNotar certificate theft. The second technique, disruption, examines the Qassam Cyber Fighters' multi-year DDoS against multiple U.S. banks and associated corporate websites. The third suggestion, functional denial, models Russian combined arms methods within the Georgian conflict as well as efforts demonstrated in Crimean and Ukrainian actions. Finally, global denial is largely theoretical and proposed eliminating all cyberspace access for the sanctioned target. Developed options suggest some initial options while leaving the far edges of possibility for later planning.

1. Breach

The first option, breach, exposes network vulnerabilities. Breach means strive to create persistent network access. Digitally identifying individual accounts through national or open-source intelligence utilizes CES strategies similar to the popular Target or DigiNotar data breaches. Breach generates increased access and knowledge regarding activities within crisis areas.

As an example, in 2013, Target, a large US retailer, experienced significant network breaches. This breach used third party vendors for initial accesses, positioned malware on Point of Sale (POS) devices, and removed consumer data

from compromised systems. The breach path obtained over 40 million user credit records and 70 million data files.[59] The two-stage attack succeeded due to careful attacker planning and poor Target security measures. Similar planning methods support CES strategies to demonstrate that sanctioned entities are inadequate in protecting constituencies. Protecting populations from outside threats is vital to both image and operations for most national governments. A government who cannot protect their population could likely lose face during international negotiations and local elections.

Breach means could target sanctioned corporations to generate data for other CES strategies. Russian corporations who experienced continuous disruption, functional denial, and breach would face marketability declines, creating additional government pressures to change policies. Applied pressure seeks CES's end goal through enhancing sanctions against national decision makers. The Target breach collected unencrypted data from POS infrastructure vulnerabilities and used syntactic malware to tag and exfiltrate information. Target's data was transferred to Russian criminals and sold on the black market.[60] This example highlighted organizational and individual impacts

[59] U.S. Senate Committee on Commerce, Science, and Transportation. *A "Kill Chain" Analysis of the 2013 Target Data Breach* (2014). From https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwiO2JX50KfUAhWCSyYKHZeYBhUQFgglMAE&url=https%3A%2F%2Fwww.commerce.senate.gov%2Fpublic%2F_cache%2Ffiles%2F24d3c229-4f2f-405d-b8db-a3a67f183883%2F23E30AA955B5C00FE57CFD709621592C.2014-0325-target-kill-chain-analysis.pdf&usg=AFQjCNFotjLB0rDJZO-j_46n5vWhxJ31wg

[60] Committee on Commerce. *A "Kill Chain" Analysis*, (2014).

available by compromising initial interactions and archival data. These methodologies support a CES strategy. Rather than apply a broad data vacuum, breach tools installed across POS systems could work to deny identified users from reaching their financial accounts. Once monetary accounts are identified, sanctioning agencies could transfer captured funds and account ownership to international aid organizations or selected opposition groups.[61] This transferal approach is similar to the current bill, S939, the "EL CHAPO Act", introduced in the U.S. Congress which proposed using seized property from a known criminal, in this case the Mexican drug kingpin, El Chapo, to fund border security measures.[62]

Individual breaches would highlight those areas sanctioned by U.S. or allied organizations. A single compromised account or system could prove sufficient to deny requisite financial access to key targets. The implemented strategy effects are similar to nationally-sponsored identity theft except using the breach method to support government endorsed options. A national cyber element could obtain third-party credentials, trace accounts, and close personal finance options until behavior changed while maintaining communication channels for conflict resolution. Acknowledging CES acts may benefit sanctioning powers through allowing negotiations while altering regional perceptions. Sponsored government digital

[61] Individual assets may be frozen but the author prefers leaving them within either a locked account or transferred to a holding location rather than disseminated. The outright removal of an individual's property may violate international law even with proper sanctioning.

[62] Rep. Cruz (TX), "Ensuring Lawful Collection of Hidden Assets to Provide Order Act." *Congressional Record* 163: 20, (Feb. 6, 2017) p. S873, Rep. Brooks (AL), "EL CHAPO Act." 115 Congress, 1st Session (2017)

communication would manipulate available venues to transmit desires and terms through controlled channels. If available retail systems are insufficient to support effective sanctions, PoS or similar authentication systems within government websites and networks offer additional breach options.

Breach's real advantage occurs in the intentional wealth redistribution made possible through owning data access. Once shares or accounts are controlled through cyberspace, the sanctioning nation could repurpose those funds to international requirements. The U.S. Congress stated in its House Resolution 499 that Russia should stop using coercive economic measures against the Ukraine and other regional countries.[63] This allows a potential interpretative expansion where those funds should be returned to the Ukraine. Here, the U.S. could adjust financial flows directly rather than wait for Russian government officials to compensate the Ukraine for damages. Data control could avoid the delays experienced in waiting for post-conflict financial resolution with unwilling partners.

Another breach option emerges from studying the sophisticated cyber-attack suffered by the Dutch digital certificate company, DigiNotar. Certificates, a digital financial transaction staple, are essential to secure internet interchange. Digital certificates guarantee three key functions; website authenticity, email, file and programming authenticity and integrity, and confidentiality through public key encryption. DigiNotar's firm was hacked on 10 July, 2011 and false certificates generated. The attack was

[63] Rep. Royce (CA), "Condemning the Violation of Ukrainian Sovereignty, Independence and Territorial Integrity by Military Forces of the Russian Federation." *Congressional Record* 160: 40, (March 11, 2014) p. H2268-73

discovered 19 July and false certificates revoked during initial mitigation. Public notice occurred 28 August and more false certificates, 531 in total, were discovered and mitigated. On 20 September, less than ninety days later, DigiNotar filed for bankruptcy, the firm's integrity irreparably damaged.[64] Manipulating certificates by challenging authenticity, preventing security, or infecting systems with secondary malware could prove vital to coercing sanctioned individuals by manipulating functional abilities and perceived reputations.

DigiNotar's breach used syntactic options and information functionality to manipulate secure communication methods. Simultaneously, the manipulation pulled the economic rug from beneath regional, digital commerce for targeted actors. Manipulation affected DigiNotar and individual's digital certificates and could function similarly through CES. Broadly modifying certificate vendor permissions could camouflage CES breach attempts against sanctioned individuals. One example would be selecting a wide customer list for apparent action when only certain individuals, like the thirty-one Russians indicated by the U.S. EO, warrant deeper influences.

As a theoretical example, a CES strategy using breach against certificates could prevent Bank Rossiya from accessing user data, denying some financial transactions while allowing other customers to use networked services. Certificate denial would acknowledge requested transactions without confirming authentication. Most users experience this when internet browser services prohibit connections due

---

[64] Nicole van der Meulen, *DigiNotar: Dissecting the First, Dutch Digital Disaster*, [6 No. 2] J. OF STRATEGIC SEC. 46, 47-49 (2013).

to unrecognized certificates or mismatched protocols. Individual certificates can be compromised further through additional techniques. Duplicating individual certificates could freeze accounts, transfer property, or generate additional accesses. Certificates fill a dual-role as both a known strength and a vulnerability within financial systems. The DigiNotar hack used this vulnerability to ruin the company as a side benefit of hacking their certificates. All transactions requiring certificates could be selectively affected including; blocking future financial exchange, bill payments, internet shopping, and potentially disabling secure communication. These interruptions could be effective when employed versus senior leaders in Russia, Crimea, or Russian-backed Ukrainian rebels relying on secure communications.

2. Disruption

One example of disruption techniques through DDoS appears against several U.S. bank chains. The Iranian-based Izz ad-Din al-Qassam Cyber Fighter's (QCF) group has conducted cyberspace disruptions against U.S. banks since 2012. Sanctions mirroring QCF behaviors could target identified Russian corporations like the Bank Rossiya. Since September 2012, QCF employed DDoS attacks against multiple U.S. banks including Bank of America, Wells Fargo, US Bank, JP Morgan Chase, Sun Trust, PNC Financial Services, Regions Financial, and Capital One as a supposed retaliation for an anti-Islamic video.[65] QCF is

[65] Emilio Iasiello, *Cyber Attack: A Dull Tool to Shape Foreign Policy*, NATO, 5th International Conference on Cyber Conflict, 1-18 (2013). From https://ccdcoe.org/cycon/2013/proceedings/d3r1s3_Iasiello.pdf

tentatively associated with Iranian and Palestinian groups but continues to publicly deny explicit origins.[66] US enforcement has not conclusively, or publicly, confirmed QCF's origin.

QCF attacks are tentatively attributed to Iran with no formal US indictments. Deceptive techniques disguising QCF's origins likely prevent policy makers from retaliatory actions. CES techniques may conceal effect origins or sanctioning individuals may acknowledge disruption attempts. Any Bank Rossiya or Chernomorneftegaz CES effort could be publicly declared, for example, to highlight international solidarity against a recalcitrant Russia. Declared events may be more effective but also will increase interstate tensions.

QCF attacks strike semantic and syntactic vulnerabilities.[67] Most attacks simply deny customer website access while approximately 25% attempt application layer strikes. Syntactic strikes against applications are disguised in larger attacks and incapacitate a banking infrastructure's web-servers.[68] Syntactically-based server incapacitation could disrupt a bank's long-term functionality. Technique effectiveness measurements should consider attack volume rates or secondary scans showing customer accesses to banking web portals during disruptive strategies. Sanctioning actors should be able to determine how

[66] Matthew J. Schwartz, *Threat Intelligence Can Rebuff DDos Attacks*, Information Week, Apr 22, 2013: 12.

[67] Semantic refers to website defacement and disruption while syntactic references software vulnerabilities.

[68] Robert Lemos, *Large Attacks Hide More Subtle Threats in DDos Data*, Dark Reading, May 18, 2013. From https://www.darkreading.com/analytics/security-monitoring/large-attacks-hide-more-subtle-threats-in-ddos-data/d/d-id/1139783

disruptive CES should be modified to achieve success.

QCF's DDoS techniques do not physically destroy banking capability or intellectual capital but change access volumes and influence customers. QCF's offensive suite included the highest volume DDoS functions at the time, at 70 Gigabits and 30 million packets per second. Security experts note banking corporation's larger infrastructures require increased attack rates for success.[69] High data rates may disguise other intended targets in overall transaction noise levels and allow additional actions. Sanction enhancement strategies using DDoS could include specific individual accounts and targeted corporations. As a potential CES shortfall, undeclared DDoS could be attributed to coincidental criminal action rather than intentional, international influences.

Manipulating QCF, or other DDoS techniques could prevent sanctioned industries from conducting digital transactions. Some industries will only be minimally affected while financial or foreign exchange corporations will see immediate impacts. DDoS functions could slow or stop transactions in generating targeted economic effects. QCF-like techniques could scale to first impede, then hamper, and finally to disrupt digital businesses. Impeded economic functions could include; payroll, banking, ordering, supply, and others essential to large corporations. All functions relate to core sanction elements by denying networked financial operations.

3. Functional Denial

A third CES technique examines Russian methods unveiled during the Georgian conflict by denying cellular

[69] Iasiello. "Cyber attack" 2013.

phones or other services to individuals or corporations. Modern digital lifestyles allow individuals to automate regular bill payments and disrupting these payments disrupts associated services. Effects first appeared as secondary results, and similarly denying phones, cable, internet, or even basic utilities could be effective against sanctioned entities. In August 2008, the Russian Army invaded Georgia and conducted the first, acknowledged, large-scale combined cyber and conventional attack. The two-phased attack began with a 7 August, Russian cyber-strike against Georgian government websites before cyber-targets expanded to financial institutions. Phase one employed semantic DDoS attacks with syntactic options to overwhelm Georgian servers. Denying government availability during the initial Russian invasion demoralized the Georgian populace and prevented effective command and control. Russia's phase two targets featured more extensive DDoS and struck Georgian politician's public-facing email accounts.[70]

Some potential CES techniques emerged in the conflict's second phase. Banking strikes decoupled financial systems from international networks and crippled dependent systems through denying automatic payment avenues; Automatic Teller Machine (ATM) systems, mobile phones with direct deposit, and other assets were all denied.[71] The Georgian cyberspace response was to accept temporary information losses and transfer most information assets to

[70] Paulo Shakarian, *The 2008 Russian Cyber Campaign Against Georgia*, [91 No. 6] MILITARY REV. 63-64 (2011).

