Penetrating the State:
The Impact of the Revolution in Cyber Technology
On State Decision-Making Autonomy

Dr. Ken Brown
Halcyon Institute

30 June 2023

Abstract

During recent presidential elections, Russia launched an aggressive campaign to influence the outcome in favor of the Republican candidate. While components of this campaign involved the same methods the Soviet Union employed during the Cold War, the scale was unprecedented (Connell and Vogler 2017, 24). Unlike in the past, the Russians used social media trolls and sophisticated hacking methods based on complex codes and network penetration that lasted at least a year (Buratowski 2017, 5). Whether Russia's actions changed the election results is impossible to say, however, since they led to the resignation of National Committee leaders, exacerbated rifts within the parties, undermined trust in the Intelligence Community, and raised questions that continue to reverberate, they clearly had an impact (Banks 2017, 1487). The recent influence campaigns were not isolated events but part of a broader trend in which state and non-state actors are exploiting the rapid advancement and proliferation of cyber technology to disrupt, manipulate or undermine state decision-making processes and the people involved. Instances such as the Chinese hackers' theft of sensitive records on over twenty-five million US government personnel, Russian cyberattacks that shut down the Estonian government for three weeks, and the Stuxnet malware attack on Iran's nuclear program that destroyed over 1000 centrifuges, are all indicators of a broader trend that has accelerated over the past decade (Gootman 2016; Kello 2017, 62-63). In addition, ISIS' defacement of U.S. Central Command's web page and its aggressive social media campaigns that contributed to the recruitment of over 30,000 foreign fighters from over 100 countries, are further examples demonstrating the effectiveness that terrorist organizations have in exploiting cyber technology (Banks 2017, 1487).

Introduction

During the 2016 U.S. presidential election Russia launched an aggressive campaign to influence the outcome in favor of the Republican candidate. While components of this campaign involved the same methods the Soviet Union employed during the Cold War, the scale was unprecedented (Connell and Vogler 2017, 24). Unlike in the past, the Russians used social media trolls and sophisticated hacking methods based on complex codes and network penetration that lasted at least a year (Buratowski 2017, 5). Whether Russia's actions changed the election results is impossible to say, however, since they led to the resignation of Democratic National Committee leaders, exacerbated rifts within the party, undermined the President's trust in the Intelligence Community, and raised questions that continue to reverberate, they clearly had an impact (Banks 2017, 1487).

This campaign, however, was not an isolated event but is part of a broader trend in which state and non-state actors are exploiting the rapid advancement and proliferation of cyber technology to disrupt, manipulate or undermine state decision-making processes and the people involved. Instances such as the Chinese hackers' theft of sensitive records on over twenty-five million US government personnel in 2015, Russian cyberattacks that shut down the Estonian government for three weeks in 2007, and the 2010 Stuxnet malware attack on Iran's nuclear program that destroyed over 1000 centrifuges, are all indicators of a broader trend that has accelerated over the past decade (Gootman 2016; Kello 2017, 62-63). In addition, ISIS' defacement of U.S. Central Command's web page and its aggressive social media campaign that contributed to the recruitment of over 30,000 foreign fighters from over 100 countries, demonstrate that terrorist organizations are exploiting cyber technology as well (Alfaro-Gonzalez et. al. 2015, 13).

Despite these developments and repeated expressions of concern by government officials, industry leaders, and technical experts over the past twenty years, there is a significant gap in the literature on cyber technology's implications for the international system. Even when scholars have

explored cyber-related topics, they have tended to engage in definitional debates or to focus on the plausibility of cyberwar scenarios. As a result, a holistic analysis is generally absent.

To address this gap, I will conduct a comprehensive analysis of cyber technology's implications for states' autonomy in their foreign policy decision-making. This will involve four steps. First, I will review the extant literature, identify gaps and outline my theory. Second, I will describe my research design and define critical terms. Third, I will analyze the revolution in cyber technology to identify how it has created and increased vulnerabilities that facilitate external actors' access to critical elements of the government, industry and population. Through this process, I will identify and explore three core activities where actors' have dramatically increased their capabilities due to the revolution in cyber technology: sabotage, espionage and influence operations.

Finally, I will overlay the neoclassical realist model of international relations to assess how these activities are negatively impacting states' autonomy. In the end, I will demonstrate that cyber technology's rapidly changing, minimally attributable, and pervasive nature are providing external actors with an unprecedented ability to penetrate and influence states' decision-making processes.

Cybertechnology

Although there is a large body of literature on cyber technology, most of it is focused on two themes: 1) the risks of cyber conflict; and 2) theory application. I will discuss each of these in turn.

Cyber conflict risks

Scholars generally agree that changes in cyber technology offer significant commercial, interpersonal, and other advantages, however they diverge sharply over the risks they present. One of the primary points of contention is the concept of "cyberwar" and the potential for its occurrence. Erik Gartzke represents one end of the spectrum when he argues in "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," that fears of cyberwar are unjustified because they conflate capability with intent (Gartzke 2013, 42). From his perspective, cyber capabilities alone cannot replicate the

damage caused by other modes of combat, therefore concerns about a cyber "Pearl Harbor" are hyperbolic assertions based unlikely occurrences (60-63). Adam P. Liff takes a similar approach in his argument that, even though cyber weapons are likely to become more prevalent, they are unlikely to increase the frequency of warfare writ large (Liff 2012).

Thomas Rid also asserts that cyberwar will not occur, arguing that it is insufficiently violent to equate with war and therefore is a mischaracterization (Rid 2013, 3-10). Similarly, Kello also discounts the likelihood of cyberwar from a definitional standpoint (Kello 2017, 52). His argument, which echoes other scholars such as Farwell and Rohozinski (2011), Stone (2013), and Singer and Friedman (2014), adopts the definition that cyberwar is an act that "proximately results in death, injury or significant destruction" (Kello 2017, 52). Based on this definition, Kello posits that cyberwar has never occurred and is unlikely to happen (52). At the same time, however, he does not discount the risks entailed in the "cyber revolution," but finds that it presents a serious threat to the international system and states' dominance therein (161-162).

Jarno Limnéll takes a middle of the road approach in his argument that, while Russia's use of cyber capabilities is not at the same destructive level as other means of conflict, they nevertheless form an integral part of Russia's "hybrid warfare" model. In this capacity, cyber technology's use blurs the peace-war dichotomy and raises questions about how we categorize nonviolent but disruptive actions by other states (Limnéll 2015, 527). Thus, Limnéll does not argue one side or the other on the cyberwar question, but looks at the impact the technology is having on the frameworks states use to organize the international system and categorize conflict.

At the other end of the spectrum, scholars such as Clarke and Knake (2010), Caplan (2013), and McGraw (2013), join policymakers and practitioners in arguing that cyberwar is a reality. Clarke and Knake take an additional step in that they not only assess cyber conflict today, but also argue that it will get worse (31-32).

Despite the substantial amount of writing on categorizing cyber conflict and its associated risks, the literature suffers from two significant shortfalls. First, as recognized by Eun and Abmann, much of the debate about cyberwar centers on unrecognized definitional differences rather than substantive arguments over the severity of the threat (Eun and Abmann 2016, 346-348). Thus, even where scholars such as Kello and Caplan interpret the threat data similarly, their use of different definitions for "cyberwar" make it appear as though they come down on opposing sides of the argument. While Michael Robinson, et. al. attempt to address this definitional problem in their 2015 article, *Cyber Warfare: Issues and Challenges*, their findings raise as many questions as they attempt to answer.

Exacerbating this problem, although scholars have invested a lot of effort into the debate surrounding cyberwar, their definitional arguments reflect a Western mindset that differs from Russian and Chinese perspectives (Waltzman 2017, 3-4). Instead of treating "cyberwar" in a limited legalistic sense, commentators and practitioners in both countries generally take a broader perspective that expands beyond the perceived peace – war dichotomy (Pollpeter 2015, 139-145; Giles 2016, 4). By framing the argument in such limited terms, therefore, Western scholars are imposing their own standards on other actors' behaviors and limiting our understanding.

