CYBER SUBVERSION AND THE CONCEPTION OF CYBER-CONSTRUCTED NORMS: THE CASE OF RUSSIAN HYBRID WARFARE

Allison Moore

IR-6649-XTIA: Cyber Warfare and International Relations

October 7, 2021

Foundations

Subversion is an action done in an effort to influence domestic politics; the concept of subversion is not new has been likened to other terms such as *hybrid war*, the *gray zone*, and *political warfare*.[1] Social media and the pervasive nature of the internet has made it exponentially easier for actors to engage in subversive activities. Over the last 20 years, we have seen the emergence of *cyber subversion*, which relies upon information warfare and influence operations via the propagation of misinformation remotely throughout a state. Foundational to effective cyber subversive activities is a healthy understanding of what effective information security consists of and how adversary states implement cybersecurity concepts.

Known as the "CIA Triad," confidentiality, integrity, and availability are the three critical components of U.S. based information security.[2] The CIA Triad is the basis for a vast majority of security governance standards and is featured in major professional certification bodies.[3] It is the bedrock for most practitioners of cybersecurity and offers very simple principles to operate on.

Confidentiality. Confidentiality is similar to privacy. It is obtained in cyberspace by limiting access to network locations to only those individuals who have appropriate authorization.[4] By limiting the number of people who can access certain information, privacy is more likely to be maintained.

[1] Andrew Radin, Alyssa Demus, and Krystyna Marcinek, "Understanding Russian Subversion: Patterns, Threats, and Responses," *RAND Corporation*, 2020: 2, http://www.jstor.org/stable/resrep26519.
[2] Spyridon Samonas and David Coss, "The CIA Strikes Back: Redefining Confidentiality, Integrity, and Availability in Security," *Journal of Information System Security* 10, no. 3 (2014): 21.
[3] Samonas and Coss, "The CIA Strikes Back," 25-26.
[4] Samonas and Coss, "The CIA Strikes Back," 31-33.

Integrity. Integrity in cyberspace means that digital information has not been modified or destroyed.[5] Ensuring authenticity of digital information is extremely difficult and is best accomplished in situations where the sender and receiver utilize specific encryption techniques.

Availability. Availability means users have access to the information they are authorized to handle in a timely manner.[6] Having the ability to access information quickly can be tremendously important in certain professional fields (i.e. national security, hospitals, critical infrastructure, etc.).

Throughout this paper, I will demonstrate how state actors engaging in cyber subversive activities utilize the CIA Triad. I will first provide some technical considerations that pertain to all users in cyberspace. Then, I will consider some psychological considerations of cyber subversion and propose the conception of the *cyber-constructed norm*. Before elaborating on how these considerations factor into the case of Russia's 2016 U.S. election interference, I will discuss some methods for diminishing the effects of cyber subversion. Lastly, I demonstrate that the case of Russian interference in the U.S. 2016 election was simple cyber subversion and likely not an attempt at full-scale Russian hybrid warfare (gibridnaya voyna).

Technical Considerations

Deception

Most state actors conducting malicious operations in cyberspace rely upon various deception techniques to ensure some level of deniability. Gartzke and Lindsay point out that

[5] Samonas and Coss, "The CIA Strikes Back," 33-35.
[6] Samonas and Coss, "The CIA Strikes Back," 35.

deception is absolutely essential to any cyber operation because as soon as a victim identifies an attacker, the victim knows there is a vulnerability in their system, and they can work to patch the access vectors the attacker used.[7]

The ability for an attacker to deceive the victim allows the attacker to disrupt the CIA Triad from within the target network. By altering certain 'facts' about the attacker's identification, location, or association, the attacker may convince the victim that they are someone who has authorization, ultimately upsetting the confidentiality. The attacker may choose to affect the target's network integrity once they have gained access by launching a variety of attacks (i.e. ransomware, document manipulation, etc). Lastly, availability is easily disrupted by a denial of service (DoS) or distributed denial of service (DDoS) attack which overflow a server with more traffic than it can handle, thus preventing authorized users from accessing the material. In the case of secure servers, the attacker must first upset confidentiality by gaining access before they can attack integrity and availability.

Deception in cyberspace depends upon layers of protection, often in the form of spoofing. Spoofing is when an attacker fakes their sending address (two methods are discussed below) to gain access to a secure system.[8] I will discuss some of the layers of protection attackers use; however, the following list is not exhaustive. Key to each layer is the disconnection between the attacker and any financial transactions.[9] This includes paying for software or hardware as well as using an Internet Service Provider (ISP) tied to an attacker's personal financial account.

---

[7] Erik Gartzke and Jon Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015): 326, https://www.jstor.org/stable/26486804.

[8] U.S. Department of Commerce, "Glossary," *National Institute of Standards and Technology,* September 7, 2021, https://csrc.nist.gov/glossary/term/spoofing

[9] David M. Rohret and Micheal E. Kraft, "Catch Me if You Can: Cyber Anonymity," *Journal of Information Warfare* 10, no. 2 (2011): 15-16.