[71] Marian Lazar (2012). The Russian Cyber Campaign Against Georgia (2012). In *The Complex and Dynamic Nature of the Security Environment*, 500-506. Bucharest, Romania: National Defense Univ., 2012.

neutral third party, geographic locations such as Poland, Estonia and the U.S.[72] Though physically separated, geographic isolation without network separation does not reduce CES impacts. Information movement did not prevent all of the Russian denial actions in Georgia as localized disruptions continued. CES employment would intentionally deny a sanctioned actors' financial accounts to prevent automatic payment, causing individual decision maker stress, and seeking broader impacts against Russian corporations. The overall CES intent remains shifting Russian national calculus on Ukrainian-associated decisions. Minimizing collateral impacts would allow some network functionality, even in sanctioned systems. Shifting accounts to other servers or nations could occur although cyber techniques can follow targets across geographic barriers.

Mirroring Georgian techniques could form a sanctioning state bot-net as an allied offensive network. The technique appears similar to the QCF scenario while being more easily attributable. A state wishing to publicly confirm their cyberspace options may select this option. Imagine a botnet horde, semantically altering all Bank Rossiya sites to post, "Bank Rossiya has been internationally sanctioned for supporting an illegal invasion by the Russian government against a sovereign state" or other, similar messages. Denying phone lines could minimize secondary effects to the local population who use associated services. Finally, controlling Global Cyber Commons access through network manipulation may allow information regarding crisis

[72] Col. Stephen W. Korns, *Botnets Outmaneuvered: Georgia's cyberstrategy disproves cyberspace carpet-bombing theory* ARMED FORCED JOURNAL (Jan. 1, 2009) Retrieved June 3, 2017 from: http://armedforcesjournal.com/botnets-outmaneuvered/

resolution to be transmitted to sanctioned decision makers.

4. Global Denial

The most impactful CES technique would be global denial. This technique strives to prohibit any digitally supported financial activity, globally, for the sanctioned entity and, for the time being, remains theoretical. There are no demonstrated public methods to support this means. Developing accesses and tools supporting global denials would be time and resource intensive. One envisions entering identifying characteristics within applications to use botnets, worms, or other methods thereby temporarily preventing financial functionality for a network or individual. Modern sanction systems notify banks, review accounts and deny transactions through regulation. Cyber tools would aim to prevent sanctioned individuals from completing any digital transactions, globally. For Russia, global CES denial would block all sanctioned individuals and corporations from completing any digital transaction for non-humanitarian purposes. Funds could be identified and tracked to prevent sanctioned individuals from disguising or transferring assets away from sanctioned techniques. One common sanctioning state concern is that blocked states sometimes no longer possess negotiation channels. Digital enforcement methods may allow communication channels like email or text to remain open despite physical blockades in other areas. These guaranteed channels would allow crisis resolution attempts or further sanction threats to be communicated securely and completely. Ensured digital communication channels could verify message transmission and reception to intended parties. CES allows sanction actions and negotiating resolution in the same, interdependent channel with guarantees provided through

cyber tools to ensure messages are transmitted and received by the intended party in some cases. The channel created to deny financial actions to the sanctioned party, could also be used to transmit to blockaded individuals. For example, think if Stuxnet had left messages inside Iranian systems suggesting which actions were required before centrifuge damaging, cyber activity was turned off by the initial actor.

B. Political and Technical Limitations

CES offers a strong theoretical argument, however, serious limitations do exist including: escalation and redline perceptions, legal constraints, and technical shortfalls. Each limitation possesses potential for policy and operational challenges. However, considering challenges enables developing a well-rounded, foreign policy toolkit including CES.

First, many policy makers fear crisis escalation. An initial escalatory action in many wargames is described as cyber-conflict, which increases or causes misunderstanding of redlines. Most politicians prefer not to see a soft power approach like CES degrade to unrestrained kinetic warfare. The same individuals fear expanding current cyber operations as they imagine all cyber-tools expanding past implanted controls similar to organic viruses. Despite common organic analogies, viruses and bacteria are much more sophisticated than cyber tools and more likely to adapt to new environments than manmade and constrained, cyber techniques. Current U.S. policy allows kinetic combat actions with relatively minor approval processes within declared Combatant Commander Areas of Responsibility. National cyber-tools remain much more tightly controlled than kinetic weapons despite the difference in scope. A 2,000-lb. bomb can be employed against a wide target

variety while cyber tools effect only a unique operating system, application or user. Transferring a constrained cyber method to another system could be considered similar to cross-species, organic virus transmission, possible but not likely. As mentioned earlier, covert operations still require congressional notifications and Presidential findings before action. Required cyber implementations approvals frequently limit offensive cyber techniques to previously approved military actions or require a Presidential finding for covert action. No U.S. government has publicly endorsed offensive cyber methods outside of either of these kinds of military actions.[73] Uncertainty regarding expressed cyber policy or escalation potential may impact U.S. decisions on CES means.

Another escalation element involves perceived international cyber redlines. Redlines provide operational and policy limitations to U.S. actions including those in cyberspace. Policy makers may be disinclined to add cyber provocations to tense diplomatic environments. Libicki argues for probabilistic versus determinist redlines in showing how varied trigger points allow more actor flexibility.[74] Probabilistic elements utilize declared lines, like "if you cross the border, we will respond". Determinist redlines suggest aggregated activity standards for situational responses, like "if you cross the border with a battalion, we may respond, or we may wait for additional actions and respond later". This variability creates monumental

---

[73] Catherine Theoharry & Anne I. Harrington, *Cyber operations in DoD policy and plans: Issues for Congress* Congressional Research Service R43848 at 16 (2015).

[74] Martin C. Libicki, *Two, Maybe Three Cheers for Ambiguity*, in CONFLICT AND COOPERATION IN CYBERSPACE: THE CHALLENGE TO NATIONAL SECURITY, by Panayotis A. Yannakogeorgos & Adam B. Lowther, 27-34 (2014).

difficulties when evaluating how the Russian government would respond to CES supporting the Ukraine. Evaluating state redlines should be no different than any other sanction although policy makers will require time to adapt to new domains like cyberspace. One can think of the first CES action as similar to the Cuban Missile Crisis, one knows new tools are available, but not how the other will use them. Adaptation will require similar timelines to when national strategies incorporated nuclear deterrence models, full-spectrum operations, and smart power techniques. CES success will likely go far to change hearts and minds on cyber-weapon employment.

Next, legal constraints pose potential limitations. Operationally, policy makers will require demonstrated planning showing how CES techniques meet U.S. laws, LOAC considerations, and UN guidelines. Any involved allies may pose additional constraints. As seen during Operations ALLIED FORCE and UNIFIED PROTECTOR, sometimes NATO partners have additional restrictions on appropriate responses. Kinetic actions require legal review before implementation and CES will likely require qualified lawyers evaluating options. The constantly changing restrictions and sheer volume of U.S. law make it impossible to consider even a fraction of potential alternatives here. However, the case study examines published U.S. policy and potential CES techniques in the Ukrainian crisis.

Third, technical shortfalls exist in the accesses and tools needed to affect digital networks. In simpler terms, one needs the door key, the knowledge of what is behind the door, and the capability to manipulate the underlying environment. Cyber tools have significant intelligence requirements for use, especially within restrictive environments like government networks or private digital accounts. Cyber-attacks require established access into

targeted systems and networks. Access provides the right path to manipulate a network and requires substantial intelligence prior to implementation. Each previous technique category highlighted known accesses and vulnerabilities. Intelligence operations need to recognize, discover and manipulate potential gaps before CES employment.

Possessing the right tool is not the only limiting factor. Cyber-associated intelligence agencies typically develop accesses for intelligence value and may not want to burn those accesses for sanction effects. Developing access for CES strategies requires a different focus and possibly organic access control by associated agencies. Coordinating access development and control across multiple agencies remains an issue for additional discussions. Obtaining timely access may be initially challenging but still likely faster than the decades one could spend enforcing ineffective Cuban and Iranian sanctions.

Associated with access is the difficult task of understanding how and where cyber techniques can be applied. Successfully attributing incoming cyber-attacks remains as challenging for defenders as discovering original vulnerabilities and accesses for attackers. Websites and tools offer penetration tips in both white-hat and black-hat applications. The most effective CES techniques may use microforce influences to disrupt or deny an individual's information accesses prior to affecting national decision calculus. All proposed techniques begin with finding a small vulnerability while ultimately affecting large activity swathes. In modern international relations, cyber vulnerabilities in corporations or leadership channels appear as common as finding national economic trade options for traditional sanctions. Individual effects require careful planning to prepare a selected network for desired outcomes.

Planning will also help minimize secondary and tertiary effects on the broader population. Resource investments should not vary greatly between large scale effects and individual sanctions.

After obtaining access and evaluating vulnerabilities, one must have the proper tool available. Cyber-weapons are difficult to stockpile usefully and predictably. The techniques above suggest where options exist although all will require design modifications before use. Starting with disruption, all presented techniques were narrowly targeted based on objectives. CES techniques require the same focus. The next crisis' necessary cyber-tool may not be the one employed previously. Cyber restricted employment comparisons to kinetic options shows the benefit and disadvantages when managing government acquisition needs against future crisis. However, cyber offers the only reversible weapons in modern history. The theory, proposed by Rowe et. al, advocates releasing only cyber-weapons whose effects may be reversed once a desired impact is achieved.[75] In the Ukraine, one could impact the multiple individuals mentioned and remove those effects as desired actions occur. This method blends neatly with targeted sanctions by removing any damage once all parties reach an agreement, unlike kinetic strikes destroying command structures. These technical limitations may seem initially daunting but are no more so than similar tactical and technical challenges faced during either the Combined Bomber Offensive or the Apollo Program. Just like those concerns, resources and national desire will likely help solve

[75] Neil C. Rowe, *et al. Challenges in Monitoring Cyberarms Compliance*, in CONFLICT AND COOPERATION IN CYBERSPACE, by Panayotis A. Yannakogeorgos & Adam B. Lowther, 81-99 at 92, (2014).

this problem.

IV. A UKRAINIAN CASE STUDY

CES uses cyber means to improve financial sanction effectiveness in achieving U.S. national ends. The suggested strategies above are applied here to the recent Ukrainian crisis. CES complements U.S. policy by implementing economic sanctions against individual and corporate actors to manipulate international decision-making calculus through microforce applications. The cyberspace domain's unique advantages allow CES to apply pressure differently than traditional sanctions. Techniques affecting governmentally sanctioned entities already exist in the public cyber domain. Increasing economic sanctions overall effectiveness without incurring national costs in either tangible, such as military blockades, or intangible, such as public image, areas is a valuable diplomatic tool. The case presented here allows U.S policymakers to verify the CES guidance, standards, and application employed as well as projected effectiveness in the Ukraine crisis.

This case examines how U.S. policy sets cyber guidance, what regional conflict standards exist, how CES techniques may be applied, and what effectiveness metrics are needed. First, guidance evaluates whether sufficient state controls exist to impose cyber sanctions. Most guidance emerges from public policy statements, legislative acts, or national decrees. Second, standards are assessed by determining possible and effective CES methods against cyber techniques already employed regionally. Third, and potentially the most controversial section, several CES strategies are suggested. As a strategic look, even though discussing techniques, this area is hypothetical since no tool modeling conducted against regional networks has occurred.

Finally, CES effectiveness metrics are only suggested because implementing any new action can be difficult if one does not know where national success may lay in any particular case. No sanction can succeed without positively changing the decision calculus involving the sanctioned state. These areas suggest how CES extends current policy and highlights how cyber means increase sanction effectiveness in one scenario.