Second, scholars tend to focus on cyber's kinetic-like effects and gloss over less physically destructive factors such as social media and espionage. For example, Lucas Kello rarely discusses social media in his expansive study on the cyber revolution even though he recognizes its potential power to influence states' populations (Kello 2017, 50). Analysis of the internet's and social media's non-kinetic impacts are typically left to other scholars whose efforts are divorced from the larger cyber discussions (Alarid 2009; Fidler 2016; Rudner 2017). As a result, cyber technology is not addressed comprehensively, which means it is not possible for us to fully understand its potential risks, opportunities, problems and solutions.

One exception to this pattern is Joseph Nye, who conducts a broad-sweeping analysis of cyber technology to support his argument that it is having a diffusing effect on power unlike any other time in human history (Nye 2011, 113). According to Nye, this diffusion is the result of rapid internet proliferation and its low usage costs, which have given individuals and non-state actors a greater voice in politics and capabilities previously reserved for governments (116-117). While he provides a holistic analysis that is rare in this field, Nye stops short of exploring how cyber technology writ large is impacting states' autonomy.

Unfortunately, the War in Ukraine has only seemed to validate the narratives of who want to downplay its significance. Such a conclusion, however, is misinformed and improperly framed. Specifically, Russia and Ukraine, as well as other countries and corporations, have dedicated extensive resources to conducting offensive and defensive operations in cyberspace before and during the conflict. Many of these operations were invisible to those not directly involved and likely were purposely constrained to avoid unintended consequences (Bateman, Beecroft, and Wilde 2022). As such, it is clear the combatants are taking the cyber domain seriously as an operating environment. Moreover, the benchmark many naysayers use is unreasonably high. As demonstrated by the war, and as argued in this paper, cyber operations are most effective in a supporting role or as a tool for indirect warfare, such as espionage and clandestine influence activities (Mueller, Jensen, et. al. 2023). Measuring cyber operations through the lens of conventional military applications is both unrealistic and impractical.

Offense-defense Balance and International Relations

When discussing theory, scholars primarily focus on two areas: 1) the offense-defense balance; and 2) the applicability of existing international relations theory to cyberspace. In the first category, most scholars agree that, due to its inherent complexity, rapidly changing nature, limited attribution and low barrier to entry, cyberspace is offense dominant (Nye 2011; Saltzman 2013; Kello 2017, 68). For Kello, these factors, plus non-state actor empowerment and the lack of a verifiable weapons convention,

substantially increase the risk of the security dilemma and the attending potential for conflict (Kello 2013, 32-33). Saltzman reaches a similar conclusion, although she argues that the offense-defense theory is outdated in view of its focus on kinetic effects and territory-based conflicts (Saltzman 2013). Aquilla also argues that cyberspace is offensive dominant, but rather than seeing it as a threat, he concludes that cyber capabilities will reduce major conflicts since they provide options for states to achieve objectives short of war (Aquilla 2011, 43).

Jon Lindsay is one of the few who finds that cyberspace is not an offense-dominant domain. In his article, "The Impact of China on Cybersecurity: Fiction and Friction," Lindsay argues that overstating the threats posed by Chinese cyberattacks poses a greater danger than their actual capabilities (Lindsay 2015, 29-37). Libicki also argues that cyberspace is defensively dominant, although he concludes that, since cyber capabilities alone cannot deny adversaries' access to or the use of their conventional and nuclear weapons, the defense has primacy (Libicki 2011, 73).

These articles and books, however, suffer from the same limitations as above since the scholars focus primarily on computer network attack scenarios and ignore the role of social media and other aspects of cyber technology in influencing international security. Considering the billions of internet and social media users across the globe, scholars' failure to take their potential impacts into account is a fundamental shortfall.

Regarding existing international relations theory, Choucri argues that current theories fall short in explanatory power when applied to cyberspace (Choucri 2012). To fill this gap, he applies lateral pressure theory, which posits that states inherently expand activities outside their boundaries and, when one state's expansion impacts upon another's interests in that space, hostility is likely (38). Since cyberspace is a natural extension of other venues for state behavior, lateral pressure theory applies there as well (134). Choucri's book, however, is focused at the international level and therefore does not delve deeply into cyber technology's impact on international conflict or state decision-making autonomy.

Overall, this review demonstrates that scholars are wrestling with the same fundamental question: how do we need to adjust our cognitive, structural and theoretical frameworks to accommodate the challenges created by rapid changes in cyber technology? Although no work could address this question in totality, to partially fill the gap, I will explore how these changes are impacting states' autonomy. Specifically, I will argue that the revolution in cyber technology is undermining state autonomy by providing external actors with unprecedented access to foreign policy decision-making processes through novel, insidious methods that exploit technologies on which societies and governments are heavily reliant.

For a theoretical framework, I will use neoclassical realism, which argues that, while anarchy and relative power capabilities drive foreign policies, they do so through the imperfect "transmission belt" of domestic politics (Rose 1998, 146-147; Schweller 2004, 164). To represent this process, neoclassical realism introduces two intervening variables in the causal chain: 1) political leaders' perceptions of relative power arrangements in the international system; and 2) leaders' ability to mobilize the domestic human and material resources necessary to implement their decisions (Rose 1998, 147; Zakaria 1998, 34-35). Moreover, these two factors are not separate, but interact and influence each other. As such, leaders with perceived high levels of power will likely be able to overcome internal resistance which will make them more ambitious than those who see themselves as relatively weak (Rose 1998, 151). In addition, since leaders cannot objectively know their state's level of relative power, or the true nature of the international system, they will act on perceptions and within the context of internal politics which can create unpredictable behavior (152-153, 167).

It is important to note, however, that there is no one accepted neoclassical realist theory, but different variations built upon the same basic assumptions. For example, Schweller argues that there are four unit level variables within the causal chain that determine whether and how a state balances against a threat: 1) elite consensus; 2) regime vulnerability; 3) social cohesion; and 4) leadership cohesion

(Schweller 2004, 169). Alternatively, Kitchen argues that the intervening variables should be combined into the common concept of strategic ideas (Kitchen 2010). Since both Schweller's and Kitchen's variables are included in Roses'1998 framework, I will use his version of the theory for this paper.

According to neoclassical realism then, to influence a state's foreign policy, actors should target leaders' perceptions of relative power and the processes used to mobilize domestic resources for decision implementation (Figure 1). Thus, to evaluate the potential impact of cyber technology on states' decision-making autonomy, I will assess how the revolution has facilitated external actors' ability to access and affect these intervening variables through espionage, sabotage and influence operations.