Attackers will tend to use public networks with a virtual private network (individuals) or a secure organizational network designed for near anonymous cyber operations (organized groups or state actors) to mask their activities.

Internet Protocol Address. Each user is assigned an Internet Protocol (IP) address every time they connect to the internet. These addresses are a combination of numbers that identify a user throughout their browsing experience and can change based on a number of factors. Experienced attackers will spoof their IP address and ensure they use a new one that matches the country of their virtual private network and/ or proxy servers (discussed below) every time they connect to the target network.[10]

Virtual Private Network. A Virtual Private Network (VPN) is a secure, encrypted connection that masks a user's Internet Protocol (IP) address.[11] A VPN can disguise a user's IP address to make it appear like an IP address that originates from another country or region.

Media Access Control Address. The Media Access Control (MAC) address is an alpha-numeric code assigned to each physical device that connects to a network.[12] Attackers can spoof their MAC address to prevent identification. MAC addresses are linked to a physical device that may be tied to a financial transaction. If an attacker isn't careful, their MAC address may reveal their personal finance account and their identity.

Virtual Machine. A virtual machine (VM) is essentially a computer inside of a computer. An attacker can download free VM software from their choice of several companies and install a

[10] Rohret and Kraft, "Catch Me if You Can," 15.
[11] U.S. Department of Commerce, "Glossary," https://csrc.nist.gov/glossary/term/virtual_private_network
[12] U.S. Department of Commerce, "Glossary," https://csrc.nist.gov/glossary/term/media_access_control_address

free operating system (Windows, Macintosh, Linux, etc) on the VM. A new MAC address and IP address can be assigned to a VM each time a user boots the VM.[13]

Proxy Server. A proxy server acts as a mediator between a user and a server, effectively breaking the connection between the two in order to provide the user with more privacy.[14] Experienced attackers utilize multiple anonymous proxy servers throughout each internet session.[15]

These are only a few of the layers of deception users can apply to maintain anonymity. However, these layers each have possible vulnerabilities and do not guarantee complete protection of identity or state of origin.

Reconnaissance

Before conducting any type of offensive cyber campaign, attackers conduct reconnaissance. Reconnaissance can be conducted in a number of ways but is vital to developing a plan of action for further cyber operations. Generally, an attacker will first seek out open source information that is available on their target before attempting to gain access to the target network. Once the attacker is able to access the network, they will often spend a substantial amount of time gathering information on the network structure and searching for vital documents or vulnerabilities. Conducting thorough cyber reconnaissance can allow an attacker to better design their operation to damage a victim's CIA Triad. If the attacker is a state actor,

[13] U.S. Department of Commerce, "Glossary," https://nsrc.org/workshops/2014/nsrc-ubuntunet-trainers/raw-attachment/wiki/Agenda/update-vm-mac-address.htm
[14] U.S. Department of Commerce. "Glossary," https://csrc.nist.gov/glossary/term/proxy
[15] Rohret and Kraft, "Catch Me if You Can," 15.

reconnaissance plays a vital role in ensuring the operation will achieve any policy goals associated with the operation.

Open Source. Open-source intelligence (OSINT) is publicly available and can be pieced together to develop an understanding of the target's situation. OSINT is widely accessible through the internet and has become easier to find due to the development of highly customizable search engine algorithms. OSINT is extremely important in cyber reconnaissance for targeting as well as payload design.

Targeting. OSINT provides ample opportunity for targeting. Hackers can find targets for whaling (similar to spear phishing but targeting higher level executives) and spear phishing simply by visiting a company's public website. Many companies post contact information for high level executives or information technology (IT) specialists directly on their webpage. Technology companies also post updates to recent vulnerabilities and subsequent patch information online for their customers. Hackers can leverage this information to target computers that have not patched the vulnerability yet.

Payload Design. In some instances, OSINT may provide enough information to design malicious payload- such as malware. Hackers frequently post information on their own and other hackers' attacks (and sometimes their payload) on the dark web, accessible through the Tor Browser. State sponsored hackers can learn about the innerworkings of some targets via OSINT on the dark web. The payload may also be an article of misinformation (e.g. "fake news"). OSINT is invaluable in attacks leveraging misinformation. Attackers can gather an understanding of social divides within a nation using OSINT and generate a payload designed to further those divides.

Social Engineering.

Social Engineering attacks are those that seek to utilize human interaction to convince a target to divulge information. These attacks can take place in person, via telephone *(vishing)*, text message *(smishing)*, or in cyberspace *(phishing)*.[16] In cyberspace, phishing is very common and often includes a malicious attachment or link that either: prompts malware to download, or requests log in information from the user.

Social Engineering attacks are generally used to establish initial entry into a victim's network. A successful phishing attempt can result in an employee divulging their username and password to the target network. This is the first break in the CIA Triad- confidentiality. The attacker uses the deception that comes with using the login information of someone who is authorized access to avoid detection of the violation of confidentiality.