A quick crisis background is essential for proper orientation. The regional crisis began late 2013 over whether Ukrainian international trade agreements should be European-focused or maintain a Russian preference. The traditionally Russian aligned Ukrainian government clashed with their people before President Yanukovych and his supporters fled the country on 21 February 2014. Immediately after, a Ukrainian political coup on 27 February 2014 completed the political transition to a European-centric focus and activists from both pro-Ukrainian and pro-Russian sides took to the streets to protest as neither side was content. The most severe clashes between the pro-Ukrainian and pro-Russian groups initially occurred in the Crimean province.

On 1 March 2014, Russian President Vladimir Putin received parliamentary approval to invade the Ukrainian regions and deployed troops charged with protecting Crimean-based ethnic Russians. On 16 March, Crimea held a provincial referendum and overwhelmingly voted to join Russia with a 96% voter turnout and over 80% of the populace voting for secession. Although the Ukraine, the U.S., the European Union and several other nations denounced the vote as illegal, Russian President Putin annexed Crimea the following day.[76] The U.S. and the

[76] Steven Woehrel, *Ukraine: Current Issues and U.S. Policy*, at 4, Congressional Research Service, (2014).

European Union have levied numerous sanctions while diplomatic attempts at formal conflict resolutions continue. Ongoing activity shows border conflicts, Russian support for separatists inside Ukrainian territory, and no apparent crisis resolution in the near term. The Ukrainian conflict provides a useful framework to show how a CES could be employed inside of current national guidelines. Attempting to influence Russian decision making through CES begins with understanding what U.S. national leadership's ends are for the Ukrainian crisis.

A. CES Guidance

When employing CES, one should first consider whether national guidance appears sufficient to develop clear ends. U.S. guidance regarding Ukrainian sanctions is sufficient to implement clear objectives for the following reasons: (1) US Executive Orders govern sanction policy in the region, (2) the Department of Treasury's published guidance implementing sanctions are detailed down to the individual, (3) U.S. legislation including congressional actions and Executive Orders define the Ukraine as a national security interest. US Executive Orders (EO) govern sanction policy within the Russian region. Presidential EO and the DoT's Office of Foreign Asset Control (OFAC) expansions sanctioning Russia is sufficiently directive to generate microforce options, suggest accesses, and direct priorities for CES planning and employment.[77] The multiple

[77] Department of the Treasury. UKRAINE AND RUSSIA RELATED SANCTIONS http://www.treasury.gov/resource-center/sanctions/Programs/Pages/ukraine.aspx (last visited June 3 2017).

EOs issued by President Obama identified those forces undermining Ukrainian stability and integrity as an emerging US national security threat. Four orders, EO 13660, EO 13661, EO 13662, and EO 13685 are currently published on the current crisis with each addressing slightly different categories.[78] The first three highlight Ukraine while EO 13685 addresses Crimea. The orders identify both individual and corporate actors with a range from politicians and generals to banks and factories. The description's breadth includes categorical guidance to sanction those who contribute to Russian military efforts. The broad guidance would allow further sanctioning activity against almost any Russian economic industrial function.

EO guidelines clearly define initial sanctions, though depend on OFAC development for additional emphasis

[78] The first order, issued 6 March 2014, declares restraints on persons identified by the Secretary of Treasury and State, within five categories, as contributing to Ukrainian unrest. The second EO, issued on 16 March, continues to expand, and provides four more categories including Russian government officials and arms merchants. The second EO further identifies seven Russian government individuals directly as sanction targets. The third EO provides three more categories, but highlights any individual operating within Russian Federation economic sectors including: financial services, energy, metals and mining, engineering, defense or related material. The description's breadth allows almost any Russian economic industrial function to receive sanctions. All EOs order any property and interests currently residing within the US, transferred later or within control of any US person blocked and states they, "may not be transferred, paid, exported, withdrawn, or otherwise dealt." THE AMERICAN PRESIDENCY PROJECT *Blocking Property of Certain Persons Contributing to the Situation in Ukraine*, Exec. Order No. 13660, 79 Fed. Reg. 46 (March 10, 2014); THE AMERICAN PRESIDENCY PROJECT, *Blocking Property of Additional Persons Contributing to the Situation in Ukraine*, Exec. Order No. 13662. 79 Fed. Reg. 56 (March 24, 2014).

points. No individuals were immediately identified by OFAC after publishing the initial EO. After the second EO, four more actors were identified for sanction by OFAC in addition to naming seven other actors through annexes. Following the third EO, 20 more individuals and Bank Rossiya were identified by OFAC as sanctioned entities. As Ukrainian events continued to degrade through 2014, seven additional Crimean individuals and a Crimean gas and oil exploration company, Chernomorneftegaz, were sanctioned. The OFAC's Sanction's Program, has developed a Sectoral Sanctions list to identify all individuals available for sanction through at least physical addresses.[79] Other information associated with listed individuals includes: name and aliases, date and place of birth, and official positions. Corporate identities feature: names, physical addresses, web addresses and emails. All information can be supplemented by intelligence sources once a CES strategy is implemented

The provided descriptions highlight the opportunity for CES in the Ukrainian conflict. U.S. policy identifies individuals and corporations who are sufficiently distinct from others to meet at least LOAC definitions, if not other international law requirements. Cyber operators, following Presidential guidance, could use multiple techniques against individuals, corporations, or government agencies. Individual, identifying characteristics will allow techniques to use narrow effects or manipulate entire networks. The recent SCADA attacks against the Ukraine in 2015 demonstrated their network vulnerabilities.[80] The details

[79] Office of Foreign Assets Control, http://www.treasury.gov/resource-center/sanctions/Pages/default.aspx (accessed April 15, 2014).
[80] Robert M. Lee *et al., Analysis of the Cyber Attack on the Ukrainian Power Grid*, (2016).

sufficiently distinguish between sanctioned individuals and potentially innocent victims.

U.N. sanctioning processes prefer to notify affected and sanctioning governments before implementing sanctions. A request for exception to U.N. due process and prior notice rules appears within section 7 of all currently referenced EOs. This section 7 exception states the U.S. will begin sanctioning activities without notifications as early action U.S. legislation supports the EOs desire to act without prior notification. The guidance here is H.R. 4152, *To Provide for the costs of loan guarantees for Ukraine*, passed on 3 January 2014, and states US policy as, "to use all appropriate economic elements of US national power, in coordination with US allies to protect the independence, sovereignty, and territorial and economic integrity of Ukraine"[81] Another relevant Act HR 4278, the Ukraine Support Act, explicitly refers to sanctions and passed the House on 27 March 2014.[82] This House bill became S2183 in the Senate and a part of public law in April 2014.[83] HR 4278 specifically provides sanction guidance both complementing published EO and expanding their scope. The most recent bill introduced was HR 830, "Stability and Democracy for Ukraine" which shows a continued desire in

[81] Rep. Rogers (KY) *Support for the Sovereignty, Integrity, Democracy, and Economic Stability of Ukraine Act of 2014*, 22 U.S.C. 8901, Apr. 3, 2014, P.L. 113-95 (113th Congress), H.R. 4152.

[82] Sen. McConnel (KY), *United States International Programming to Ukraine and Neighboring Regions*, 22 U.S.C. 6211, Apr. 3, 2014, P.L. 113-96 (113th Congress), S.2183, H.R.4278 [introduced by Rep. Royce (KY)].

[83] Sen. McConnell (KY) *United States International Programming to Ukraine and Neighboring Regions*, S. 2183, Apr 3. 2014, P.L.113-96 (113th Congress).

section 201 to prohibit financial transactions with Russia, and reaffirms the previously mentioned Executive Orders.[84] The guidance extracted from U.S. Presidential EO, DoT actor development, and existing US legislation demonstrate sufficient guidance to implement CES against potential vulnerabilities within the Ukrainian conflict.

B. CES Standards

The next strategic step would assess regional standards through analysis of currently employed cyber techniques throughout the region. LOAC proportionality means using minimal force and employing similar methods. Standard cyber techniques used by either Russia or the Ukraine will likely limit how CES techniques are employed. Detected methods may legally justify equivalent U.S. CES techniques against Russia. Simply put, if Russia introduced cyber-weapons into the conflict against the Ukraine, such as the 2015 and 2016 SCADA attacks, no legal reason exists why the U.S. and allied nations should not use CES techniques to resolve the conflict.

One cyber-weapon weakness regards whether a tool can be captured and reprogrammed to affect original users. Part of the Ukrainian, and U.S., risk is whether Russian cyber expertise is sufficient to subvert CES techniques and redirect them. Ukrainian cyber activities suggest no new strategies are being introduced although, at the tactical level, several new applications have appeared. Since 7 March 2014, the Ukrainian conflict has included publicly recorded cyber events on both sides.

---

[84] Rep. Engel (NY) *Stability and Democracy for Ukraine Act*, H.R. 830, 115th Congress, 1st Session (2017).

Initially, on the Ukrainian side, the pro-Ukrainian Kibersotnya group's attacks directly defaced Russian news websites with Distributed Denial of Service (DDoS) techniques.[85] Connection through the top-level public and private websites were blocked by the defacements. Non-specific but Ukrainian associated hackers have claimed to have rerouted links, stolen data, and compromised passwords. DDoS attacks prevented individuals from reaching government sites in order to deny support and direction during the crisis. Initial FSB attribution credits multiple Ukrainian hackers with defacements without a final judgment.[86] Overall, both identified techniques influenced a wider spectrum than this CES proposal, probably due to the overall directional lack underlying the Ukrainian cyber effort. CES's disruption, breach, and functional denial techniques all appear within Ukrainian cyber activity.

On the Russian side, a pro-Russian group, Cyber Berkut, used DDoS tools against NATO and Ukrainian media websites. Cyber Berkut initiated attacks after NATO's public statement denounced Crimea's independence

---

[85] Government and Commercial systems included the Russian presidential website, Central Bank of Russia, Ministry of Foreign affairs and the energy consortium Gazprom.

[86] *The Ukrainian Crisis - A Cyber Warfare Battlefield*, OSNET Daily. April 10, 2014. http://osnetdaily.com/2014/04/the-ukrainian-crisis-a-cyber-warfare-battlefield/ (accessed April 11, 2014). The FSB, Federal'naya Sluzhba Bezopasnosti, or Federal Security Service, was created from the largest remaining element of the KGB after the dissolution of the Soviet Union. Originally focused only on counterintelligence, they have since assumed other duties and function as a national intelligence agency for Russia. Andrei Soldatov, & Irina Borogan, *The Mutation of Russian Secret Services*, Argentura.ru. 2011, http://www.agentura.ru/english/dosie/mutation/ (accessed May 3, 2014).

referendum and deployed personnel to Kiev.[87] A second local hacktivist group, Anonymous Ukraine (AU), appears in cyber activity dating back to November 2013. In May 2014, AU released intercepted emails between a US Army Attaché and a senior Ukrainian Army Official coordinating for potential U.S. aid and support.[88] Again, one sees the prevalence for broad activity rather than targeted events coordinated within a central plan. Other government emails were likely included in the interception. The email intercept shows government officials within both conflicting parties and outside entities as validated vulnerabilities. Russian disruption and breach techniques mimic the same proposed CES options.

One regionally unique cyber-attack does appear with a named infiltration. Regional security filters detected a Russian military cyber espionage tool, known as Snake or Ouroboros, throughout Ukrainian information systems. Snake implantation allows operators complete network access but may include as yet undetected clandestine destructive options. Some cyber techniques can conceal additional microforce techniques against specific systems within the overall code. Stuxnet demonstrates where a tool designed for information gathering also affected centrifuge operations. Since 2010, fifty-six Snake infections occurred globally with thirty-two Ukrainian networks overall, and twenty-two since January 2014.[89] Undetected infections

---

[87] Matthew J. Schwartz, *DDoS Attacks Hit NATO, Ukrainian Media Outlets*, DarkReading. March 17, 2014. http://www.darkreading.com/attacks-and-breaches/ddos-attacks-hit-nato-ukrainian-media-outlets/d/d-id/1127742 (accessed June 4, 2017).

[88] *Id.*

[89] Sam Jones, *Ouroboros: Cyber Snake Infects Ukraine Computer Networks*, FINANCIAL TIMES, (Mar 7, 2014).

could be much wider. Snake mimics the CES suggested breach technique.