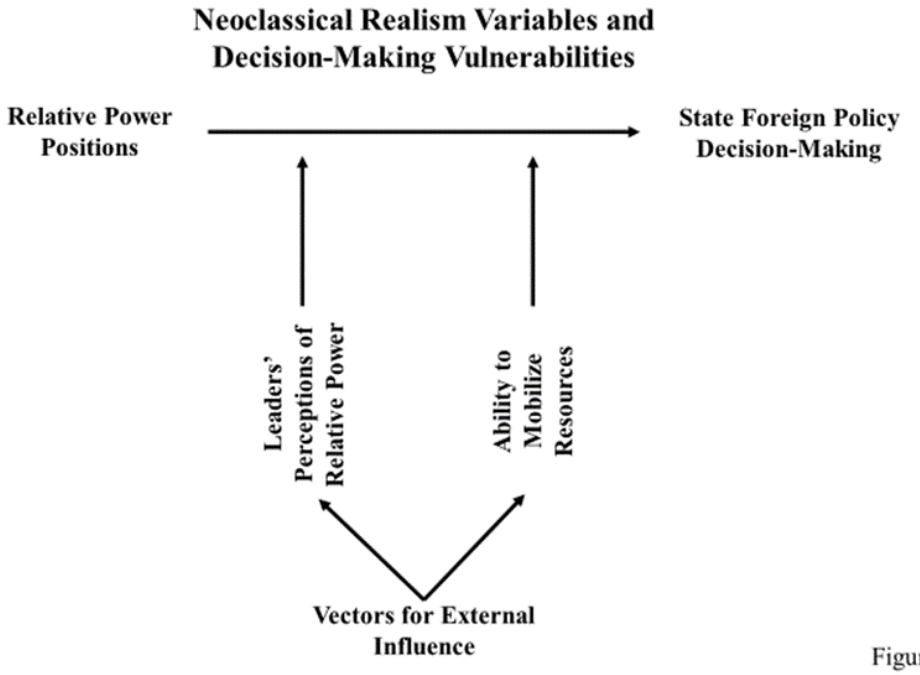

Figure 1

Methodology

To explore the hypothesis that the revolution in cyber technology (independent variable) is undermining states' autonomy in their foreign policy decision-making (dependent variable), I will use a quantitative and qualitative comparative analysis that assesses changes from 1994-2017. To measure fluctuations in the independent variable, I will use metrics reflecting cyber technology's proliferation and integration, as well as the vulnerabilities these developments have created inside states. For the

dependent variable, I will assess how external actors are exploiting these vulnerabilities through cyber-enabled sabotage, espionage, and influence operations. I will then apply the neoclassical realist framework to demonstrate how actors are undermining states' autonomy in their foreign policy decision-making. For a framework, I will use the US government.

Definitions and Measurement

Before providing measurement data, there are three terms that must be defined. First, as used in this paper, cyber is the functional equivalent of anything directly or indirectly connected to or resident within cyberspace, regardless of whether it is accessible through the worldwide web (Clarke and Knake 2007, 69). Thus, the term includes not only the traditional internet, but also social media, smart phones, industrial control mechanisms, and "cyber archipelagos," or systems separated from networks through air gaps or other controls (Kello 2017, 45). Second, the revolution in cyber technology refers to changes that have occurred in the development and use of any cyber capability. Finally, the term "state autonomy" refers to the freedom of a state's designated leaders to make and implement decisions consistent with its laws and structures without interference by external actors. Where a state has total control over its internal functions, it therefore has complete autonomy, as opposed to a state where external meddling in its processes is common.

To measure the revolution in cyber technology, I will review the history of cyber developments by providing quantitative and qualitative descriptions of the proliferation and integration of the technology into everyday life. This will include changes in the number of internet web addresses and users, geographical penetration, vulnerabilities, and government and civilian reliance on cyber infrastructure. For data, I will draw from government sources, scholarly literature, and online databases such as wearesocial.com and statistica.com. Collectively, these data will provide strong measures of how much cyber technology has changed over the past thirty years.

For changes in state autonomy, I will highlight how actors' exploitations of cyber technology have enabled them to penetrate more deeply into state infrastructures with limited attribution and minimal accountability. Specifically, through analysis of current literature, reports, and practical examples, I will demonstrate how external actors are using these capabilities to conduct espionage, sabotage, and influence operations to an unprecedented degree and scale. I will then use the neoclassical realist framework to assess how these developments are impacting state decision-making autonomy.

The Revolution in Cyber Technology

The evolution of the internet from a government run experiment to a global system of integrated networks was a complicated process driven by necessity, innovation and, to some degree, fortuitous timing (Naughton 2016). Although the internet's history stretches back to the 1930s, the key event that created today's system was the 1994 National Science Foundation decision to make the existing government-only network into an open architecture that favored collaboration over security (Naughton 2016, 11-12). Due to that decision, the internet moved from a single owner program to a commercial platform chartered to different service providers who agreed to use a common network language but otherwise were free to operate the system as they desired (12).

This free enterprise approach, plus the invention and proliferation of the World Wide Web application and *Mosaic* browser, resulted in an explosion in internet access and use in the United States and Europe that quickly spread to East Asia (Naughton 2016, 12-14; Murphy and Roser 2017). As a result, from 1995 to 2000 the number of internet users in these regions expanded from over thirty-eight million to approximately four hundred million (Internet Live Stats, 2017; Murphy and Roser 2017). Coupled with technological improvements in processor speeds and transmission capacity, along with the associated reduced costs, growth became self-perpetuating and exponential (Alberts et. al. 2000, 247-251). By 2005, internet users had increased to approximately one billion worldwide and access had spread to every continent (Internet World Stats 2005; Murphy and Roser 2017). This trend has continued

and, as of 2017, there are nearly four billion users, with an average regional penetration rate of 50% of the population across the globe (Internet World Stats 2017).

As the internet grew in size, capability and use, governments and businesses saw opportunities for efficiencies, cost savings and increased customer access. Unfortunately, the early internet architecture was immature and could not support the dramatic increase in commerce, which led to the "bubble" that burst in 1999 (Naughton 2016, 15). The growth of the 90s, however, set the physical and innovative foundations for the development of "Web 2.0," which moved the network from one of static information exchange to user interface and data creation in the early 2000s (Naughton 2016, 16-17). With the technology clearing these developmental hurdles, US internet-based commerce accelerated from an estimated $10.1 billion in fourth quarter 2001 to an estimated $111.5 billion in second quarter 2017 (US Department of Commerce 2002; 2017). At the same time, US government and civilian critical infrastructure reliance on the internet for everyday activities increased dramatically (Genge et. al. 2015, 3-4; US GAO 2017a, 2). As a result, most US commercial, societal and governmental functions now rely heavily upon the internet backbone for their daily operations (Geer 2013; Rinear 2015, 683).

While the integration of the internet into everyday lives and government functions gained efficiencies and generated tremendous economic benefits, it also greatly increased vulnerabilities (Caplan 2013, 94-96). From a statistical perspective, US internet-based vulnerabilities identified per year from 2001 to 2017 increased from 1677 to 12161, with those considered to pose high risks of exploitability and impact increasing from 772 to 3430 (NIST 2017). Averaging across the decade, over 5000 new vulnerabilities have been identified per year (NIST 2017; Statistica 2017). Considering that this does not include undetected vulnerabilities, the degree and scope of the challenge is evident.

At the same time, however, the US and other governments have taken aggressive steps to defend their networks and prevent their exploitation by criminals and hackers (Knake and Segal 2016, 22-24). For instance, in 2000 the US Congress created the Federal Computer Incident Response Center, later the

US Computer Emergency Readiness Team (US-CERT), to protect the federal government's computer networks and work with private industry to coordinate cyber security efforts (US-CERT 2017). Also, in 2015 President Obama signed Executive Order 13694, which authorizes the Treasury Department to block a person's or organization's access to any of their property within US control if they are determined to be involved in harmful cyber activities (Obama 2015). In addition, in 2016 the US federal government instituted the Cybersecurity National Action Plan, designed to address information technology shortfalls through education, modernization, and programmatic changes, and a budget of $19 billion (White House 2016a). This is emblematic of global investments in cybersecurity by governments and industries, which are projected to reach $120 billion in 2017, with a projected increase to $1 trillion by 2021 (Morgan 2017).

Despite such investments, however, governments and private enterprises face a Sisyphean task. As mentioned in the literature review, scholars largely see cyberspace as offensive dominant and as virtually impossible to defend against every vulnerability (Rinear 2015, 686-687). Since the internet is a massive, rapidly changing, human created structure, defects and vulnerabilities in software and hardware are bound to exist or develop over time (Singer and Friedman 2014). Adding to the complexity, much of the US infrastructure is privately owned, and the government does not exert direct control over how it is operated and protected (Caplan 2013, 93). This is exacerbated by private owners' hesitancy to report intrusions, as well as concerns about regulatory meddling in their business decisions, and the privacy implications raised by cooperating with the government (Caplan 2013, 94-95; Lindsay and Cheung 2015, 376-377).