Key Loggers. Once an attacker has gained access to the target network, they spend as much time as necessary- and available- surveilling the network structure and extending their influence within the network. A Key Logger provide attackers with the ability to monitor and record the keys that a user presses on their keyboard.[17] This can enable an attacker greater access into a network structure by recording usernames and passwords into various systems.

[16] Cybersecurity and Infrastructure Security Agency (CISA), "Avoiding Social Engineering and Phishing Attacks," Security Tip (ST04-014), October 22, 2009, https://us-cert.cisa.gov/ncas/tips/ST04-014

[17] U.S. Department of Commerce, "Glossary," https://csrc.nist.gov/glossary/term/key_logger

Algorithms and Bots

Algorithms take in sets of data, conduct computations, and output results that conform to the rules of the algorithm.[18] Algorithms are everywhere in cyberspace: Computer software is lines of code that compose various algorithms, every click of the mouse commands a new process; Social media platforms use algorithms to determine what content and advertisements to display to their users; Search engines use algorithms to prioritize search results; Music and video streaming services use algorithms to provide recommendations to customers. Attackers can use this to their advantage by relying upon algorithms to assist with the propagation of malicious payload.

Bots are automated algorithms that execute various tasks online.[19] They serve both genuine and malicious purposes. Several legitimate websites use chatbots to automate customer service. Attackers can use bots for just about anything: DoS or DDoS attack; propagation of social media posts; and even to inflate product prices by flooding a market with bulk purchases, removing all of the stock for regular customers, and selling the items at a higher price.

Psychological Considerations

The Power of Social Media

In a 2018 mathematics analysis, Quinn proved the concept of six degrees of separation on social media through mathematical analysis of actual social media accounts (i.e. 99.7% of people

[18] U.S. Department of Commerce, "Glossary," https://csrc.nist.gov/glossary/term/algorithm

[19] Oz Sultan, "Tackling Disinformation, Online Terrorism, and Cyber Risks into the 2020s," *The Cyber Defense Review* 4, no. 1 (2019): 49, https://www.jstor.org/stable/26623066.

are within six relationship "hops" of knowing each other).[20] This demonstrates how social media connects individuals to people they may never actually meet in real life. To further increase the impact of social media, a 2021 Pew Research Center report found that the vast majority (70%) of adult Americans use social media, with well over half visiting social media sites on a daily basis.[21] Not only do most Americans use social media, but most Americans are also connected to the majority of other Americans through their friends and social media relationships.

Considering international social media use, 49% of the total world population used social media in 2020 (an increase of 9.2% since 2019), with individual social media use averaging 2 hours and 24 minutes a day.[22] As more states lift domestic internet restrictions and more people decide to engage with social media, the more digitally connected the world becomes. Content originating in one state can easily circulate through social media and impact users in another state all the way across the globe.

Susceptibility and Risk Factors

In 2020, Van Bavel, et al. developed a model for the belief and dissemination of misinformation based on multiple risk factors: Partisan bias, polarization, political ideology, memory, cognitive style, and morality and emotion.[23] These risk factors can be divided into categories of applicability to either individuals, groups, or message content.

---

[20] Anne Quinn, "Social Media Mathematics," *The Mathematics Teacher* 111, no. 5 (2018): 392–93, http://www.jstor.org/stable/10.5951/mathteacher.111.5.0390.
[21] Brooke Auxier and Monica Anderson, "Social Media Use in 2021," *Pew Research Center,* 3-8.
[22] We Are Social, "Digital 2020," 2021, https://wearesocial.com/digital-2020
[23] Jay J. Van Bavel, Elizabeth A. Harris, Philip Parnamets, Steve Rathje, Kimberly C. Doell, and Joshua A. Tucker, "Political Psychology in the Digital (Mis)information Age: A Model of News Belief and Sharing," *Social Issues and Policy Review* (2020): 1-14.

Susceptibility of Individuals. Partisan bias, memory, and cognitive style apply to the individual user. Partisan bias deals with an individual's tendency to maintain their political identity, even if their party's message has been discredited as false.[24]

An individual's memory also factors into their belief and dissemination of misinformation with three factors: age, exposure, and timing. Van Bavel, et al. note that elderly people share seven times the number of fake news as their younger counterparts.[25] Prior exposure to misinformation also contributes to an individual believing new fake news.[26] The timing of misinformation may also contribute substantially to an individual's dissemination of fake news. Misinformation disseminated in close proximity to political events is likely more effective than misinformation that is distributed early enough for individuals to forget about when it comes time to vote.