The broadest Russian event was the attack on Ukrainian power systems during the December 2015 to January 2016 period. The event consisted of a hacker attack on multiple Ukrainian corporations with the goal of disrupting power distribution in the short-term. This was the first recorded attack conducted against a SCADA system to specifically prevent power distribution. Sandworm, a Russian-backed hacker group, used Black Energy 3, a malware tool, to infiltrate business systems and then digitally move from those systems to field sites where actual power distribution was influenced.[90] The hackers likely began reconnaissance six to nine months prior to the actual attacks. The attack ultimately blocked power to 225,000 customers over several hours.[91] Also noted was KillDisk malware use to delete information from infected computers and slow the recovery processes.[92] The same software, Black Energy 3 and KillDisk, was also noted during the same timeframe on a Ukrainian mining company and a large railway operator.[93]

---

[90] Danika Blessman, *Black Energy Malware is Back and Still Evolving*, (2016) https://www.solutionary.com/resource-center/blog/2106/01/black-energy-malware (last accessed June 4, 2017).

[91] Robert M. Lee *et al.*, *Analysis of the Cyber Attack on the Ukrainian Power Grid.* (2016).

[92] Symantec Security, *Destructive Disakil Malware Linked to Ukraine Power Outages Also Used Against Media Organizations*, (2016) https://www.symantec.com/connect/tr/blogs/destructive-disakil-malware-linked-ukraine-power-outages-also-used-against-media-organizations?page=1 (last accessed June 4, 2017).

[93] John Leyden, *Black Energy Trojan Also Hit Ukrainian Mining Firm and Railway Operator*. (Feb. 15, 2016)

Both Ukrainians and Russians have deployed cyber tools regionally. Choosing cyber methods means both parties seek domain influences to favorably affect the conflict's eventual resolution. Selected and confirmed cyber targets to date include government websites, banks, and personal emails. All will likely continue to appear on future vulnerability lists. Additionally, both short duration influences and longer-term infiltrations are present. LOAC analysis suggests CES appears proportional with the existing techniques. In a broader sense, CES may be more humanitarian than infantry attacks or no-fly zone enforcement. U.S. CES implementation is well within overall legal and regional standards. Both standards and guidance sections favorably support CES employment.

C. CES Techniques

While discussed above in greater detail, CES techniques for breach, disruption, functional denial, and global denial are suggested here as strategic options. Specific vulnerabilities are referenced from above sections. This element covers how each item could alter the conflict and lead to rapid resolution. Actual implementation will rely on developed tools and accesses, most likely outside of public discussion channels. After all, fully identifying tools and vulnerabilities prior to use helps defenders patch those same channels.

The first implemented technique should be breach. Much as with the Snake technique above, breach methods

---

http://www.theregister.co.uk/2016/02/15/blackenergy_trojan_trend_micro (last accessed June 4, 2017).

introduce all sanction accesses. Breach techniques generate accesses and intelligence to increase later effectiveness. Studies, such as the one by Aaltola et. al., demonstrate methods patterning networked activities through the global commons and show potential vulnerabilities.[94] CES strategies could use techniques to rapidly create multiple accesses across wide-ranging regional systems. Multiple breach methods could generate increased data and minimize mitigation by local cyber-security due to confusion and complication. Breach should be publicly denied and minimally impactful on system performance to maximize the tool's lifespan in affected systems. Examples of breach successes could be used during negotiations to demonstrate potential power.

If breach alone is insufficient to reduce a crisis, disruption attempts could be introduced. The discussed DDoS methods do not require internal network access but only external port awareness. As seen with QCF attempts against U.S. banks, increasing the overall traffic for corporations can reduce digital transactions. The available bot-net size, strength, and tool sophistication will drive overall effectiveness. Disruption can affect OFAC designated individuals by reducing their ability to coordinate government efforts. In-person meetings may, of course, still occur while reduced internet access, especially across large areas will slow Russian government response times.

Once breach or other methods generate sufficient access, if further escalation is required, functional denial can be used to prevent Russian individuals and corporations from conducting activities. Combining phone service functional denial with internet disruption as in the Georgia

[94] Mika Aaltola *et al.*, *The Challenge of Global Commons and Flows for US Power*, (2014).

example will prevent coordinated Russian responses. Functional denial should also strive to decouple corporations from their international financial channels. Most large corporations, especially the Russian oil and gas corporations, depend on international income. This method, paired with analysis, can identify sanctioned individual and corporate accounts to digitally separate the funds. Once separated, funds may be transitioned to generate Ukrainian humanitarian aid, restore the stolen accounts in HR 4152, or any other financial relief.

Finally, CES global denial, if tools and vulnerabilities are available, would eliminate Russian access to any cyberspace options. Other than specific white-listed options to encourage communication and resolution, removing internet access within a modern society could generate significant impacts. Initial implementation should only deny labeled sanctioned individuals. Subsequent deployment could reach OFAC suggested, rather than specified, Russian targets. Implementing global denial would remove the need for either disruption or functional denial but is potentially more difficult to implement.

Operational means surely exist to employ all developed CES strategies in the Ukrainian crisis although whether any nation also possesses the desire to employ these techniques is a separate question. Each method suggests where targets are available and implementation can be conducted while limitations including access and tool availability were discussed earlier. Further, once implementation occurs, it will be important to understand where Russian redlines exist. Redlines may cover how fast, and to what degree CES can be implemented without impacting non-cyber areas. As a technical alternative, in each area, CES methods provide expanded options to implement an already approved sanction regionally rather

than merely preventing Russian access to U.S. and EU accounts through traditional means as occurs today. In many cases, these funds may already be undervalued or difficult to reach. Expanding sanction options logically means regional pressure will increase and may drive more expedient conflict resolution. Overall, sanction effectiveness rests not within the specific techniques but in altering national decision calculus.

D. CES Effectiveness

CES employment goals are interrupting financial flows without humanitarian impact to affect national decision calculus. CES effectiveness means impacting sanction enforcement to drive conflict resolution quicker, at lower cost, and with less negative humanitarian impact than traditional sanction enforcement or military options. Since traditional sanction timelines can be measured in decades, projected cost over time versus a faster resolution with CES is an important effectiveness consideration. Since CES has not been implemented anywhere, no quantitative data exists to support potential cost savings. However, all sanctions evaluate three qualitative effects after implementation; (1) does the sanctioned state begin or continue useful discussions with the implementer, (2) does depriving resources shift regional power, and (3) whether increased sanctions are required. State negotiation involvement is a binary measurement even if diplomatic teams can add various qualitative standards. Diplomatic discussions requesting sanction abatement may also indicate success. Additionally, functional denial or breach may impact individual negotiators who will be measured through their participation or communications passed through white-hat CES channels. National intelligence services may also

uncover specific, individual impacts, and reduce uncertainty volumes regarding future conflict resolution negotiations.

Effectiveness measures should relate how implemented CES changes negotiations between the targeted state and the implementing country. Currently, the U.S. continues discussions with Russia regarding the Ukraine but no conflict resolution is imminent. Some Treasury metrics can be employed to assess status. These measures may include how many resources were employed to achieve sanction effects versus the reduction in financial power to sanctioned entities through trade volume, direct investment, or national economic products. Although not a total measurement, when Russia invaded the Ukraine on 1 March 2014, a ruble was worth .02775 U.S. Dollars (USD). One year later, one ruble was worth .01638 (USD), a drop of just over 40% demonstrating a significant loss in individual purchasing power. The lowest point over the same interval was .1435 (USD) but the ruble does appear to have stabilized at between .17 and .18 (USD) during April to June 2015.[95] Even those numbers still show a 30% comparative decrease. Prior to the 1 March date, over the past ten years, the Russian ruble had only closed lower against the dollar over a several day span in February 2008.[96] Not directly attributable to sanctions, similar or additional metrics could show increased effectiveness for CES. Public statements reflecting on sanctions can be measured by frame and discourse style analysis to assess CES's regional power impacts. Data to measure all areas can emerge from national intelligence

[95] XE.com."RUB/USD chart" http://www.xe.com/currencycharts/?from=RUB&to=USD&view=2Y (accessed June 4, 2017).
[96] *Id.*

services, trade reports, media publications, or other social sources.

Shifting regional power can be measured either quantitatively or qualitatively. Russian military deployments can be tracked through both measurements. CES effectiveness metrics could track order of battle intelligence and supplies delivery to determine whether funds exist to move military units in the affected area. Social media and news interviews can show both equipment supply rates and morale for troops at economically depressed locations. Supply chain statistics from sanctioned corporations may also be measured. If leadership decides to shift funds directly to opposition groups; both transfers and end-user effectiveness with those funds can be evaluated by trade volume and secondary effects. For example, funds held by Leonid Slutsky, a State Duma Deputy identified in the 16 March EO, could be used for the desire expressed in HR 4152 sec 3.9 to support Ukrainian Government efforts, "to recover and return to the Ukrainian state funds stolen by former President Yanukovych..." and others. Effectiveness could be measured through either funds removed, or funds returned to the Ukrainian state as a percentage of the overall totals reported stolen. Breach, disruption, functional denial, and global denial methods all assist in providing relevant data to improve sanction effectiveness.

The final effectiveness question assesses whether increased sanctions are likely to achieve desired effects. This assessment is forward looking through using behavioral trends. Measurements may be scaled regarding state political shifts referencing particular positions. Both intelligence sources and media reporting will inform planners regarding increased sanction necessity. In Russia, some sources may highlight discrepancies between original, international agreements and subsequent actions. One example is the

punitive trade measures Russia has imposed on Ukraine, Moldova, and Georgia.[97] These show how Russia has tried to alleviate the gap in their own finances through punitive tariffs on neighbors. Scaling future CES or other sanctions to influence emerging situations will largely depend on the sanctioned countries' perceived responses. For the Ukraine, policy makers will likely set timelines for scaled Russian responses such as government statements, actions like withdrawing troops or establishing weapons cantonments, and full crisis resolution. If timelines are not met, additional sanctions can be undertaken. When timelines are met, cyber effects can be quickly reversed. CES generates increased effectiveness during scaling because since techniques allow escalation, or reversal through altering coding. It is much easier to undo an IP address within code than rebuild a fallen bridge. Reversibility within traditional sanctions can be similarly slow. One important policy consideration will be how many resources are required to scale CES effects. Specific metrics to measure CES effectiveness in each situation will also require further development.

V. CONCLUSION

Cyber Enhanced Sanctions are not merely more cyber-warfare methods but a strategic attempt to bring new tools into international relations. Planners have sought to implement targeted sanctions for twenty years by purely diplomatic measures but cyberspace microforce effects may tip the balance. Some limitations exist regarding willpower,

---

[97] Denis Cenusa, *et al*, *Russia's Punitive Trade Policy Measures towards Ukraine, Moldova and Georgia*, Centre for European Policy Studies Working Document 400, September 2014.

legality, or tools and access but most can be alleviated through discussion and planning. Even legal questions can be addressed through constructivist activities in normative construction such as those used when accelerating President Obama's drone war.[98] If limitations are mitigated, CES will expedite effects compared to traditional sanctions by bringing the opposing state to the bargaining table, shifting regional power balances, or threatening increased sanctions.

The examined areas demonstrate where CES has applicability and will likely improve conflict resolution within the Ukraine. Existing guidance clearly demonstrates how CES could be applied within the scenario. Standards show where CES fits within international legal guidance and regional standards. Technique implementation demonstrates specific areas where CES will improve national power means. Finally, the effectiveness summary demonstrates how CES strategies can be measured against commonly regarded sanction metrics, if implemented. All examined areas show where CES could improve financial sanctions applications within this crisis. From the Ukrainian standpoint, CES is a tool that policy makers should consider examining for inclusion within the smart power toolkit.