Finally, human nature plays a substantial role in opening systems to attacks even when they are well protected (US Senate 2014). From poor network maintenance habits to exploitation through psychological manipulation (phishing), users tend to be the weakest link in the defensive chain (GAO 2017b). While governments and industry have attempted to offset these risks through training and

software, users continue to accidentally or purposely create opportunities for external actors to penetrate systems and inflict harm (US Senate 2014; Libicki et. al. 2015, 33).

Even if it was possible to create a perfect defense against cyberattack or exploitation, however, that would not address the risks posed by actors' opportunities to influence populations through social media and other internet-based communications platforms. Due to the widespread proliferation of smartphones and other handheld devices, and social networking applications, it is now possible for anyone with internet access to communicate with anyone else nearly anywhere in the world (We Are Social 2017). While this creates opportunities for people to connect across borders and break down social barriers, it also offers violent extremists, criminals and other countries' intelligence organizations a venue for manipulation and recruitment (Aly et. al. 2017). In addition, with over three billion social media users on nearly three billion mobile devices using applications with growing encryption capabilities, it is becoming increasingly difficult for regulators and security officials to identify and address security risks (US House of Representatives 2015, 35-36; We Are Social 2017).

While the above demonstrates the challenges and vulnerabilities associated with the revolution in cyber technology, the question remains as to how external actors are exploiting them to undermine state autonomy. This will be the focus of the next section.

Exploiting the Revolution

Although some scholars argue that cyber vulnerabilities are overstated (Lindsay 2013), and concerns about their exploitation conflate opportunity with intent (Gartzke 2013), global trends indicate the opposite. To demonstrate this, and to assess the risks these developments pose, I will explore how the revolution in cyber technology is changing external actors' abilities to penetrate and undermine states through international sabotage, espionage and influence operations.

Sabotage

According to the Oxford English Dictionary, sabotage is defined as an act to "deliberately destroy, damage, or obstruct (something), especially for political or military advantage" (Oxford 2017). Thus, sabotage can range from infiltration of armed attackers into a target country, to acts of deliberate interference with government processes to delay or confuse them (OSS 1944, 14-15). Traditionally, this involves highly trained personnel, operating clandestinely within a country and often at extreme risk of prosecution or personal harm if captured (6). Due to their secretive nature and reliance on a limited number of trained personnel, therefore, traditional sabotage operations are limited in scope, reach and impact.

The revolution in cyber technology, however, has changed sabotage in significant ways. First, although it still requires skilled personnel to conduct cyber-based sabotage activity, the level of training is significantly different from that envisioned by the Office of Strategic Services Manual. Rather than requiring extensive skills in clandestine operations, cyber sabotage can have substantial effects employing simple techniques such as Distributed Denial of Service attacks (US-CERT 2016b). In addition, the level of up-front investment for a successful cyber sabotage operation has dropped considerably due to the growing availability of hackers for hire, "off the shelf" malware, widely available online hacker training programs, and knowledge sharing forums (FBI 2017; US-CERT 2016b).

Second, it is no longer necessary to infiltrate someone into a target country to conduct sabotage or to recruit saboteurs. Instead, using the vulnerabilities and access offered by cyber technology, attacks can be conducted from outside the target country by nearly anyone with internet access (Rinear 2015, 686-687). Third, the scope, reach and impact of sabotage operations have been greatly expanded due to the ability of malware to attack multiple systems simultaneously and to adapt itself to defensive efforts and network changes (Kello 2017, 71). At the same time, due to networks' complexity, the average time from malware infection to detection is 240 days (Kello 2017, 69). Thus, it is often difficult to detect the

source of interruptions and to counteract them until well after the damage is done. Finally, due to the limited attributability associated with network operations, even once the intrusion has been detected, it is difficult to determine who is responsible and how to respond to their actions (Singer and Friedman 2015, 73). Thus, cyber sabotage requires far less risk for the saboteurs who can inflict greater harm over a longer period with limited repercussions.

One of the most well-known acts of cyber sabotage was the Stuxnet attack on Iran's nuclear program in 2009-2010. This attack, which has been attributed to the United States and Israel, set new standards in the use of cyber technology to inflict physical harm (Lindsay 2013). Moreover, Stuxnet successfully attacked a system that was theoretically isolated from external access and destroyed over one thousand centrifuges by inducing chronic fatigue in their operating systems (Farwell and Rohozinski 2011, 23). Put in traditional sabotage terms, the Stuxnet operation was the equivalent of an undetected attack that destroyed one thousand strategically important targets on a heavily armed island over the course months, after which the saboteurs escaped without harm, identification or repercussions.

Despite its impact, some argue Stuxnet demonstrates that cyber sabotage is insufficiently destructive, too expensive and too difficult to represent a significant threat (Lindsay 2013). To a degree, this argument makes sense. The Stuxnet attack was highly complex and involved years of expensive research and code development that an actor without advanced technical capabilities and detailed knowledge about the target would find impossible to execute (Singer and Friedman 2014).

However, these assessments underplay both the significance of the event and its non-physical components. First, Stuxnet was the first cyber event to generate physical damage (Farwell and Rohozinski 2012, 114). Thus, it represents a sea change in what is possible. Second, the attack not only damaged over one thousand centrifuges but created confusion and undermined the scientists' confidence in the instruments and themselves (115-116; Kello 2017, 135). By focusing solely on physical damage,

those who downplay Stuxnet and cyber sabotage in general ignore such effects, which can potentially last longer than those inflicted by an explosion.

In addition, it is important to consider that sabotage includes interference with government processes, which means it is not limited only to physical destruction. As such, there have been numerous cyber sabotage incidents of varying sophistication over the past ten years. These include Russia's attempted manipulation of the 2017 French and 2016 US presidential elections (CSIS 2017; ODNI 2017), North Korea's December 2014 attack on nuclear power plant operations in South Korea (Lee and Lim 2016), Iranian attacks on the Saudi oil company Aramco in 2012 (Bronk and Tikk-Ringas 2013) and Russian attacks on Estonia in 2007 (Kozlowski 2014). Also, considering that data itself has become a valuable commodity, attacks have also inflicted substantial and costly harm on governments and businesses by simply deleting or manipulating data on their operating systems (Regulating Internet Giants 2017). Thus, sabotage activity has not only expanded in scale, but also in the scope of targets subject to attack.

Espionage

Espionage, or spying, has been used by governments and others for thousands of years to collect information on enemies or opponents (Crowdy 2006). Traditional espionage operations are lengthy, expensive processes that require highly trained officers to conduct clandestine operations in often dangerous and undesirable locations (Hulnick 2003, 169-172). Since intelligence officers usually have limited freedom of undetected movement within the target country, espionage operations typically require the recruitment of local members of the population to collect sensitive information that they then pass on to the foreign handler (167). The work can be dangerous and, because the officers must rely on locals for access, the information they provide can be wrong or purposely deceptive (170).

While traditional espionage continues to have value, the revolution in cyber technology has greatly expanded the opportunities available to rapidly steal large amounts of data with limited

attribution, and without the need to build a risky network on the ground in the target country (Fidler 2012, 29). Thus, the opportunities offered by cyber exploitation exceed what an individual or even group of officers could collect in the same span of time (Kello 2017, 72). In addition, since cyber espionage provides direct access to the desired information rather than relying on a local network, the chances of error and purposeful deception are reduced.

Cyber espionage's potential value is demonstrated by Chinese hackers' successful theft of the advanced F-35 fighter aircraft and 21.5 million sensitive records on US government personnel with high level security clearances (Lotrionte 2015, 453; Gootman 2016). Through the F-35 thefts, China gained direct access to advanced technology that provided them a leap forward in military capability they otherwise would not have been able to achieve in the same amount of time (US Senate 2016). Such unpredictable technology advances have direct implications for relative power calculations in East Asia. In addition, the sensitive personnel records contain vast amounts of personal information that would allow the possessor to destroy a person's credit rating, identify and harass friends and relatives, or to design personally targeted phishing campaigns. Unfortunately, no one knows who has the data or what they intend to do with it, which leaves the victims in a state of uncertainty (Gootman 2016, 521).