Lastly, an individual's cognitive style renders them either more or less able to discern fact from fiction. Individuals with more analytical thinking styles ("reasoning") correlate to lower levels of susceptibility to misinformation.[27]

Susceptibility of Groups. Polarization and political ideology both contribute to group susceptibility to misinformation. Polarization is the disparity between extremes of the political spectrum and is higher in a two-party system.[28] High levels of polarization equate to higher levels of misinformation dissemination and the propagation of a cycle of "polarization reinforcement."[29] Van Bavel, et al. state that Republicans are more likely to believe non-political

[24] Van Bavel, et al., "Political Psychology in the Digital (Mis)information Age," 6-7.
[25] Van Bavel, et al., "Political Psychology in the Digital (Mis)information Age," 13.
[26] Gordon Pennycook and David G. Rand, "The Psychology of Fake News," *Trends in Cognitive Sciences* 25, no. 5 (2021): 393. https://www.sciencedirect.com/science/article/pii/S1364661321000516
[27] Van Bavel, et al., "Political Psychology in the Digital (Mis)information Age," 11.
[28] Van Bavel, et al., "Political Psychology in the Digital (Mis)information Age," 8.
[29] Van Bavel, et al., "Political Psychology in the Digital (Mis)information Age," 9.

fake news than Democrats and that partisan news is usually spread by members of the same party.[30] In an analysis of how a COVID-19 conspiracy theory became "viral," Gruzd and Mai found that the theory originated from influential conservative politicians and was shared primarily by conservative supporters.[31]

Content of the Message. Lastly, Van Bavel, et al. determined that messages containing moral-emotional language correlated to higher rates of sharing, indicating that misinformation that is surprising or elicits moral-emotions are more likely to propagate on the internet.[32]

Other risk factors that warrant more research include: religious affiliation, recent significant life events, and exposure to traumatic experience. Religious affiliation likely mirrors the effect of political affiliation and the desire for individuals to maintain a particular social image.

Social Norms

Social norms are shared understandings of appropriate behavior amongst a group. In subversion, an attacker is essentially attempting to change or create a social norm that will result in policy changes within the target state. A primary goal of cyber subversion is to instill new social norms that promote an attacker's agenda through the manipulation of cyberspace.

[30] Van Bavel, et al., "Political Psychology in the Digital (Mis)information Age," 10
[31] Anatoliy Gruzd and Philip Mai, "Going Viral: How a Single Tweet Spawned a COVID-19 Conspiracy Theory on Twitter,"*Big Data and Society* 7,no. 2 (2020): 3.https://journals.sagepub.com/doi/full/10.1177/2053951720938405
[32] Van Bavel, et al., "Political Psychology in the Digital (Mis)information Age," 13-14.

Finnemore and Sikkink describe the "norm life cycle" as a three-stage process: norm emergence, norm cascade, and internalization.[33] Norm emergence occurs when an individual or a small group- which Finnemore and Sikkink define as a "norm entrepreneur"- attempts to convince the mass population to accept a new norm.[34] The second stage consists of the propagation of the new norm throughout the state until the norms become automatic in stage three.[35] Finnemore and Sikkink primarily discuss the norm life cycle in terms of the state as the primary actor.

Not to be confused with Finnemore and Hollis's term *cybernorm*, *cyber-constructed social norms* are social norms that exist in physical space but originate in cyberspace.[36] The proliferation of the internet and the influence of individuals has changed the way we can think about the norm life cycle: The cyber-constructed norm life cycle timeline is condensed, and the primary actor is the individual within the state. Attackers can use the cyber-constructed norm life cycle to their advantage as they attempt to spread misinformation that will change people's behavior and thought processes.

Stage 1- Cyber-Constructed Norm Emergence. In the case of subversive cyber operations, the attacker is the norm entrepreneur. After reconnaissance and analysis of collected data, the attacker decides what payload (misinformation) to emplace and where to publish the payload (social media or another website). With the intent to subvert, the attacker will design the misinformation to create a change in individual thinking or behavior, which will manifest as a

[33] Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (1998): 895-896, http://www.jstor.org/stable/260136
[34] Finnemore and Sikkink, "International Norm Dynamics," 895
[35] Finnemore and Sikkink, "International Norm Dynamics," 895-96
[36] Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," *The American Journal of International Law* 110, no. 3 (2016): 426-427, http://www.jstor.org/stable/10.5305/amerjintelaw.110.3.0425.

new social norm in the physical domain. This requires substantial understanding of how a specific society operates and how its citizens think.

Stage 2- Cyber-Constructed Norm Cascade. Leveraging the influence of social media and some of the technical considerations discussed above, the norm entrepreneur can propagate a cyber-constructed social norm through cyberspace quickly. From the technical perspective, thorough reconnaissance, believable payload design, and accurate targeting increase the likelihood of pervasive cyber-constructed norm cascade. The psychological risk factors discussed above weigh heavily into how quickly and widely the information will propagate and which social groups accept or reject the new norm.

Stage 3- Internalization. If an attacker's analysis and payload design are correct in Stage 1, and the payload is distributed effectively and believed by enough individuals in Stage 2, individuals or groups may reach the point at which their changed behavior becomes automatic. In subversive operations, impacting only groups of individuals may be enough to achieve the attacker's goals.