CES strategies may provide ways to improve financial sanction effectiveness in achieving national power ends. Cyber suggests precise options are possible while meeting nebulous financial and political guidelines and still remaining inside international legal standards and other agreements. Traditional sanctions are difficult to employ and may require a decade's long commitment without achieving significant effects. In today's interdependent world, being

[98]Jeffrey Lantis, ARMS AND INFLUENCE: U.S. TECHNOLOGY INNOVATIONS AND THE EVOLUTION OF INTERNATIONAL SECURITY NORMS, (2016).

able to apply effects across multiple channels and alter those effects to dynamic situations is an invaluable tool. Similar to this method are other common debates such as identifying cyber-weapons through block-chain techniques or tool signatures. Effective sanctions in today's connected environment requires learning new means; cyber techniques may offer those solutions, or at least, expanded options.

The continuing Ukrainian dispute with Russia demonstrates an international crisis where financial sanctions, as they exist today, seem incapable of reaching a resolution within a reasonable time. Ongoing hardships for the Ukrainian people will only be resolved by forcing Russia's hand to end the conflict. Smart power options generated through CES strategies and cyber employment offers expanded opportunities. Developing and implementing Cyber Enhanced Sanctions in accordance with published policy and legislation will increase economic sanction effectiveness. Publicly available tools demonstrate several fundamental approaches including: breach, disruption, functional denial, global denial, or combinations of the same. All techniques could be modified for emerging policy and capability restraints or planned as wholly new options.

One of CES's most appealing options to any leader should be the available malleability including identifying specific actors, reversing effects, and whitelisting secure communication channels. These benefits allow national leaders to scale sanctions to fit every developing crisis rather than being a cookie-cutter tool. In addition to scaling, these cyber enhancements will allow some mid-level, sanctioned leaders to negotiate without navigating national hierarchies, potentially avoiding their leadership and crafting alternative solutions.

CES benefits should, in time, make this option an essential component in any national economic strategy through increasing overall sanction effectiveness. Improved effectiveness occurs in three areas: generating increased intra-state discussion opportunity, shifting regional power between internal players and providing expanded options when required. Thirty years of implementing minimally effective Iranian sanctions and Russian leaders continuing to ignore current US sanctions clearly means additional tools are badly needed as part of the U.S. toolkit.

CES allows sanctions, on political leaders, to be adjusted dynamically rather than waiting for regulatory and legislative action. Cyber-enhanced Sanctions (CES) demonstrate the potential means to increase financial sanction effectiveness and achieve national ends without committing costly or politically sensitive military forces. CES should be the first power step for the U.S. in any foreign crisis requiring sanction. Even if military forces have the only expertise to support CES, it will still be better than the massive financial and physical commitments required for conventional wars in distant lands or non-effective traditional sanctions. CES strategies may generate substantial and measurable success for national policy makers without decade-long commitments to sanctions or boots on the ground. In sum, implementing Cyber Enhanced Sanction strategies with the discussed guidelines and potential techniques appears both possible and effective in the near to mid-term as an option in the U.S. foreign policy toolkit.

North Korea: The Cyber Wild Card 2.0

Rhea Siers*

NOTE: This article was written in large part prior to the cyber actions against SONY. Given recent events, we are republishing this article to provide insights on the growth of North Korea's cyber capabilities.

If you are worried about North Korea's nukes, you probably should be even more concerned about Pyongyang's cyber weapons. Much has been made of the alleged attribution of North Korea for the cyber attacks against SONY. But even prior to the SONY fracas, there was considerable concern about North Korea's recent attacks against on several South Korean institutions involved in security research.[1] In fact, following these security related incidents, Hewlett Packard provided a detailed analysis of North Korea's cyber apparatus and capabilities.[2] Certainly, the North Korean attacks against the South demonstrate a degree of cyber capability, but the real question is whether North Korea sees cyber attack against the US, specifically

* *Rhea Siers, J.D.* is currently the Senior Fellow for Cyber Policy and Law at the Institute for Information Infrastructure Protection and a member of the adjunct faculty at the Elliott School of International Affairs, GWU as well as Johns Hopkins University. She is also a Senior Subject Matter Expert at RANE, the Risk Analysis Network and Exchange and Special Counsel at Zeichner, Ellman and Krause, New York.

[1] Lucien Constantin, *Cyberspies attack key South Korean institutions, North Korean Hackers suspected*, PC WORLD, http://www.pcworld.com/article/2048580/cyberspies-attack-key-south-korean-institutions-north-korean-hackers-suspected.html.

[2] HP Security Research, *Profiling an enigma: The mystery of North Korea's cyber threat landscape* (Aug. 2014), http://h30499.www3.hp.com/hpeb/attachments/hpeb/off-by-on-software-security-blog/388/2/HPSR%20SecurityBriefing_Episode16_NorthKorea.pdf.

targeting U.S. economic and business institutions, as a viable and destructive weapon. The Democratic People's Republic of Korea's (DPRK) motivations need to be carefully compared to the PRC, their cyber enabler and sponsor, which uses its cyber capability for espionage and commercial advantage, but not to directly damage the US economy.

I. THE GROWTH OF NORTH KOREA CYBER CAPABILITIES

In its annual report to Congress regarding the capabilities of the DPRK, the Department of Defense shares the view that North Korean cyber capabilities pose a serious threat beyond the immediate region:

> Given North Korea's bleak economic outlook, OCO may be seen as a cost-effective way to develop asymmetric, deniable military options. Because of North Korea's historical isolation from outside communications and influence, it is also likely to use communications and influence, it is also likely to use Internet infrastructure from third-party nations. This increases the risk of destabilizing actions and escalation on and beyond the Korean peninsula.[3]

In fact, the state-run North Korean newspaper, Minju Joson, has criticized the US cyber operations policy

[3] "Military and Security Developments Involving The Democratic People's Republic of Korea", Office of the Secretary of Defense, Annual Report to Congress, 2013, 11, http://www.defense.gov/pubs/North_Korea_Military_Power_Report_2013-2014.pdf.

(Presidential Policy Directive 20) as "a declaration of cyber war" and noted "the cyber attack in internet network may bring irrevocable financial and material damage to the opponent side in a moment".[4] The realization of the cyber threat to its own critical infrastructure has led the North Koreans to build their program and develop a solid cyber cadre – their first generation of "cyber warriors" and to build beyond defensive capabilities. In his article on North Korean cyber development, Christian Science Monitor reporter Mark Clayton discussed the details of the North Korean program with several experts, including Alexandre Monsourov of the Johns Hopkins' US-Korea Institute, who noted that the North Koreans are on a clear path to develop cyber capabilities targeting their perceived primary adversaries – "South Korea, the US, and Japan."[5] Clayton writes that several experts see current North Korean efforts as "a kind of cyber-sword sharpening". Further, like DoD, he notes that cyber is the ideal weapon for a "cash strapped" nation.[6]

In its extensive report on North Korean capabilities, Hewlett Packard (HP) notes that the DPRK is "remarkably committed" to the development of its cyber capabilities, including training up a new generation of cyber warriors.[7]

---

[4] Minju Joson, *North Korean Newspaper hits out at U.S. cyber warfare policy*, NORTH KOREAN TECH, Aug. 12, 2013, http://www.northkoreatech.org/2013/08/12/north-korean-newspaper-hits-out-at-u-s-cyber-warfare-policy.

[5] Mark Clayton, *In Cyberarms race, North Korea emerging as a power, not a pushover*, THE CHRISTIAN SCIENCE MONITOR, Oct. 19, 2013, http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover.

[6] *Id.*

[7] HP Security Research, *Profiling an enigma: The mystery of North Korea's cyber threat landscape* (Aug. 2014),

The HP report notes an extensive cyber structure and cites South Korean estimates of a cyber offensive corps that may be the third largest in the world.[8] The North Korean cyber units, known as Office No. 91 and Unit 121, operate under the authority of the DPRK's Reconnaissance General Bureau, which oversees both conventional intelligence and cyber operations. Most interesting is the fact that these two units are actually resident in the PRC, not in North Korea.[9] This is due to the fact of North Korea's heavy internet restrictions limiting outgoing connections, which necessitates DPRK's reliance on other nations for their networks and botnets. [10] North Korea's "digital deprivation"[11] forces its dependence on the PRC as well limits, for now, the vulnerability of the DPRK's own networks.

While a large cyber corps does not guarantee sophisticated or broad impact immediately, one can see the gradual development in the efficacy of North Korean cyber attacks in the last ten years. According to Hewlett Packard, the DPRK was able to successfully penetrate 33 of 80 South Korean Military wireless communications networks in 2004. South Korea attributed this attack to their northern neighbor as well as an intrusion later that same year into the US State Department computers.[12] Of course, given the difficulties in

---

http://h30499.www3.hp.com/hpeb/attachments/hpeb/off-by-on-software-security-blog/388/2/HPSR%20SecurityBriefing_Episode16_NorthKorea.pdf.

[8] Charlie Osborne, *North Korea cyber warfare capabilities exposed*, ZDNET, Sept. 2, 2014, http://www.zdnet.com/article/north-korea-cyber-warfare-capabilities-exposed.

[9] *Id.*

[10] *Id.*

[11] *North Korean Cyber Rattling*, THE ECONOMIST, May 17, 2013, http://www.economist.com/blogs/babbage/2013/05/digital-warfare.

[12] *Id.*

proving attribution, these reports are not definitive but certainly reflect available evidence.

McAfee's analysis of attacks against South Korean government and banking sites in 2011 and 2009 also concludes that there was a definite improvement in capabilities by the perpetrator, which they attribute to North Korean elements. The McAfee report concluded "the combination of technical sophistication juxtaposed with relatively limited execution and myopic outcome to bringing a Lamborghini to a go cart race." Why use advanced capabilities for a rather low-level attack? According to McAfee, "the motivations appear to outweigh the attack, making this truly seem like an exercise to test and observe responses."[13]

Isolated and impoverished, how did North Korea improve its status among cyber actors during such a short period? While Pyongyang certainly benefitted from the cyber expertise of its patron in Beijing, it also clearly views its cyber capability as a key national resource perhaps gradually approaching the level of its nuclear aspirations. North Korea is developing its youngest students, pushing computer science, and recruiting the "best and the brightest" among university students, including programs sending them overseas for advanced training.[14] This cyber cadre is then directed to two cyber units. In 2009, it is believed that

---

[13] TEN DAYS OF RAIN: EXPERT ANALYSIS OF DISTRIBUTED DENIAL-OF-SERVICE ATTACKS TARGETING SOUTH KOREA (McAfee 2011), https://www.mcafee.com/us/resources/white-papers/wp-10-days-of-rain.pdf.

[14] Mark Clayton, *In Cyberarms race, North Korea emerging as a power, not a pushover*, THE CHRISTIAN SCIENCE MONITOR, Oct. 19, 2013, http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover.

Kim Jong Il expanded the cyber units by two-hundred percent, from 1,000 hackers to 3,000 hackers.[15] The PRC continues to play a key role in the development of cyber capability by North Korea and it is probable that the PRC actually hosts North Korean cyber warriors on their servers.[16]

II. CYBER AND CRIME – THE FUTURE OF NORTH KOREA'S LIMITED ECONOMIC LIFEBLOOD?

Criminal activity is one of the few locomotives that drive the very limited North Korean economic engine, along with military technology sold to other state and non-state actors of course. In a recent Brookings institute report, North Korea was depicted as utilizing criminal activity to obtain hard currency and moving towards a "Criminal Market Economy."[17] The criminal activity, which was initially sponsored and encouraged by the DPRK regime, has expanded to criminal "elites" in the population who expanded distribution networks of drug smuggling and several types of counterfeiting, including currency and pharmaceuticals.[18]

Just as other transnational criminal syndicates have moved into cyber crime, so is North Korea expected to use

---

[15] Youkyoung Lee, *North Korea Cyber Warfare: Hacking 'Warriors' Being Trained in Teams, Experts Say*, HUFF POST, Mar. 24, 2013, http://www.huffingtonpost.com/2013/03/24/north-korea-cyber-warfare-warriors-trained-teams_n_2943907.html.

[16] *Id.*

[17] Parameswaran Ponnudurai, *North Korea Moving Towards a 'Criminal' Market Economy*, Apr. 15, 2014, http://www.rfa.org/english/news/korea/illicit-04152014015031.html.