Since those conducting cyber operations are operating in a virtual world in which their identities and associations are purposely murky, attribution is difficult, and accountability is unlikely (Healy 2011). This uncertainty leaves policy makers in a quandary since they want to respond, however, they often feel that the evidence is insufficient to hold the source nation responsible (Rid and Buchanan 2014). Thus, as with the changes to sabotage, cyber espionage opportunities have greatly increased actor capabilities while options for accountability have become more limited.

Influence Operations

The locus of all conflict and politics is in the human mind, which is why actors have used influence operations for millennia (Rawnsley 2009, 92). Typically, this involved the distribution of

messages through posters, leaflets, the news media or broadcasts over the television or radio (Gardner 2009, 19-20). In addition, the products used were usually designed to appeal to a broad audience and they were subject to interference by editors, enemies, and governments. In today's cyber-enabled environment, however, the scope, reach and precision of these activities have changed (Waltzman 2017, 2-3).

Rather than relying primarily on traditional media, broadcasts, or clandestine networks to infiltrate and distribute information, external actors can now use the internet and social media to rapidly deliver messages from almost anywhere to individuals or mass populations (Rawnsley 2009, 93). As discussed, above, the sheer volume of users, rising encryption rates, and multitude of devices raises significant challenges for governments attempting to interfere with these activities. In addition, due to advanced graphic design capabilities and the availability of detailed personal data, those messages can be precisely tailored to deliver the greatest impact (Rawnsley 2009, 83). Thus, due to the revolution in cyber technology, influence operations have increased dramatically in their scope, reach and impact.

One case that demonstrates the power of cyber-enabled influence operations is the Islamic State's recruitment and radicalization campaign. In 2014, when the Islamic State of Iraq and Syria (ISIS) broke off from al Qaeda to create their own organization, they launched an aggressive, unprecedented social media and internet propaganda program. Unlike their mujahedeen predecessors in the Afghan-Soviet War of the 1980s, however, ISIS did not need to rely on favorable media coverage, smuggled tapes, and Western support to communicate with the outside world, but could do so easily through cyber capabilities (Gunaratna 2002, 20; Malet 2013, 106). Recognizing the value this opportunity posed, they became highly active on social media, with an estimated 46,000 Twitter accounts producing an average of 7.3 tweets per day in 2014 (Berger and Morgan 2015, 34). In addition, ISIS used graphic design programs to develop professional looking magazines and videos that they posted online and publicized through social media blitzes. Although it is unclear how much of a role these products played in their

successes, the fact that ISIS was able to recruit over 36,000 foreign fighters from over 100 countries within eighteen months, as compared with a maximum of 20,000 over ten years for the pre-cyber mujahedeen, indicates that cyber technology had a substantial impact (Hegghammer 2010, 61; U.S. House 2015, 11).

Other actors have recognized the opportunities cyber-enabled influence operations pose and are actively exploiting them. Specifically, Russia used aggressive media and internet campaigns in Crimea and Donbas, Ukraine and are currently engaged in active operations to undermine NATO cohesion and destabilize the Baltic governments (Bulakh et. al. 2014, 47-48; Giles 2016). In addition, social media is playing a central role in the Kashmir and Hamas-Israeli conflicts (Karatzogianni 2009, 7; Seo 2012; Safi, 2017). One of the most destructive cyber campaigns, which arguably combined influence operations, sabotage and espionage, was Edward Snowden's theft and subsequent release of 1.5 million classified documents through WikiLeaks in 2013. These compromises not only inflicted grave damage on US foreign policy and intelligence capabilities, but also exacerbated an undercurrent of distrust of the government among members of the American public that continues to reverberate today (US House 2016).

Intervening Variables and State Autonomy

In view of the above developments, the revolution in cyber technology has dramatically enhanced external actors' abilities to create effects inside states' borders. To assess how these changes are impacting state decision-making autonomy, I will evaluate the revolution's impact on neoclassical realism's two intervening variables using the US government as a framework.

Leader's Perceptions of Relative Power

The revolution in cyber technology has impacted this variable in three ways. First, it has raised fundamental questions about what power is and how it is calculated. While the definition of power is widely debated among scholars, leaders typically focus on material measures, such as military,

economic and technological capabilities (Rose 1998, 146). These metrics, however, are often purposely hidden or subject to deception and misinterpretation, which can lead to miscalculations in balancing behavior and military responses (Schweller 2004). With the advent of cyberspace and its attending vulnerabilities, this uncertainty has only become more pronounced.

Specifically, the revolution in cyber technology has created a new domain where capabilities are rapidly evolving, largely invisible, minimally attributable, and have a broad range of potential applications (Kello 2017). With the proliferation of these capabilities to state, criminal, activist and extremist actors, it is unclear who has cyber capabilities and what they intend to do with them. As demonstrated in the above examples of sabotage, espionage and influence operations, this has enabled less objectively powerful actors to surreptitiously create deleterious effects inside more powerful states. Thus, it has become increasingly difficult for leaders to measure cyber power, to understand who has it, and to determine whether they are a threat.

Second, the dramatic increase in known and unknown vulnerabilities, and the demonstrated intent of multiple actors to exploit them, have undermined states' sense of security and perceptions of power. For the United States, this is evident in its security strategies, spending priorities and repeated statements of concern about the potential damaging effects of cyber operations (DOD 2015; The White House 2016a; 2016b; 2016c). In addition, considering the activities' limited attributability and the lack of applicable international standards, leaders are often left not only questioning who conducted a cyber operation, but also how to appropriately respond (Rinear 2015). Thus, even if they were able to accurately measure cyber power, leaders may not be able to use their own capabilities, which severely undermines their relative power position (Zakaria 1998, 38-39).

Finally, cyber espionage has provided actors with the ability to rapidly increase their own technological and military capabilities in ways not previously available. As a result advances in cyber technology, competitors are now able to steal vast amounts of information in a short period of time

without the need to recruit people inside the target country. As demonstrated by China's theft of the F-35 plans and Snowden's compromise of millions of state secrets, this information can greatly accelerate technological advancements and undercut security arrangements, which create a direct impact on real and perceived measures of power. If states are unable to protect sensitive information from theft and exploitation by an outside actor, then their leaders' ability to comfortably assess relative power positions, and to make informed decisions about them, is substantially degraded.

Mobilizing Domestic Resources

In assessing a leader's ability to mobilize domestic resources to implement foreign policy decisions, an initial point of consideration is the size and complexity of the state's national security apparatus. In the United States, to make a major decision the president relies on inputs from advisors, the National and Homeland Security Councils and their staffs, as well as information from seventeen intelligence agencies, and at least six departments with over 860,000 government employees (OPM 2017; Trump 2017). In addition, to implement those decisions, the president must rely on Congress for resources and legal authorities, which involves 535 representatives and senators and their staffs, as well as 323 million constituents (US Census Bureau 2016).

This open architecture, with its inherent institutional competition for resources and power, provides external actors with multiple potential points of entrance. While this has been a factor in varying degrees since the Nation's founding, as reflected above, the revolution in cyber technology has not only created additional vulnerabilities, but has also given external actors unprecedented access and influential power inside states. As demonstrated by Russia's sabotage of the 2016 US presidential elections, Snowden's compromise of 1.5 million classified documents, and ISIS' aggressive influence operations, these activities can have real effects on leaders' popular legitimacy, influence with other countries, trust in their advisors, and ability to maintain internal security.