Diminishing the Effects of Cyber Subversion

Policy Based Mitigation

Social Media Misinformation Policies. Since the 2016 election interference incident, social media groups have begun revamping and publicly publishing their policies on misinformation. In 2020, Facebook released a detailed report on accounts they removed that demonstrated "coordinated inauthentic behavior" (CIB).[37] This May, Facebook released another document

[37] Facebook, "July 2020 Coordinated Inauthentic Behavior Report," (2020), https://about.fb.com/news/2020/08/july-2020-cib-report/

describing the state of influence operations (IO) which details how the Facebook CIB policy has assisted in removing hundreds of IO threats.[38] Although these policies have not completely mitigated or removed the threat of propagation of subversive content via social media, these efforts are trending in the right direction and are setting a new standard for other social media platforms.

U.S. National Cybersecurity. A report released by the U.S. intelligence community in March 2021 stated that Russia attempted to engage in election interference through influence operations in the 2020 U.S. election.[39] Although Russia actively tried to influence voters to select President Trump, they did not operate on the same scale as the 2016 election, nor did they attempt to manipulate votes.[40] This is likely due to an increase in U.S. cybersecurity policies and TTPs (tactics, techniques, and procedures). As more *cybernorms* emerge, more refined U.S. cybersecurity policies can emerge and further decrease foreign interference in U.S. domestic politics.

International Policies. The lack of overarching international guidelines, policies, or laws cultivates an atmosphere of chaos in cyberspace. The world needs *cybernorms*, preferably ones that carry the "legitimacy of law."[41] An international cyber law could instill good behaviors and would provide internationally agreed upon ramifications for violating those behaviors. The presence of possible international punishment may act as a form of deterrence to states who are considering engaging in cyber subversion.

---

[38] Facebook, "Threat Report: The State of Influence Operations 2017-2020," (2021).
[39] Greg Myre, "Intelligence Report: Russia Tried to Help Trump in 2020 Election," *National Public Radio* (2021). https://www.npr.org/2021/03/16/977958302/intelligence-report-russia-tried-to-help-trump-in-2020-election
[40] Greg Myre, "Intelligence Report," https://www.npr.org/2021/03/16/977958302/intelligence-report-russia-tried-to-help-trump-in-2020-election
[41] Finnemore and Hollis, "Constructing Norms," *441*

Technical and Psychological Mitigation

Social media platforms use several algorithms for two primary functions. First, an algorithm is used to determine what content is applicable to the user and what type of content the user might like to see. The second function is to determine what type of advertisements might be applicable to the user. These algorithms can inadvertently cause polarization of an individual as they are constantly shown content that fits their social identity. When a user interacts with misinformation that is displayed to them, they provide social media algorithms with data that supports displaying more content of a similar nature.

Social media platforms must adapt these algorithms to consider the circulation of misinformation. They can do this by altering the algorithms in two ways. First, social media platforms can adjust the algorithms to include content that offers an alternate view of political based content. This first adaptation is unlikely to be implemented as it may result in a decline in platform usage. Secondly, platforms could include a precursor algorithm to screen the content for misinformation or untrustworthy origins.

It is more difficult to impact the psychological contributions to susceptibility of spreading misinformation at the individual level. Education and training for the mass populace could help. However, some psychological conditions cannot be corrected fully. It may be more effective and time efficient to concentrate on technical countermeasures and broad education of a state population.

Case Study: Russian Gibridnaya Voyna

Russia's Theory on Hybrid War

Russian hybrid war theory- gibridnaya voyna- is a separate concept from the Western interpretation of hybrid war and is closer in concept to an aggressive form of *subversion*. Gibridnaya voyna places an emphasis on information warfare and aims to collapse an adversary by destroying "the political cohesion of an adversary from the inside by employing a carefully crafted hybrid of non-military means and methods that amplify political, ideological, economic, and other social polarisations [*sic*] within an adversary's society."[42] Several techniques within gibridnaya voyna emphasize non-military capabilities and fall within the realm of the documented risk factors for the belief and spread of misinformation discussed above.

It is important to note that the concept of gibridnaya voyna is limited in applicability and is not formally Russian military doctrine.[43] It is also important to point out the distinct difference between cyber subversion and gibridnaya voyna. Gibridnaya voyna specifically seeks to collapse an adversary state; whereas, cyber subversion seeks to impact domestic policy through the use of cyberspace.

In this case study, I will discuss the role of Russian cyber operations in the subversion of the U.S. during the 2016 election interference campaign. First, I will elaborate on how the Russian hackers prepared the cyber battlefield. Then, I will discuss Russia's dissemination of misinformation during the election. Finally, I will question the goal and efficacy of the attack as I discuss the resultant impact of the interference.