[18] *Id.*

some of its increasing hacking expertise to diversify its criminal enterprises. However, it is unclear whether the regime would be willing to relinquish its strict control of networks to criminal syndicates in the same way that it has "delegated" other criminal activity. South Korea has already suffered massive data breaches, including the theft of thousands of credit card numbers[19] attributed to different possible perpetrators, including North Korea, as well as the loss of proprietary information by several of its key industries. The industrialized south, whose economy is highly dependent on credit cards as well, makes a tempting target for criminal as well as political purposes.

It is clear that North Korea has focused on upgrading its criminal cyber enterprise, as demonstrated by reports that it is responsible for "the Lazarus Group." The Lazarus Group is believed to be connected to the SONY hack as well as to the eighty-one million dollars stolen from the Bangladesh Central Bank.[20] Some analysts believe that the Lazarus Group is also connected with the WannaCry ransomware.[21]

---

[19] Choe Sang-Hun, *Theft of Data Fuels Worries in South Korea*, N.Y TIMES, Jan 20, 2014, http://www.nytimes.com/2014/01/21/business/international/theft-of-data-fuels-worries-in-south-korea.html?_r=0.

[20] Michael Corkery & Matthew Goldstein, *North Korea Said to Be Target of Inquiry Over $81 Million Cyberheist*, N.Y. TIMES, Mar. 22, 2017, https://www.nytimes.com/2017/03/22/business/dealbook/north-korea-said-to-be-target-of-inquiry-over-81-million-cyberheist.html.

[21] Andy Greenberg, *The Wannacry Ransomware Has A Link to Suspected North Korean Hackers*, WIRED, May 15, 2017, https://www.wired.com/2017/05/wannacry-ransomware-link-suspected-north-korean-hackers.

III. KEY QUESTIONS

Three questions emerge in assessing North Korean intentions and capabilities: (1) Should we assume that since the PRC actively hosts and enables DPRK cyber operations that the Chinese can inhibit North Korean offensive cyber intentions as they continue to build an independent capability? (2) Under what circumstances would North Korea consider a destructive cyber attack against key US economic and financial interests? (3) Given North Korea's proclivity to provide other destructive technologies and military assistance to rogue states and non-state actors, would the DPRK also assist them with destructive cyber capabilities?

IV. CAN CHINA INHIBIT NORTH KOREAN INTENTIONS?

There is no question that the China-DPRK relationship is a very strong alliance across all sectors. But as the Council on Foreign Relations notes, this alliance does not mean control by the PRC, including in the nuclear arena.[22] Control may become even less likely in the cyber realm where expert cyber operators can diminish the possibility of clear and/or immediate attribution. If North Korea moves away from the necessity of Chinese cyber platforms, it can perform more independently and in concert with its own strategy and economic needs. However, North Korea remains dependent on these platforms at the current time and it is unclear as to whether North Korean cyber

[22] Jayshree Bajoria & Beina Xu, *Backgrounder: The China-North Korea Relationship*, COUNCIL ON FOREIGN RELATIONS, Feb. 21, 2013, http://www.cfr.org/china/china-north-korea-relationship/p11097.

operations are partitioned from their Chinese patrons. One can assume there is significant oversight over any Chinese platforms being leveraged by DPRK cyber operators. Recent reports indicate that North Korea is using nodes in Malaysia for a few of its cyber activities and in an effort to deny attribution, but this does not signal wholesale movement away from China.[23]

It should be noted as an isolated and sanctioned state, North Korea does not have any compelling interest in avoiding disruptions to the world economy. What would be the impact on Pyongyang of a major disruption to the Western banking system? Even the Bank of China has terminated its relationship with North Korean financial institutions.[24] North Korea's relationship with foreign banks is severely limited due to sanctions and while it has successfully circumvented sanctions and increased some trade, Pyongyang uses small Chinese regional banks and other underground methods to move money internationally. Having been exiled from major world banks, North Korea has adopted many of the same money laundering and movement techniques as criminal and terrorist organizations – using money brokers or trading in gold for hard currency.[25] In other words, this is not a state that would necessarily hesitate at cyber attacks on US financial centers out of a need

---

[23] Eleanor Albert, *Backgrounder: North Korea's Military Capabilities*, COUNCIL ON FOREIGN RELATIONS, Aug. 15, 2017, https://www.cfr.org/backgrounder/north-koreas-military-capabilities.

[24] Keith Bradsher & Nick Cumming-Bruce, *China Cuts Ties with Key North Korean Bank*, N.Y. TIMES, May 7, 2013, http://www.nytimes.com/2013/05/08/world/asia/china-cuts-ties-with-north-korean-bank.html?_r=0.

[25] Leon Sigal, *How North Korea Evades Financial Sanctions*, 38 NORTH, May 3, 2013, http://38north.org/2013/05/lsigal050313.

to protect its own economy, investments and trading capabilities.

Then there is the issue of North Korea becoming a "cyber hired gun" – paid to conduct attacks or provide plausible deniability for other cyber "have nots" – from other states to terrorist or criminal organizations. If it is true that the global missile or nuclear market is no longer as successful or lucrative for Pyongyang due to successful international interdiction efforts,[26] North Korea must find yet another way to circumvent sanctions and bring in hard currency. While some have suggested that North Korea is working with Iran in this area, there is little concrete evidence to suggest this is true. The analogy to North Korean nuclear cooperation with Iran has not yet been indicated except in one claim that Israel may have such evidence.[27] Both countries have made considerable progress in their cyber capabilities, but one wonders whether Iran truly has a need for North Korean assistance in this area, unless it is serving as a conduit for Chinese support.

All of which leads us back to North Korea's cyber inclinations. Obviously, Pyongyang realistically views itself as a key target by the United States, Japan, South Korea, and others. Because of this, it initially focused on building its defensive capabilities. Having accomplished some limited degree of defensive capacity, Pyongyang must understand that it can use computer network exploitation of others to

---

[26] Joshua Pollack, *North Korea's Shrinking Role in the Global Missile Market*, 38 NORTH, Jul. 29, 2011, http://38north.org/2011/07/jpollack072911.

[27] Thom Shanker & David Sanger, *US Allies Trying to Battle Iranian Hackers*, N.Y. TIMES, Jun. 8, 2013, http://www.nytimes.com/2013/06/09/world/middleeast/us-helps-allies-trying-to-battle-iranian-hackers.html?pagewanted=1&_r=0&smid=tw-share.

build both a defense and attack capability. There are strong indications that it is using its cyber capability against South Korea with some success. There are two risks here – that attacks against South Korea will impact beyond these borders, a clear danger in any cyber attack scenario and of equal, if not greater concern, that North Korea, devoid of any other effective tools in its arsenal, will lash out specifically against those countries that have intensified its isolation.

In testimony before Congress, Frank Cilluffo of the Homeland Security Policy Institute stated:

> "Precisely because North Korea has fewer constraints, I would underscore that it poses an important 'wildcard' threat, not only to the United States but also to the region and broader international stability."[28]

Sometimes the threats we should prepare for and consider are those that come from entities considerably less powerful and capable than us, particularly those that could cause negative economic impact in a matter of minutes.

---

[28] Frank Cilluffo, *Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure*, TESTIMONY BEFORE THE US HOUSE OF REPRESENTATIVES, COMMITTEE ON HOMELAND SECURITY, Mar. 20, 2013, http://www.gwumc.edu/hspi/policy/Meehan_Cilluffo%20Testimony%20March%202013.pdf.

Privacy and Data Protection in India

Dhiraj R. Duraiswami*

INTRODUCTION

India's recent demonetization initiative signaled a push towards digitization and a cashless economy primarily in order to eliminate corruption and black money while also improving the quality of life of the average citizen. The Indian Finance Minister in his budget speech announced an ambitious target of 25 billion digital transactions for the year 2017-18 which appears to be in line with recent growth trends.[1] Also, as a popular outsourcing destination India already sees a large volume of data cross its borders daily for processing, storage and use. Even more significant is the prevalence of cyber-attacks and cybercrime across the globe, which makes it imperative for a robust regulatory framework augmented with strict enforcement and redressal mechanisms and the adoption of good data governance practices. Risks presented by cyber-attacks know no borders; and individuals, organizations and nations are not fully protected. India is one of the top ten countries identified for cybercrime[2] and is not among the top ten countries most

* *Dhiraj Duraiswami* is an international business and technology consultant who has advised numerous clients in the United States over the last twenty years. He is a Certified Information Systems Auditor (CISA). He earned an LL.M in Intellectual Property and Information Law from the Benjamin N. Cardozo School of Law, a post graduate diploma in International Trade from IIFT, Delhi and MBA, BL, and B.Com degrees from the University of Madras, India. He is admitted to the Bar in Chennai, India. He also serves as the Digital Content Editor for the Journal of Law & Cyber Warfare.

[1] Dipti Jain, *Can India Meet the Target of 2500 crore Digital Transactions in 2017-18?*, LIVEMINT (March 30, 2017, 04:52 PM IST), http://www.livemint.com/Politics/637uTLKanriP4PbFhhCznJ/Can-India-meet-the-target-of-2500-crore-digital-transaction.html.

[2] James Cook, *The World's 10 Biggest Cybercrime Hotspots in 2016*

prepared for cyber-attacks.[3] In 2016, according to Symantec in their Norton Cyber Security Insights Report, over 689 million people in twenty-one countries experienced cybercrime and over $126 billion spent by the victims since 2015.[4]

This article provides an overview of the current privacy and data protection laws in India, the enforcement and liability provisions of those laws, and pending regulations and trends to protect privacy and enhance data governance practices.

I. REGULATORY OVERVIEW

Protection of privacy and personal data is achieved most commonly through the regulatory framework of laws, policies and procedures that minimizes the intrusion into the privacy of individuals as a result of the collection, storage and dissemination of sensitive personal data. Such personal data generally refers to the information collected by any person, organization, government or agency and is not to be confused with trade secrets or other confidential information. There is no dedicated or omnibus piece of legislation in India that protects privacy or personal data, but there are various laws pertaining to information technology,

---

Ranked, BUSINESS INSIDER (May 14, 2017, 3:01 AM), http://www.businessinsider.com/worlds-10-cybercrime-hotspots-in-2016-ranked-symantec-2017-5/.

[3] José Santiago, *Top Countries Best Prepared against Cyber-attacks*, WORLD ECON. FORUM (22 July 2015), https://www.weforum.org/agenda/2015/07/top-countries-best-prepared-against-cyberattacks/.

[4] *2016 Norton Cyber Security Insights Report*, SYMANTEC, https://us.norton.com/cyber-security-insights-2016 (last visited July 28, 2017).

contracts, intellectual property and crimes that offer protection and impose civil and criminal liability. Presently, the provisions of the Information Technology Act, 2000 ("IT Act") and the rules issued thereunder cover the concept of sensitive personal data or information and provide the legal framework for data protection and privacy in India.

In addition to the IT Act and the implied right to privacy under the Constitution upheld by the judiciary[5], the main pieces of legislation that provide data protection include the Contract Act, 1872; The Indian Copyright Act, 1957; Indian Penal Code, 1860 and the Credit Information Companies Regulation Act, 2005. The Justice Shah Report on Privacy in 2012 recommended the passing of privacy legislation, in addition to identifying 57 specific existing sectoral and policy guidelines that have privacy implications and hence would need to be amended as the new legislation is passed.[6] A draft privacy protection bill was introduced in the Indian Parliament in 2014 and is expected to be reviewed and passed as law in response to concerns regarding personal data protection in the country.[7] While the bill is pending, the focus for the purposes of this article remains on the existing laws and rules available to protect personal data.

A. Constitutional Protection

Article 21 of the Constitution of India dealing with

---

[5] *Kharak Singh v. U.P*, AIR, 1963 SC 1295 (India).

[6] *Report of the Group of Experts on Privacy*, GOV'T OF INDIA PLANNING COMM'N, (16 October, 2012), http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf.