In addition, the perceived and real risks of cyber sabotage raise concerns about the ability of the military, law enforcement, emergency management and other critical organizations to implement the president's decisions in the face of degraded communications, transportation infrastructures, production facilities, and financial institutions. Although scholars and practitioners debate how much of an impact cyber sabotage could potentially have on these functions, the growing number of detected high risk vulnerabilities in US critical infrastructure indicates that there is reason for concern. In addition, even if the risks are not as high as the data indicate, the mere perception of their existence creates uncertainty and raises the risk of conflict where a technical malfunction is misinterpreted, or sabotage is misattributed, leading to action against an innocent external actor. Thus, even if sabotage did not directly prevent leaders from implementing decisions, it could cause them to act in a way that leads to unnecessary conflict, wastes resources, and undermines confidence in themselves and their staffs.

Along the same lines, the revolution in cyber technology raises fundamental questions about the validity of available information. As reflected in the ongoing propaganda campaigns by actors in Russia, India, Pakistan, Israel and the Palestinian territories, people can now flood the internet, social media and traditional sources with deceptive or confusing data that create or exacerbate societal and institutional rifts. In addition, the dramatic increase in questionable information can undermine leaders' trust in their information sources and create uncertainty or even resistance that can disrupt complex, consensus-based decision-making processes such as that used in the United States (O'Leary 2017).

Also, the revolution in cyber technology has raised polarizing issues that are impacting US national security and the president's ability to garner domestic support for foreign policy decisions. Not only did Russian interference in the 2016 presidential election create questions about the results' validity, but it also raised the specter of collusion, generated a lengthy and acrimonious investigation, and produced popular backlash. In addition, intelligence programs to monitor the internet and social media have created substantial privacy concerns, as demonstrated by some American's responses to

Snowden's compromises, which only increased their fear of government overreach. In a nation in which domestic politics have a direct impact on foreign policy and supporting resources, such developments can greatly hinder leaders' abilities to implement their preferred decisions.

Finally, the revolution in cyber technology has generated tensions between some industries and the government over regulation of the infrastructure and access to information. Examples include the legal battle between Apple and the FBI over access to encrypted information on one of the San Bernardino killer's iPhone and Twitter's refusal to provide its data feed to the Intelligence Community (Stewart and Maremont 2016; Zetter 2016). These tensions can have a negative impact not only on the government's ability to collect intelligence and enforce their laws, but can also undermine their relationships with important players in the state's economic well-being, and the owners of critical infrastructure. This can also hinder decision-making implementation and harm leaders' ability to respond to emergencies while creating additional opportunities for external actors to exploit vulnerabilities with less likelihood of accountability.

Gaps and Additional Research

While the above provides a strong case that the revolution in cyber technology is having a negative effect on state decision-making autonomy, it suffers from two significant shortfalls. First, due to the newness of the subject, the rapidly evolving nature of cyber technologies, and government and industry efforts to protect information about their cyber programs and vulnerabilities, there are limited data available. Thus, the conclusions are based on examples that are arguably insufficient to establish firm trends. As time and experience provide additional empirical evidence and actor practices, this gap will narrow.

Second, due to different institutional and decision-making structures within governments, as well as varying levels of accountability, the impact of the revolution in cyber technology may differ markedly among states. In addition, a nation's vulnerabilities are directly impacted by its level of technological

integration, security measures, and societal openness (Clarke and Knake 2012, 147-149). As such, since my analysis is based on the United States, additional research is necessary to identify how generalizable my conclusions are across states with different types of regimes, societies and levels of technological development.

Conclusion

The revolution in cyber technology has had positive impacts, but it has also created vulnerabilities that external actors are exploiting to penetrate states and impact their critical functions. Due to the increased importance of the cyber backbone to societies, the government, and private enterprise, these vulnerabilities represent significant risks that must be accounted for in assessing state security.

Unfortunately, scholars have been largely remiss in conducting a holistic analysis of the risks these vulnerabilities pose. Rather than looking at the problem comprehensively, scholars have tended to engage in definitional debates, to focus on cyber technology's potential kinetic effects, or to take a segmented approach in which different components of the revolution are assessed independently. Thus, the literature is largely missing a comprehensive assessment of the impact of the cyber technology on state decision-making autonomy.

To address this gap, I first conducted a historical analysis of cyber advancements over the past twenty years. Through this process, I described how cyber technology has proliferated and become integrated into the government and society, resulting in dramatically increased vulnerabilities. Next, I explored how these developments have changed sabotage, espionage and influence operations by providing external actors with the ability to surreptitiously penetrate states and undermine their security in unprecedented ways. Finally, using the neoclassical realist theory of international relations, I explored how these developments are undermining state autonomy by providing external actors with the ability to

impact leaders' perceptions of power, and their capability to mobilize domestic resources to implement foreign policy decisions.

Overall, I demonstrated that the technologies' speed of change, deep integration, and inherent vulnerabilities, have provided external actors with the enhanced ability to penetrate states and create negative effects inside their borders. At the same time, limited attributability, archaic standards, and decreased risk to those conducting cyber sabotage, espionage, and influence operations, have degraded states' ability to identify the perpetrators and act against them. As a result, state decision-making autonomy is being directly undermined due to leaders' lessened ability to measure relative power and to apply the states' resources in the face of external efforts to degrade infrastructures, exacerbate uncertainty, create bureaucratic confusion, and exploit domestic divisions.

While additional information is necessary to further explore how these trends will evolve, and further research is required to understand their implications for governments other than the United States, the above analysis indicates that the revolution in cyber technology has created extensive vulnerabilities inside states, and that actors are actively exploiting them to the detriment of state autonomy. Whether actors' abilities to conduct cyber-enabled sabotage, espionage and influence operations will continue to grow, or will be offset by defensive measures, is impossible to say. However, current trends indicate that existing technical, structural and legal frameworks are inadequate, and therefore must be adapted to the risks posed by actor's exploitation of rapidly evolving and spreading cyber technology.

Focusing on only one component of the problem, or dismissing concerns about extensive vulnerabilities as alarmist hyperbole, is to ignore growing evidence that the revolution in cyber technology is a disruptive force that cuts to the very center of state sovereignty and the international system as we know it. Much like the development of bomber aircraft and nuclear weapons, we must look beyond the horizons of the world we know, and attempt to adapt to changes that are going to

happen whether we acknowledge them or not. In the end, either we must shape the future, or others will do it for us.

Bibliography

Alarid, Maeghin. 2009. "Recruitment and Radicalization: The Role of Social Media and New Technology." In *Impunity: Countering Illicit Power in War and Transition* eds. Michelle Hughes and Michael Miklaucic. London: Routledge.

Alberts, David S., John J. Garstka and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*. CCRP (2000). Government report and printing.

Alfaro-Gonzalez, Lydia, RJ Barthelmes, Christina Bartol, et. al. *Report: Lone Wolf Terrorism.* Georgetown University June 2015.

Aly, Anne, Stuart Macdonald, Lee Jarvis, and Thomas M. Chen. 2017. "Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization." *Studies in Conflict & Terrorism* 40 (1): 1-9.

Aquilla, John. 2011. "The Computer Mouse that Roared: Cyberwar in the Twenty-First Century." *Brown Journal of World Aff*airs 18 (Fall/Winter) 39-48.

Banks, William. 2017. "State Responsibility and Attribution of Cyber Intrusions After *Tallinn 2.0*." *Texas Law Review* 95: 1487-1513.

Bateman, Jon, Nick Beecroft, and Gavin Wilde. 2022. "What the Russian Invasion Reveals About the Future of Cyber Warfare." Carnegie Endowment for International Peace. https://carnegieendowment.org/2022/12/19/what-russian-invasion-reveals-about-future-of-cyber-warfare-pub-88667

Berger, J.M. and Jonathon Morgan. 2015. The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter. The Brookings Project on U.S. Relations with the Islamic World. https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf

Borghard, Erica D. and Shawn W. Lonergan. 2016. "Can States Calculate the Risks of Using Cyber Proxies?" Orbis. Foreign Policy Research Institute, 395-416.