---

[42] Ofer Fridman, *Russian 'Hybrid Warfare': Resurgence and Politicisation.* New York: Oxford University Press, 2018, 96

[43] Fridman, *Russian 'Hybrid Warfare,'* 98

Operational Preparation of the Cyber Battlefield

Reconnaissance. Russian reconnaissance began in 2014 with the Internet Research Agency's (IRA) collection and analysis of data about U.S. social media use.[44] This long-term study allowed the IRA to identify natural fault lines within the U.S populace. By 2016, the IRA was creating social media profiles and posing as American nationals with strong political views to gain information on radical groups within the U.S.[45] To increase the presumed validity of IRA social media accounts, the IRA utilized thousands of bots to increase viewers and "likes" of IRA social media accounts.[46] The bots would also assist in the future propagation of misinformation.

On another front, likely beginning with OSINT, Russian intelligence based advanced persistent threat (APT) 29 (known as Cozy Bear) targeted U.S. Democratic National Committee (DNC) employees in spear phishing campaigns.[47] The spear phishing campaigns were successful at providing Cozy Bear with access to the DNC network and personal emails for several DNC and Clinton Campaign personnel.[48]APT 28 (Fancy Bear) also began with a spear phishing campaign in 2016 which gave the Russian APT access to the Democratic Congressional Campaign Committee (DCCC) network.[49] Once Fancy Bear had initial access, they leveraged malicious code that contained a key logger, which eventually gave them access to the DNC

[44] Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics,* New York: Oxford University Press, 2020, 230
[45] Buchanan, *The Hacker and the State,* 231
[46] Robert D. Blackwill and Philip H. Gordon, "Containing Russia: How to Respond to Moscow's Intervention in U.S. Democracy and Growing Geopolitical Challenge," *Council on Foreign Relations,* Council Special Report no. 80 (2018): 7
[47] Eric Lipton, David E. Sanger, and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *The New York Times* (2016), https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html
[48] Eric Lipton, David E. Sanger, and Scott Shane, "The Perfect Weapon,"
[49] Buchanan, *The Hacker and the State,* 219-220

network.[50] With troves of documents, emails, and information, the Russian groups began preparing for their main operation by registering for the domain "DCLeaks.com."[51]

Planning for Cyber Operations: Considering the CIA Triade.

Confidentiality. The confidentiality of the DNC and DCCC networks was corrupted during reconnaissance as soon as the first employee divulged their login information in the spear phishing campaign. The Russians continually disrupted the confidentiality of the network as they collected more login information and gained more access to various networks and folders. Furthermore, the hackers destroyed confidentiality when they decided to release secure documents to the public (unauthorized users).

Integrity. There are two considerations for integrity of the DNC and DCCC networks and documents. First, the integrity of democratic documents came into question as soon as the Russian hackers gained access to the network, simply because they had the ability to edit or delete anything. Secondly, the Russians could utilize the long-term reconnaissance to determine how best to manipulate documents before disseminating them to the public. Identification of social and political divides fostered the manipulation of documents and the development of fake documents to promulgate American division.

Availability. Due to the desire to remain undetected, the Russian attackers did not manipulate the availability of data to authorized data; however, in a sense, they manipulated the pillar of availability when they decided to incorporate the dissemination of documents on DCLeaks.

[50] Buchanan, *The Hacker and the State,* 220
[51] Buchanan, *The Hacker and the State,* 221

Misinformation Dissemination: Perpetuating a Cyber-Constructed Norm

Both the social media front and the DCLeaks front contributed to the propagation of misinformation. APT 28 and APT 29 posted thousands of documents on DCLeaks, some of them legitimate and some fake documents designed to seed doubt about Hillary Clinton.[52] The IRA used the power of social media to distribute misinformation and polarizing content.

Norm Emergence. During their reconnaissance, the IRA likely realized the prevalence and applicability of the psychological risk factors discussed above and incorporated moral-emotional content into highly politicized comments in support of Donald Trump in an effort to subvert the U.S. election. The IRA employed messages designed to evoke emotional responses that focused on political topics and religion; they also organized group protests on conflicting belief structures in close proximity in the physical domain to discredit the Clinton Campaign.[53] All of these actions tied together to produce a cyber-constructed norm that centered around the distrust of Hillary Clinton.

Norm Cascade. In line with the risk concept of polarization, Buchanan notes that conservative individuals were more likely to visit fake news sites than liberals prior to the 2016 election.[54] He also discusses how the content of messaging was used to incite protests and violence in physical space. The Russians also relied upon social media algorithms and bots to perpetuate advertisements to social media users.[55] Russian efforts to propagate a cyber-constructed norm aimed at damaging support for Hillary Clinton resulted in only a slight decline in favorability for

[52] Blackwill and Gordon, "Containing Russia," 8
[53] Buchanan, *The Hacker and the State,* 235
[54] Buchanan, *The Hacker and the State,* 233
[55] Buchanan, *The Hacker and the State,* 234

Clinton over a two-week period.[56] However, support for Donald Trump jumped drastically over the same period.[57]

Internalization. The question now, is if the Russian's norm proliferated to the point of internalization. The answer is: perhaps. Hillary Clinton's favorability rating has not recovered since the election.[58] However, if the intent of Russia's norm was to deter Americans from Democrats as a group or to cause America to dissolve completely, they were unsuccessful.