[7] Ranjani Ayyar & Rachel Chitra, *Data Privacy Back in Spotlight,* THE TIMES OF INDIA (January 19, 2017, 09:43 AM IST), http://timesofindia.indiatimes.com/trend-tracking/data-privacy-back-in-spotlight/articleshow/56658914.cms.

the fundamental freedom to life and liberty has been interpreted to include the concept of the privacy right. The constitutionally guaranteed right to free speech and expression provided under Article 19(1)(a) can have privacy read into such individual fundamental rights, which however, as with other existing fundamental rights, are only enforceable against the state and subject to reasonable restrictions that may be imposed under Article 19(2). Indian courts have given paramount importance to such a perceived, albeit limited, right of privacy which can only, in their opinion, be fettered for compelling reasons, such as national security and in the interests of the public.[8] However, the Supreme Court of India has yet to conclusively decide if such a right to privacy is a fundamental right guaranteed under the Constitution, though a challenge was allowed in 2015, with the matter pending and referred to a larger bench of the apex court for a decision.[9]

It is relevant to note that privacy has been recognized as a fundamental human right; enshrined in numerous international human rights instruments[10] including the

---

[8] *Kharak Singh v. U.P*, AIR, 1963 SC 1295 (India); *Gobind v. M.P.*, AIR, 1975 SC 1375 (India); *R. Rajagopal v. Tamil Nadu* (1994) 6 SCC 632 (India); *People's Union of Civil Liberties (PUCL) v. Union of India*, AIR, 1997 SC 568 (India); *Dist. Registrar and Collector, Hyderabad v. Canara Bank*, AIR, 2005 SC 186 (India).

[9] *Puttaswamy v. Union of India*, http://judis.nic.in/supremecourt/imgs1.aspx?filename=42841 (last visited June 18, 2017).

[10] G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948); G.A. Res. 45/158, United Nations Convention on Migrant Workers (Dec. 10, 1990); G.A. Art. 16, Convention of the Protection of the Child, 1577 U.N.T.S., 3 (Nov. 20, 1989); G.A. Art. 17, International Covenant on Civil and Political Rights, 999 U.N.T.S, 171 (Dec. 16, 1966); Organization of African Unity, *African Charter on the Rights and Welfare of the Child* art. 10, Jul.11, 1990,

International Covenant on Civil and Political Rights ("ICCPR"). Article 17 of the ICCPR provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation". States party to the ICCPR have a positive obligation to "adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy]"[11]. India is also party to The Universal Declaration of Human Rights, whose Article 12 provides privacy protection.

B. Information Technology Act, 2002 and Privacy Rules

The Information Technology Act ("IT Act"), read along with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("Privacy Rules"), contains specific provisions that constitute the relevant national law regulating the collection, transfer and use of

---

CAB/LEG/24.9/49 (1990); Organization of American States, *American Convention on Human Rights* art.11, Nov.21, 1969, O.A.T.S. No.36, 1144 U.N.T.S.123; African Union *Declaration of Principles on Freedom of Expression* art.4, Oct.22, 2002, available at: http://www.refworld.org/docid/4753d3a40.html [accessed 2 July 2017]; Inter-American Commission on Human Rights, *American Declaration of the Rights and Duties of Man* art.5, May.2, 1948, OEA/Ser. L./V.II.23, doc. 21, rev. 6 (1948); League of Arab States, *Arab Charter on Human Rights* art.17, Sep.15, 1994, http://www.refworld.org/docid/3ae6b38540.html [accessed 2 July 2017]; Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms* art. 8, Nov.4, 1950, E.T.S 5, 213 U.N.T.S. 221.

[11] *ICCPR*, General Comment No. 16 (1988), para. 1.

personal information. The IT Act is specifically intended to protect electronic data, which by definition includes non-electronic records or information that have been, are currently or intended to be processed electronically. Additionally, the IT Act regulates other aspects of information technology including electronic commerce and cybercrimes.

The Privacy Rules[12] require corporate entities collecting, processing and storing personal data including sensitive personal information to comply with prescribed procedures. It distinguishes between the "personal information" and "sensitive personal data or information" ("SPDI") as a subset of personal information. Personal information is defined as any information that relates to a natural person, which either directly or indirectly, in combination with other information that is available or likely to be available to a corporate entity, is capable of identifying such person.[13]

The Privacy Rules identify the following personal information as SPDI:

- passwords;
- financial information, such as bank account or credit card or debit card or other payment instrument details;
- physical, physiological and mental health condition;

[12] *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*, MINISTRY OF COMMC'N. & INFO. TECH., GOV'T OF INDIA, http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf (last visited June 27, 2017).

[13] *Id.*, Rule 2(1) (i).

- sexual orientation;
- medical records and history;
- biometric information;
- any detail relating to the above as provided to body corporate for providing services; and
- any information received under the above by body corporate for processing, stored or processed under lawful contract or otherwise.[14]

"Biometrics" has been defined to mean the technologies that measure and analyze human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns, hand measurements and DNA for authentication purposes.[15] However, any information freely available in the public domain is exempt from the above definition.

1. Reasonable Security Practices and Procedures

Any corporate entity that possesses, manages or handles any SPDI in a computer resource that it owns, controls or operates, under section 43-A of the IT Act, is liable for civil liabilities. These liabilities require compensation for negligence in implementing and maintaining "reasonable security practices and procedures" in relation to such SPDI that results in wrongful loss or wrongful gain to any person. This section along with the Privacy Rules has compelled companies collecting and using

[14] *Id.*, Rule 3.
[15] *Id.*, Rule 2(1) (b).

such personal data to review their contractual arrangements in order to ensure that their data security practices and procedures are at par with those that are stipulated.[16] The Privacy Rules stipulate that "reasonable security practices and procedures" to be adopted by any corporate entity to secure sensitive personal information are procedures that comply with the IS/ISO/IEC 27001 standard on "Information Technology – Security Techniques – Information Security Management System – Requirements".[17] Any industry association or corporate entity following any other standard for data protection is required to get its pertinent codes for data protection best practices approved and notified by the Government of India.[18] Such corporate bodies which have implemented the stipulated standard or approved codes also need to get the same certified or audited by an independent auditor approved by the Central Government. Further, an audit has to be carried out by such an auditor at least once a year or whenever there is a significant upgradation of processes and computer resources.[19]

2. Collection, Processing and Transfer

The Privacy Rules require any corporate entity or any person acting on its behalf to obtain prior consent in writing from the information provider(s) regarding the purpose of usage of the SPDI.[20] The corporate entity is required to take reasonable steps to ensure that the information provider is notified, at the time of collection of the SPDI or other

[16] *Id.*, Rule 8(1).
[17] *Id.*, Rule 8(2).
[18] *Id.*, Rule 8(3).
[19] *Id.*, Rule 8(4).
[20] *Id.*, Rule 5(1).

personal information of: the collection of information, the purpose of collecting such information, the intended recipients of the information and the name and address of the agency collecting and retaining the information. Such information may only be collected for a lawful purpose connected with the functioning of the corporate entity.[21] The corporate entity must also ensure that the information is used only for the purpose collected and that it does not retain the sensitive personal information for longer than for the required purpose.[22]

The Privacy Rules also mandate that any corporate entity or any person who on behalf of such entity collects, receives, possess, stores, deals or handles such information provide a privacy policy that discloses its practices regarding the handling and disclosure of personal information, including sensitive personal information, and ensure that the policy is available for view, including on the website of the corporate entity or the person acting on its behalf.[23] The providers of information should be allowed to review and correct the information they had so provided to ensure that no part of the information is inaccurate or deficient.[24] Further, the provider of information has to be provided a right to opt out or retract the consent earlier provided. However, in case the provider of information does not provide or subsequently withdraws consent, the corporate entity will have the option not to provide the services or goods for which the information was earlier sought.[25]

The corporate entity or the person collecting the data on its behalf must obtain the consent of the provider for any

[21] *Id.*, Rule 5(2).
[22] *Id.*, Rule 5(4).
[23] *Id.*, Rule 4(1)(i).
[24] *Id.*, Rule 5(6).
[25] *Id.*, Rule 5(7).

transfer of sensitive personal information to any other corporate entity or person in India, or in any other country provided that the transferee ensures the same level of data protection adhered to by the data collector under the Privacy Rules.[26] The transfer may be allowed only if is required for the performance of a lawful contract between the corporate entity or any person acting on its behalf and the provider of information. A corporate entity may not transfer any sensitive personal information to another person or entity that does not maintain the same level of data protection as required in the IT Act and Privacy Rules.

Contracts regulating between the data collector and the transferee should contain adequate indemnity provisions for a third-party breach, must clearly specify the end purposes of the data processing, including who would have access to such data, and clearly specify a mode of transfer that is adequately secured and safe. Such contracts are required specifically to include provisions that entitle the data collector to distinguish between "personal information" and "sensitive personal information" that it wishes to collect or process; this is to represent that the consent of the person(s) concerned has been obtained for collection and disclosure of such personal information or sensitive personal information; and to outline the liability of the third-party transferee.

3. Enforcement, Breach Notification and Redressal

The erstwhile Department of Electronics and Information Technology (upgraded to full-fledged ministry in July 2016) was the government agency empowered to

[26] *Id.*, Rule 7.

administer the IT Act. The DEITY periodically publishes rules for the regulation of data privacy and personal data protection. In this regard, DEITY notified and brought into force the Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 ("Cert-In Rules").[27] The Cert-In Rules impose mandatory notification requirements on service providers, intermediaries, data centers and corporate entities in the event of certain types of "Cyber Security Incidents" including unauthorized access of IT systems or data. The Cert-In Rules define "Cyber Security Incidents" as

> Any real or suspected adverse events, in relation to cyber security, that violate any explicitly or implicitly applicable security policy, resulting in: unauthorized access, denial or disruption of service; unauthorized use of a computer resource for processing or storage of information; or changes to data or information without authorization.[28]

Any occurrence of the following types of cyber security incidents will trigger the notification requirements under the Cert-In Rules:

- targeted scanning/probing of critical networks/systems;

---

[27] *Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013*, NOTIFICATION, MINISTRY OF ELECS. & INFO. TECH., GOV'T OF INDIA, http://meity.gov.in/writereaddata/files/G_S_R%2020%20%28E%292_0.pdf (last visited June 27, 2017).

[28] *Id.*, Rule 2(1)(h).

- compromise of critical information/systems;
- unauthorized access of IT systems/data;
- defacement of websites or intrusion into website and unauthorized changes such as inserting malicious code or links to external websites;
- malicious code attacks such as spreading virus, worms, trojans, botnets/spyware;
- attacks on servers such as database, mail, DNS and network devices such as routers;
- identity theft, spoofing and phishing attacks;
- denial of service (DoS) & distributed denial of service (DDoS) attacks;
- attacks on critical infrastructure, SCADA systems and wireless networks;
- attacks on applications such as e-governance and e-commerce etc.[29]

Upon the occurrence of any of these events, companies are required to notify the Indian Computer Emergency Response Team ("CERT-In") CERT-In is a government body established to collect, analyze and disseminate information on cyber incidents, as well as provide forecasts and alerts about cyber security incidents, provide emergency measures for handling cyber security incidents and coordinate cyber incident response activities. Such notifications are required to be made within a reasonable time, so as to leave scope for appropriate action by the authorities. It is important to follow "breach notice obligations" which would depend upon the "place of occurrence of such breaches" and on whether or not Indian customers have been targeted. The specific format and

[29] *Id.,* Annexure to the Cert-In Rules.

procedures for reporting cyber security incidents are set out by CERT-In on its official website.[30] CERT-In currently functions under the newly constituted Ministry of Electronics and Information Technology ("MEITY").

Besides the civil liabilities prescribed under section 43-A, section 72-A of the IT Act imposes punishment for disclosure of "personal information" by any service provider, without the consent of the data subject or in breach of an agreement with such subject, and with the intent to, or knowing that it is likely to cause wrongful gain or wrongful loss. The IT Act provides for criminal sanctions of up to three years in prison and/or a fine of up to INR 500,000 in respect of intentional or negligent disclosure of an individual's personal information, obtained under a contract, where such disclosure is made without the consent of the concerned individual or in breach of the concerned contract.