Bronk, Christophy and Eneken Tikk-Ringas. 2013. "The Cyber Attack on Saudi Aramco." *Survival* 55(2): 81-96.

Bulakh, Anna, Julian Tupay, Karel Kaas, Emmet Tuohy, Kristiina Visnapuu and Juhan Kivirahk. 2014. "Russian Soft Power and Non-Military Influence: The View from Estonia." In *Tools of Destabilization: Russian Soft Power and Non-Military Influence in the Baltic States,* ed. Mike Winnerstig. FOI, 30-69.

Buratowski, Michael. "The DNC server breach: who did it and what does it mean?" *Network Security*. October 2016.

Caplan, Nathalie. 2013. "Cyber War: the Challenge to National Security." *Global Security Studies* 4 (Winter): 93-115.

Choucri, Nazli. 2012. *Cyberpolitics in International Relations.* Cambridge: The MIT Press.

Clarke, Richard A. and Robert K. Knake. 2010. *Cyber War*. NY: HarperCollins.

Connell, Michael and Sarah Vogler. 2017. *Russia's Approach to Cyber Warfare.* CNA (March).

Center for Strategic and International Studies (CSIS). 2017. *Significant Cyber Incidents Since 2006.*

Crowdy, Terry. 2006. *The Enemy Within*: *A History of Spies, Spymasters and Espionage.* Oxford: Osprey Publishing.

Eun, Yong-Soo and Judith Sita Abmann. 2016. "Cyberwar: Taking Stock of Security and Warfare in the Digital Age." *International Studies Perspectives* 17: 343-360.

Farwell, James P. Farwell and Rafal Rohozinski. 2012. "The New Reality of Cyber War." *Survival* 54 (August–September): 107–120.

---. (2011) "Stuxnet and the Future of Cyber War." *Survival*. 53(1): 23-40.

Federal Bureau of Investigation (FBI). 2017. *Public Service Announcement: Booter and Stresser Services Increase the Scale and Frequency of Distributed Denial of Service Attacks.* https://www.ic3.gov/media/2017/171017-2.aspx (accessed December 6, 2017).

Fidler, David P. 2012. "Tinker, Tailor, Soldier, Duqu: Why cyberespionage is more dangerous than you think." *International Journal of Critical Infrastructure Protection* 5: 28–29.

Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38 (Fall): 41–73.

Geer, Dan. 2013. "Resolved: The Internet is no Place for Critical Infrastructure." *Communications of the ACM* 56 (June): 48-53.

Genge, Béa, István Kiss and Piroska Haller. 2015. "A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures." *International Journal of Critical Infrastructure Protection*. 10: 3-17.

Giles, Keir. 2016. *Handbook of Russian Information Warfare*. NATO Defense College.

Gootman, Stephanie. 2016. "OPM Hack: The Most Dangerous Threat to the Federal Government Today." *Journal of Applied Security Research* 11(4): 517-525.

Gunaratna, Rohan. 2002. *Inside Al Qaeda: global Network of Terror*. New York: Columbia University Press.

Healy, Jason. 2011. "The Spectrum of National Responsibility for Cyberattacks." *Brown Journal of World Affairs.* 57 (Fall/Winter): 57-70.

Hegghammer, Thomas. 2010. "The rise of Muslim Foreign Fighters: Islam and the Globalization of Jihad." International Security 35 (3): 53-94.

Hulnick, Arthur S. 2003. "Espionage: Does it Have a Future in the 21st Century?" *Brown Journal of World Affairs.* 11 (Winter/Spring): 165-173.

Internet Live Stats 2017 www.InternetLiveStats.com (accessed October 25, 2017).

Internet World Stats 2005 http://www.internetworldstats.com/pr/edi008.htm (accessed October 30, 2017).

---. 2017 http://www.internetworldstats.com/stats.htm (accessed October 30, 2017).

Karatzogianni, Athina. 2009. "Introduction: New Media and the reconfiguration of power in global politics." In *Cyber Conflict and Global Politics, e*d. Athina Karatzogianni. London: Routledge, 1-10.

Kello, Lucas. 2017. *The Virtual Weapon and International Order*. New Haven: Yale University Press.

Kitchen, Nicholas. 2010. "Systemic pressures and domestic ideas: a neoclassical realist model of grand strategy formation." *Review of International Studies* 38: 117-143.

Knake, Rob and Adam Segal. 2016. "How the Next U.S. President Can Contain China in Cyberspace." *Journal of International Affairs*. 70 (Winter): 21-28.

Kozlowski, Andrzej. 2014. "Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan." *European Scientific Journal* 3 (February): 237-245.

Lee, Kyung-bok and Jong-in Lim. 2016. "The Reality and Response of Cyber Threats to Critical Infrastructure: A Case Study of the Cyber-terror Attack on the Korea Hydro & Nuclear Power Co., Ltd." *KSII Transactions on Internet and Information Systems*. 10 (February): 857-880.

Libicki, Martin C. 2011. "The Nature of Strategic Instability in Cyberspace." *Brown Journal of World Affairs* 18 (Fall/Winter) 2011: 71-79.

Libicki, Martin C., Lillian Ablon and Tim Webb. 2015. *The Defender's Dilemma: Charting a Course Toward Cybersecurity.* RAND: Santa Monica.

Liff, Adam P. 2012. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare capabilities and Interstate War." *The Journal of Strategic Studies* 35 (June): 401–428.

Limnéll, Jarno. 2015. "The Exploitation of the Cyber Domain as Part of Warfare: Russo-Ukrainian War." *International Journal of Cyber-Security and Digital Forensics* 4 (4): 521-532.

Lindsay, Joh R. 2013. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22: 365-404.

---. 2015. "The Impact of China on Cybersecurity: Fiction and Friction." *International Security* 39 (Winter): 7-47.

Lindsay, Joh R. and Tai Ming Cheung. 2015. "From Exploitation to Innovation: Acquisition, Absorption and Application." In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain,e*ds. Lindsay, Jon R., Tai Ming Cheung and Derek S. Reveron. New York: Oxford University Press.

Lotrionte, Catherine. 2015. "Countering State-Sponsored Cyber Economic Espionage Under International Law." *North Carolina Journal of International Law and Commercial Regulation* 40: 443-541.

Malet, David. 2013. *Foreign Fighters: Transnational Identity in Civic Conflicts*. Oxford: Oxford University Press.

McGraw, Gary. 2013. "Cyber War is Inevitable (Unless We Build Security In)." *Journal of Security Studies*. 36 (1): 109-119.

Morgan, Steve. "Marketing and Sizing Projections: Cybersecurity Ventures predicts spending will exceed $1 trillion from 2017 to 2021." *Cybersecurity Ventures* May 31, 2017. https://cybersecurityventures.com/cybersecurity-market-report/ (accessed November 15, 2017).

Mueller, Grace B., Benjamin Jensen, Brandon Valeriano, Ryan C. Maness, and Jose M. Macias. 2023. "Cyber Operations During the Russo-Ukrainian War." Center for Strategic & International Studies. https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war

Murphy, Julia and Max Roser. *Internet.* 2017. OurWorldInData.org https://ourworldindata.org/internet (accessed October 27, 2017).

National Institute of Standards and Technology (NIST). 2017. *National Vulnerability Database, CVSS Severity Distribution Over Time* https://nvd.nist.gov/vuln-metrics/visualizations/cvss-severity-distribution-over-time

Naughton, John. 2016. "The Evolution of the Internet: from Military experiment to General Purpose Technology." *Journal of Cyber Policy* 1 (1): 5-28.

Nye, Joseph. 2010. *Cyber Power*. Cambridge: Belfer Center for Science and International Affairs.

---. 2011. *The Future of Power.* NY: Public Affairs.

Obama, Barak. 2015. *Executive Order 13694: Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*.