Efficacy of the Operation- Has the U.S. Been Subverted, or Just Misinformed?

Clearly, Russia was attempting to influence U.S. domestic politics, but was this an act of gibridnaya voyna, or just cyber subversion? And were there any long-lasting impacts on the U.S.?

Temporary Chaos. As with most things, the confusion caused by the 2016 election interference was temporary. Eventually, investigators determined the Russians were responsible for hacking the DNC and DCCC. Investigators and researchers also determined that the Russians had manipulated information on social media as well as on DCLeaks. Armed with this knowledge, the American public was afforded the opportunity to consider the impact their social media use may have had on their perceptions and political ideology. As of right now, it does not appear that

[56] Andrew Dugin, "Hillary Clinton's Favorable Rating Still Low," *Gallup,* (September 28, 2018), https://news.gallup.com/poll/243242/snapshot-hillary-clinton-favorable-rating-low.aspx
[57] Dugin, "Hillary Clinton's Favorable Rating Still Low," https://news.gallup.com/poll/243242/snapshot-hillary-clinton-favorable-rating-low.aspx
[58] Dugin, "Hillary Clinton's Favorable Rating Still Low," https://news.gallup.com/poll/243242/snapshot-hillary-clinton-favorable-rating-low.aspx

Russian cyber subversion has caused enough polarization within the U.S. to destabilize and collapse the country. If this was an attempt at gibridnaya voyna, it was an unsuccessful one.

Long-Term Impacts in An Alternate Reality. The design of Russia's cyber-constructed norm tells a different story from an attempt at gibridnaya voyna. Radin, Demus, and Marcinek also discuss the possibility for another reason why Russia would interfere in U.S. elections, outside of gibridnaya voyna. Perhaps Russia was not trying to destroy the U.S. but was simply attempting to influence Americans into selecting a president who would be more supportive of Russian policy goals.[59] Rather than attempting to collapse the U.S. political system, maybe Russia was simply trying to generate support for Donald Trump because he appeared to be more pro-Russia than Hillary Clinton. If the 2016 election interference was an attempt at simple cyber subversion, it was a successful one.

Although, the election of Donald Trump was a temporary occurrence, there have been some long-term impacts from the Russian misinformation campaigns. Russian information operations aim to subvert the idea of an "objective, impartial, or nonpartisan truth" which causes individuals to believe that nothing is certain.[60] From this perspective, the Russian election interference was incredibly successful. Not only did the U.S. elect a president who was more supportive of Russian policy than the alternative, there is now a sense of uncertainty and distrust of the truth within the U.S. It is difficult to discern what is true information and what is 'fake news.' The psychological impacts of this warrant further study as impacts on many individuals may eventually 'cascade' out to effect society as a whole.

[59] Radin, Demus, and Marcinek, "Understanding Russian Subversion," 5.
[60] Allen, T.S. and A.J. Moore. "Victory Without Casualties: Russia's Information Operations." *Parameters* 48, no.1 (2018): 67

Conclusion

Hackers have several tools and technical options available to increase deception and to decrease the likelihood of their victim determining their identity. Attackers will leverage deception as they conduct their cyber operations; however, they will always conduct reconnaissance before engaging in cyber subversion. Cyber reconnaissance allows attackers to determine how to gain access to networks and assists with the development of malicious payload. Automation through algorithms and bots allow for attackers to conduct operations on a larger scale and at a faster pace. These technical considerations can allow the attacker to compromise the confidentiality, integrity, and availability of the victim network virtually undetected.

Social media is a tremendous asset to cyber subverters. Individuals from all walks of life can quickly view the information disseminated on social media. However, some individuals are far more susceptible to misinformation than others. Political affiliations, mental state, and content of the misinformation can impact how likely someone is to believe and share pieces of misinformation. As more individuals believe and share misinformation, it propagates across the internet and establishes a type of social norm.

There is room to protect individuals and states from cyber subversion. Social media platform, state, and international policies may help to deter or alleviate the impacts of cyber subverters. Psychological contributors to the spread of misinformation are harder to account for in the campaign to prevent cyber subversion.

The case of Russian election interference in the 2016 U.S. presidential election confirms the technical model discussed but questions the ultimate goal of the Russian campaign. Russian

hackers applied reconnaissance before unleashing their payload (DNC documents and misinformation). The hackers also demonstrated an understanding of the CIA Triade and information security fundamentals. Although Russia's actions during the 2016 election caused chaos and confusion, the result was temporary. This causes a second look at the theory that Russia was conducting Russian 'hybrid warfare' with the intent to collapse the U.S. Considering the long-term impacts of the interference, it seems more likely that Russia was only conducting information operations through cyber subversion in an effort to influence Americans to vote for a president who would be more supportive of Russian policy.