The Privacy Rules provide that a corporate entity must address grievances of the information provider within a specified time. The corporate entity should appoint a Grievance Officer to address such grievances within one month from receipt of the grievance. There is no specific requirement that the Grievance Officer must be a citizen of or resident of India, nor are there any specific enforcement actions or penalties associated with not appointing a data protection officer correctly. However, appointment of such an officer is part of the statutory due diligence process and it thus becomes imperative to appoint one.

In August of 2011, India's Ministry of Communications and Information issued a Press Note[31] to

---

[30] *Indian – Computer Emergency Response Team*, MINISTRY OF ELECS. & INFO. TECH., GOV'T OF INDIA, http://www.cert-in.org.in/ (last visited June 18, 2017).

[31] *Clarification on Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information)*

make some clarifications on the Privacy Rules, which included one that exempted any Indian outsourcing service provider organization that provides services relating to collection, storage, dealing or handling of sensitive personal information or personal information under contractual obligation with any legal entity located within or outside India from the collection and disclosure of information requirements, including the consent requirements discussed above, provided that they do not have direct contact with the data subjects (providers of information) when providing their services.

C. Indian Contract Act, 1872

Given the limitations of enforceability and incomprehensive nature of the IT Act and Privacy Rules in India, which is a popular off-shoring destination, redressal for violation of personal data and privacy rights can be sought within the framework of the law of contracts as provided under the Indian Contract Act, 1872. Companies generally enter into contractual agreements with other companies who may be clients, suppliers or partners and, where personal sensitive information needs to be kept secure, the agreements usually contain confidentiality and privacy clauses in addition to arbitration clauses for the purpose of resolving any foreseeable disputes. Remedies in the nature of damages or compensation can be sought for violation of any terms of the contract or for non-performance of the obligations imposed, including those specifically

---

Rules, 2011 Under Section 43A of the Information Technology ACT, 2000, PRESS NOTE, MINISTRY OF COMMC'N & INFO. TECH., PRESS INFORMATION BUREAU, GOV'T OF INDIA, http://pib.nic.in/newsite/erelcontent.aspx?relid=74990 (last visited June 18, 2017).

relating to data protection or any breach of contractual obligations in general, are provided under the Contract Act.

When US companies enter into contracts with off-shore or third party vendors in India, it is customary to include terms and specific conditions in their contracts for data protection to comply with the Graham-Leach Bliley Act, Health Insurance Portability and Accountability Act, Fair and Accurate Credit Transactions Act, etc. Typically, these vendor agreements also prescribe how the information can be disclosed and provide for implementation of necessary safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the data provided to the vendors. Since personal data collection itself is not being done in India in such cases, the process of seeking consent to collect, process, use, store or otherwise transfer such personal data will be done outside of India by the customer company, and obligations for their protection would be imposed on the Indian vendor entities.

D. Criminal Laws & Procedure – Indian Penal Code, 1860

As the Indian criminal law does not specifically address privacy or data privacy under the Indian Penal Code ("IPC"), liability for such breaches must be inferred from related crimes. Where there is a theft of data, prosecution can follow for the offenses of theft[32], misappropriation of property[33] or criminal breach of trust.[34] For example, section 403 of the IPC imposes a criminal penalty for dishonest misappropriation or conversion of "movable property" of

[32] PEN. CODE, Sections 378, 379.
[33] *Id.*, Section 403.
[34] *Id.*, Sections 405, 408, 409.

another for one's own use. Movable property has been defined as property which is not attached to anything and is not land, and can also be construed to include private personal data, which is stored in a tangible medium. The punishment for such criminal offences, as in the case of a breach of trust, is stringent by way of imprisonment which may extend to three years, a fine or both.

E. Intellectual Property Laws – Copyright Act, 1957

India's Copyright Act, 1957 governs intellectual property rights in literary, dramatic, musical, artistic and cinematographic works. Indian Courts have recognized copyright in computer databases[35] and granted them the status of "literary work" under this Act. Compilations of client or customer lists developed by a person by devoting time, money, labor and skill have been interpreted to amount to "literary work" wherein the author has a copyright under the Copyright Act. Any infringement that occurs with respect to such protected databases leads to a cause of action under the Copyright Act for the outsourcing parent entity. Copying the computer database, or copying and distributing the database without legal authorization, would amount to infringement of copyright as such and give rise to the remedies of injunction and damages for the plaintiff. Any person who knows of such infringement and conceals or abets it is also liable to pay a fine up to INR 200,000, faces imprisonment up to three years or both.

The Indian Copyright Act prescribes mandatory punishment for piracy of copyrighted matter depending on

[35] *Burlington Home Shopping Pvt. Ltd. v. Rajnish Chibber* 61 (1995) DLT 6; (1996) 113 PLR 31.

the gravity of the offence. Section 63B of the Indian Copyright Act provides that knowingly using a computer to create an infringing copy of a computer program shall be punishable for a minimum period of six months and a maximum of three years in prison. Fines in the minimum amount of INR 50,000 up to a maximum of INR 200,000 may be levied for second or subsequent convictions.

F. Credit Information Companies Regulation Act, 2005

Based on the Fair Credit Reporting Act and Graham Leach Bliley Act, the Credit Information Companies Regulation Act ("CICRA") has created a strict framework for protecting information regarding credit and finances of the individuals and companies in India. The CICRA requires that the credit information of individuals in India has to be collected as per privacy norms enunciated in the CICRA regulation. The Reserve Bank of India has notified Regulations[36] under CICRA which provide for strict data privacy principles. Entities collecting the data and maintaining the same have been made liable for any possible leak or alteration of this data. The Regulations specify the following entities as "specified users"[37] within the purview of the CICRA and authorized to collect credit information:

> (a) an insurance company as defined under the Insurance Act, 1938 and registered with Insurance

[36] *Credit Information Companies Regulations, 2006 Under Section 37 of the Credit Information Companies (Regulation) Act, 2005,* MINISTRY OF FINANCE, DEPT. OF ECONOMIC AFFAIRS, BANKING DIVISION, GOV'T OF INDIA, https://rbidocs.rbi.org.in/rdocs/Content/PDFs/69700.pdf (last viewed June 27, 2017).
[37] *Id.,* Rule 3.

Regulatory and Development Authority;
(b) a company providing cellular/phone services and registered with Telecom Regulatory Authority of India;
(c) a rating agency registered with Securities and Exchange Board of India.
(d) a broker registered with Securities and Exchange Board of India;
(e) a trading member registered with a recognized Commodity Exchange;
(f) Securities Exchange Board of India; and
(g) Insurance Regulatory and Development Authority.

II. RECENT TRENDS AND INDUSTRY INITIATIVE

A. Proposed New Legislation

Of particular interest is the petition filed recently in the Supreme Court of India challenging WhatsApp's privacy policy change allowing sharing of data with Facebook. The policy was first challenged in the Delhi High Court by petitioners who claimed violation of users' privacy.[38] In September last year the Delhi High Court had ruled that WhatsApp had to delete user account information of all those who deleted the application and that the company could not share such information with its parent company Facebook up to the date of the order. The petition specifically points out the government's responsibility to

[38] *WhatsApp Privacy Policy Case: Here's what it says and Why it Matters*, THE INDIAN EXPRESS (updated April 29, 2017 8:57 am) http://indianexpress.com/article/technology/tech-news-technology/whatsapp-facebook-privacy-case-supreme-court-everything-you-need-to-know-4631853/ (last visited June 18, 2017).

guarantee and ensure the protection of the personal and private data when using such modes of communication whereby private and confidential data and information is exchanged.[39]

In response to this case and already in earlier hearings, the Government Counsel indicated that a regulatory regime on data protection for consumers in India is expected soon,[40] while the Department of Telecommunications informed the court that over the top ("OTT") players such as WhatsApp, Facebook and Skype were sought to be covered by new regulations that are being explored. This marks the significance of the new privacy legislations that are sought to be introduced soon in addition to the available current legal framework provided by the IT Act and complemented by the other available general laws. Earlier concerns relating to the review and passage of the new Privacy Bill, due to reservations from various quarters, are sought to be addressed soon.[41]

B. Industry Initiative

Given the lack of comprehensive legislation for privacy and data protection, the private sector rather than the government has taken the initiative and made efforts to comply with the demands of privacy principles and self-regulation. The National Association of Service & Software

---

[39] *WhatsApp Case, supra* quotes from original petition.

[40] Priyanka, *Indian Govt is Working on Data Protection Law*, PIXR8, http://pixr8.com/indian-govt-is-working-on-data-protection-law (last visited June 18, 2017).

[41] Yatish Yadav, *Privacy Bill held up due to Intel Agency Reservations*, THE NEW INDIAN EXPRESS (updated 07 March 2017 03:30 AM), http://www.newindianexpress.com/nation/2017/mar/07/privacy-bill-held-up-due-to-intel-agency-reservations-1578461.html.

Companies ("NASSCOM") is India's national information technology business group and has taken various steps to drive private sector efforts to improve data security.[42] Recognizing the need to provide assurances of privacy protection of nonpublic personal information to foreign clients, many BPO service providers in India have engaged in self-regulation after recognizing the potential damage that could be inflicted on the Indian BPO industry resulting from major security abuses. Through the efforts of NASSCOM, stringent security measures have been developed and recommended to BPO service providers, such as the following:

- armed guards posted outside offices;
- entry restricted by requiring microchip-embedded swipe cards;
- bags and briefcases prohibited in the work area;
- key information, such as passwords, encrypted and unseen by employees;
- employees monitored via closed-circuit television.[43]

NASSCOM has also created a National Skills Registry as a centralized database of employees of IT vendor services and business process outsourcing ("BPO") companies.[44] This repository provides information about all

[42] Barbara Crutchfield George & Deborah Roach Gaut, *Offshore Outsourcing to India by U.S. and E.U. Companies*, 6 U.C. DAVIS BUS. L.J. 13 (2006).
[43] *Id.*, at 15.
[44] NATIONAL SKILLS REGISTRY, https://nationalskillsregistry.com/aboutus.htm (last visited June 27, 2017).

registered professionals including background check reports of the workforce employed within the IT/BPO industry. Additionally, a self-regulatory organization has been launched which will establish, monitor and enforce privacy and data protection standards for India's business process outsourcing industry supported by extensive industry membership.

III. CONCLUSION

Given the current dynamic and constantly expanding scenario in India, which is replete with challenges, increasing foreign investments and economic growth in an ever-expanding digital era, there is an unprecedented need to update privacy and data protection laws and standards in line with global initiatives which are tested and already in place. The lack of comprehensive legislation, while a matter of concern, has been offset by recent initiatives by the industry, the public and the government. These initiatives seek to bring in the needed legal framework while complementing the existing regulations and the proactive opinions and to stand by the judiciary to ensure defaulting entities are held accountable for not adequately protecting personal data. It behooves companies seeking to establish business in India to adhere to the local laws especially in the context of the increasing sensitivity of the Indian legal system towards data protection and privacy concerns.

About the Journal of Law and Cyber Warfare
The Journal of Law and Cyber Warfare is published twice per year by top legal professionals and scholars from the law, technology, security, and business industries. The views expressed in the Journal of Law and Cyber Warfare are those of the authors and not necessarily of the Journal of Law and Cyber Warfare or the Lexeprint Inc — the publishing company.

Submissions
The Journal welcomes submissions from legal scholars, technologists, mathematicians, analysts, academics, policy makers, practitioners, lawyers, judges and social scientists.

Form: Citations conform to The Bluebook: A Uniform System of Citation (20th ed. 2015). Please cite the Journal of Law and Cyber Warfare as: 5 J.L. & CYBER WARFARE __ (2017).

Electronic submissions are encouraged. Submissions by email and attachment should be directed to submissions@jlcw.org.

Subscriptions: The cost of an annual subscription is $250. Subscription requests should be e-mailed to info@jlcw.org.

Internet Address: The Journal of Law and Cyber Warfare website is located at http://www.jlcw.org.