O'Leary, Rosemary. 2017. "The Ethics of Dissent: Can President Trump Survive Guerrilla Government?" *Administrative Theory and Praxis.* 39: 63-79.

Office of the Director of National Intelligence (ODNI). *Background to "Assessing Russian Activities and Intentions in Recent US Elections:" The Analytic Process and Cyber Incident Attribution.* January 06, 2017.

Office of Personnel Management (OPM). 2017. *Sizing UP the Executive Branch Fiscal Year 2016.* June 2017. https://www.opm.gov/policy-data-oversight/data-analysis-documentation/federal-employment-reports/reports-publications/sizing-up-the-executive-branch-2016.pdf

Office of Strategic Services (OSS). *Special Operations Field Manual – Strategic Services (Provisional).* Strategic Services Field Manual No. 4 (23 Feb 1944).

Oxford. 2017. *English Oxford Living Dictionaries*. Oxford: Oxford University Press.

Pollpeter, Kevin. 2015. "Chinese Writings on Cyberwarfare and Coercion." In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain,* eds. Lindsay, Jon R., Tai Ming Cheung and Derek S. Reveron. New York: Oxford University Press.

Rawnsley, Gary D. 2009. "The laws of the playground: Information Warfare and propaganda across the Taiwan Strait." In *Cyber Conflict and Global Politics,* ed. Athina Karatzogianni. NY: Routledge.

"Regulating the internet giants: The world's most valuable resource is no longer oil, but data." *The Economist,* May 6, 2017.

Rid, Thomas. 2013. *Cyber War Will Not Take Place*. Oxford: Oxford University Press. USF Library Database.

Rid, Thomas and Ben Buchanan. 2015. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38 (1): 4-37.

Rinear, Matthew. 2015. "Armed with a Keyboard: Presidential Directive 20, Cyber-Warfare, and the International Laws of War." *Capital University Law Review* 43: 679-720.

Robinson, Michael, Kevin Jones and Helge Janicke. 2015. "Cyber warfare: Issues and challenges." *Computers and Security* 49: 70-94.

Rose, Gideon. 1998. "Review: Neoclassical Realism and Theories of Foreign Policy." Review of *The Perils of Anarchy: Contemporary Realism and International Security*, by Michael E. Brown; *Useful Adversaries: Grand Strategy, Domestic Mobilization, and Sino-American Conflict, 1947-1958*, by Thomas J. Christensen; *Deadly Imbalances: Tripolarity and Hitler's Strategy of World Conquest*, by Randall L. Schweller; *The Elusive Balance: Power and Perceptions during the Cold War*, by William Curti Wohlforth; and *From Wealth to Power: The Unusual Origins of America's World Role*, by Fareed Zakaria. World Politics 51: 144-172.

Rudner, Martin. 2017. "'Electronic Jihad': The Internet as Al Qaeda's Catalyst for Global Terror." *Studies in Conflict & Terrorism* 40 (1): 10-23.

Safi, Michael. "WhatsApp warriors on the new frontline of Kashmir's conflict." *The Guardian.* 8 July 2017, https://www.theguardian.com/world/2017/jul/08/kashmir-whatsapp-warriors-frontline-conflict-india (accessed November 30, 2017)

Saltzman, Ilai. 2013. "Cyber Posturing and the Offense-Defense Balance." *Contemporary Security Policy*. 34 (1): 40-63.

Scheweller, Randall L. 2000. "Unanswered Threats: A Neoclassical Realist Theory of Underbalancing." *International Security* 29 (Fall): 159-201.

Seo, Hyunjin. 2014. "Visual Propaganda in the Age of Social Media: An Empirical Analysis of Twitter Images During the 2012 Israeli-Hamas Conflict." *Visual Communications Quarterly* 21: 150-161.

Singer, P.W. and Allan Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press.

Statistica. 2017. *Number of common IT security vulnerabilities and exposures (CVEs) worldwide from 2009 to 2016* https://www.statista.com/statistics/500755/worldwide-common-vulnerabilities-and-exposures/ (accessed October 15, 2017).

Stewart, Christopher S. and Mark Maremont. "Twitter Bars Intelligence Agencies from Using Analytics Service." *The Wall Street Journal.* May 8, 2016. https://www.wsj.com/articles/twitter-bars-intelligence-agencies-from-using-analytics-service-1462751682

Stone, John. 2013. "Cyber War Will Take Place!" *Journal of Strategic Studies* 36 (1): 101– 108.

Trump, Donald. 2017. *Presidential Memorandum Organization of the National Security Council and Homeland Security Council*. January 28, 2017. https://www.whitehouse.gov/the-press-office/2017/01/28/presidential-memorandum-organization-national-security-council-and

U.S. Computer Emergency Response Team (US-CERT). 2017. *About us.* https://www.us-cert.gov/about-us

---. (2016) *Alert (TA16-288A): Heightened DDoS Threat Posed by Mirai and Other Botnets* (revised October 17, 2017) https://www.us-cert.gov/ncas/alerts/TA16-288A (accessed December 6, 2017).

U.S. Department of Commerce. 2002. "Retail E-Commerce Sales in Fourth Quarter 2001 were $10.0 Billion, up 13.1 Percent from Fourth Quarter 2000, Census Bureau Reports." *United States Department of Commerce News*.

---. 2017. "Quarterly Retail E-Commerce Sales 2nd Quarter 2017." *U.S. Census Bureau News*.

U.S. Department of Commerce. Census Bureau. 2016. *Quick Facts: United States Population Estimates*. https://www.census.gov/quickfacts/fact/table/US/PST045216

U.S. Department of Defense (DOD). 2015. *The Department of Defense Cyber Strategy*.

U.S. Government Accountability Office (GAO). 2017. *Cybersecurity: Actions Needed to Strengthen U.S. Capabilities.* Testimony Before the Subcommittee on Research and Technology, Committee on Science, Space and Technology, House of Representatives.

---. 2017. *Cybersecurity: Federal Efforts Are Under Way that May Address Workforce Challenges.* Testimony Before the Subcommittee on Information Technology, Committee on Oversight and Government Reform, House of Representatives.

U.S. Congress. House of Representatives. 2015. *Final Report of the Task Force on Combating Terrorist and Foreign Fighter Travel.* https://homeland.house.gov/wp-content/uploads/2015/09/TaskForceFinalReport.pdf

---. 2016. *Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden.* https://intelligence.house.gov/uploadedfiles/hpsci_snowden_review_declassified.pdf

U.S. Congress. Senate. 2016. *Testimony Before the Senate Appropriations Subcommittee on Defense*.

U.S. Congress. Senate. 2014. Homeland Security and Governmental Affairs Committee. *The Federal Government's Track Record on Cybersecurity and Critical Infrastructure*.

Waltzman, Rand. 2017. *The Weaponization of Information: The Need for Cognitive Security.* Santa Monica: RAND.

We Are Social. *Global Snapshot: Digital in Q3 2017.* (Aug. 2017) https://wearesocial.com/blog/2017/08/three-billion-people-now-use-social-media

The White House, Office of the Press Secretary. 2016. *Fact Sheet: Cybersecurity National Action Plan*. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

---. 2016. *Statement by the President on the Report of the Commission on Enhancing National Cybersecurity.* https://obamawhitehouse.archives.gov/the-press-office/2016/12/02/statement-president-report-commission-enhancing-national-cybersecurity

---. 2016. *Fact Sheet: Actions in Response to Russian Malicious Cyber Activity and Harassment*. https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and

Zakaria, Fareed. 1998. *From Wealth to Power: The Unusual Origins of America's World Role*. Princeton: Princeton University Press.

Zetter, Kim. "The FBI Drops its Case Against Apply After Finding a Way into that iPhone." *Wired.* March 28, 2016 https://www.wired.com/2016/03/fbi-drops-case-apple-finding-way-iphone/ (accessed December 1, 2017).