The concept of cyber-constructed norms and the norm life cycle can aid in analyzing the intent and effects of future cyber subversion attempts. Further research on the application of the cyber-constructed norm life cycle to other cases of cyber subversion and influence operations may provide more insight on the connection between the cyber, psychological, and physical domains.

Bibliography

Allen, T.S. and A.J. Moore. “Victory Without Casualties: Russia’s Information Operations.” *Parameters* 48, no.1 (2018): 59-71.

Auxier, Brooke, and Monica Anderson. “Social Media Use in 2021.” *Pew Research Center.* (2021): 1-18.

Buchanan, Ben. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics.* Cambridge: Oxford University Press, 2020.

Blackwill, Robert D., and Philip H. Gordon. “Containing Russia: How to Respond to Moscow’s Intervention in U.S. Democracy and Growing Geopolitical Challenge.” *Council on Foreign Relations,* Council Special Report no.80 (2018)

Cybersecurity and Infrastructure Security Agency (CISA). “Avoiding Social Engineering and Phishing Attacks.” Security Tip (ST04-014). October 22, 2009. https://us-cert.cisa.gov/ncas/tips/ST04-014

Dugin, Andrew. “Hillary Clinton’s Favorable Rating Still Low.” *Gallup.* (September 28, 2018). https://news.gallup.com/poll/243242/snapshot-hillary-clinton-favorable-rating-low.aspx

Facebook. “July 2020 Coordinated Inauthentic Behavior Report.” (2020). https://about.fb.com/news/2020/08/july-2020-cib-report/

Facebook. “Threat Report: The State of Influence Operations 2017-2020.” (2021).

Gartzke, Erik, and Jon R. Lindsay. “Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace.” *Security Studies*24, no. 2 (2015): 316-348. DOI: 10.1080/09636412.2015.1038188

Gruzd, Anatoliy, and Philip Mai. “Going Viral: How a Single Tweet Spawned a COVID-19 Conspiracy Theory on Twitter.” *Big Data and Society* 7, no. 2 (2020): 3. https://journals.sagepub.com/doi/full/10.1177/2053951720938405

Finnemore, Martha, and Kathryn Sikkink. “International Norm Dynamics and Political Change.” *International Organization* 52, no. 4 (1998): 895-896. http://www.jstor.org/stable/260136 895-96

Finnemore, Martha, and Duncan B. Hollis. “Constructing Norms for Global Cybersecurity.” *The American Journal of International Law* 110, no. 3 (2016): 425–79. http://www.jstor.org/stable/10.5305/amerjintelaw.110.3.0425.

Fridman, Ofer. *Russian ‘Hybrid Warfare’: Resurgence and Politicisation.* New York: Oxford University Press, 2018.

Lipton, Eric, David E. Sanger, and Scott Shane. "The Perfect Weapon: How Russian Cyberpower Invaded the U.S." *The New York Times* (2016). https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

Myre,Greg. "Intelligence Report: Russia Tried to Help Trump in 2020 Election." *National Public Radio* (2021). https://www.npr.org/2021/03/16/977958302/intelligence-report-russia-tried-to-help-trump-in-2020-election

Pennycook, Gordon, and David G. Rand. "The Psychology of Fake News." *Trends in Cognitive Sciences* 25, no. 5 (2021): 393. https://www.sciencedirect.com/science/article/pii/S1364661321000516

Quinn, Anne. "Social Media Mathematics." *The Mathematics Teacher* 111, no. 5 (2018): 390–97. http://www.jstor.org/stable/10.5951/mathteacher.111.5.0390.

Radin, Andrew, Alyssa Demus, and Krystyna Marcinek. "Understanding Russian Subversion: Patterns, Threats, and Responses." *RAND Corporation*, 2020: 1-32. http://www.jstor.org/stable/resrep26519.

Rohret, David M., and Michael E. Kraft. "Catch Me If You Can: Cyber Anonymity." *Journal of Information Warfare* 10, no. 2 (2011): 11–21. https://www.jstor.org/stable/26486804.

Samonas, Spyridon, and David Coss. "The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security." *Journal of Information System Security* 10, no. 3 (2014): 21-45.

Sultan, Oz. "Tackling Disinformation, Online Terrorism, and Cyber Risks into the 2020s." *The Cyber Defense Review* 4, no. 1 (2019): 43-60. https://www.jstor.org/stable/26623066.

U.S. Department of Commerce. "Glossary." *National Institute of Standards and Technology*. September 7, 2021. https://csrc.nist.gov/glossary

Van Bavel, Jay J., Elizabeth A. Harris, Philip Parnamets, Steve Rathje, Kimberly C. Doell, and Joshua A. Tucker. "Political Psychology in the Digital (Mis)information Age: A Model of News Belief and Sharing." *Social Issues and Policy Review* 2020: 1-14.

We Are Social. "Digital 2020." 2021. https://wearesocial.com/digital-2020