CHAPTER 21

INTERNATIONAL CYBER CONFLICT AND NATIONAL SECURITY

RYAN C. MANESS AND BRANDON VALERIANO

Introduction

The 2016 U.S. presidential election hack was a campaign of espionage and disinformation that continues to have a lasting impact on the United States. Russia's cyber and information operations sowed public discontent in American institutions and actively supported President Donald Trump.[1] The hacking of Democratic Party networks, primarily the Democratic National Committee (DNC), and then subsequently strategically releasing information to the whistleblowing site WikiLeaks, sowed doubt about the honesty and integrity of then candidate Hillary Clinton. Russia continued this clandestine and overt cyber activity in the French election in May 2017, and Germany took active measures to minimize Russian influence in its election in September 2017.[2]

Although disinformation campaigns have been part of both Western and Russian national security policy for decades, this direct assault on Western powers through the cyber realm is an example of the brazen form of activity in this domain of conflict. While the international system has avoided cyberwar with death and destruction, there has been a rise of political warfare activities short of war aided by cyber disruption and espionage attacks.

United Arab Emirates (UAE) hackers were named as the culprits hacking news organizations of the Gulf nation of Qatar, including the Qatari News Agency (QNA) and Al Jazeera.[3] False information regarding the emir of Qatar's affinity for Iran, Israel, and various Shia terrorist organizations sparked a Middle East crisis where five states, including Saudi Arabia, the UAE, Bahrain, Egypt, and Jordan, cut off diplomatic relations as a result.[4] For the first time, a cyberattack may be the origin of a larger military conflict in the Middle East that could have dramatic repercussions for America's strategic partners. Russia is also being implicated in releasing the emails of the UAE ambassador to the United States, showing nefarious activates such as pay-to-play schemes with top U.S. officials, which could further shake up the United States' relationships with Persian Gulf countries.[5] All these incidents have clear and dramatic repercussions for national security and strategy.

After a relative period of restraint and self-control by state actors in the cyber realm from 2000 to 2016,[6] 2017 is off to a more dangerous start, demonstrating clearly the critical issue cyber security has become. It seems that U.S.-led cyber norms that have held for most of the twenty-first century may be losing agenda-setting power.[7] In addition to Russian-origin cyber activities, an Indian SU-30 was brought down near the Chinese border, possibly as a result of a cyber operation;[8] the Vietnamese have been accused of hacking and releasing phone conversations between U.S. President Donald Trump and Philippine President Rodrigo Duterte;[9] and North Korea has been implicated in the global WannaCry ransomware attack that plagued systems around the world.[10]

Popular discourse has argued that the cyber domain is growing ever more dangerous and that future warfare will be Netcentric.[11] However, when the evidence is examined over the last fifteen years, we see a much different pattern.[12] Events like Stuxnet, operations meant to cause physical harm, are rare; instead the pattern demonstrates a greater dependence on disruption and espionage activities in cyberspace. While the cyber domain is dangerous, with the possibility of escalation often stated, we have witnessed very few events that could suggest that dramatic escalation does happen in the domain. Instead operations are mostly meant to support national interests, with plausible deniability aided by covert disruption events, or they seek to alter the balance of information between two sides.

In this chapter, we demonstrate the trend of cyber conflict through evidence and theory, and we also discuss the advantages of taking a macro perspective on data in the field of cyber security. What we have seen in the twenty-first century is that cyber as a strategy has been used as an auxiliary role in times of combat and as disruption and espionage during peacetime. This chapter explores the different perspectives of the cyber threat by various academics and practitioners in the field, followed by an empirical description of who does what to whom in terms of state-based cyber actions. Understanding the nature of the cyber threat is critical in understanding the course of national security. Future operations will be aided and enable more cyber conflict, but this domain has not demonstrated an independence where the actions we witness are divorced from traditional national security concerns. Instead, cyber conflict reinforces traditional geopolitical struggles and enables weak actors to send cheap signals. Cyber power allows major powers to reinforce their control of the international system rather than enabling new actors in the national security domain. These results, implications, and inductive theories are critical to understanding the course of international politics in the digital age.

Perspectives on the Cyber Threat

There are prognosticators, skeptics, and those with a more moderate tone in the perception of the threat that cyber tactics pose to the international system.[13] This outlay demonstrates a theoretical vibrancy in the field that can be considered nascent at this point. Those who may be deemed prognosticators or revolutionists would say that future conflict will be Netcentric, where the digital battlefield will dominate, or that cyber will be an active part of warfighting by states, which makes digital arms races and offensive-capability production paramount.[14] The cyber skeptics say that the digital realm will be relatively conflict free and that the free flow of information and ideas will continue unabated.[15] The digital realm may also be a harbinger of the spread of democracy globally as it is utilized to reach oppressed peoples and convince them to rise up and free themselves from oppression, a frame called "digital liberation."

However, there is a middle tack of scholarship that refutes both extremes and argues that popular discourse has largely gotten the cyber threat perspective wrong.[16] Cyber conflict will be an issue moving forward, but not in the traditional conflict sense. Cyber conflict will be one of information asymmetries, where espionage and disruptive propaganda campaigns will be the focus of geopolitical actors, and its use during conventional warfighting will also be used along these lines.[17] Norms will be active and constraining, but also generally in need of reset and maintenance.[18] Liberation technologies have not come to pass and have instead enabled states to maintain control over protesters and activists.[19]

A debate between Jon R. Lindsay and Lucas Kello in the pages of *International Security* play out these disagreements as to where the cyber conflict literature stands at this time.[20] Kello declares that cyber tactics increase the possibility for harm in the intentional system.[21] The probability of this playing out in real conflict scenarios needs to be questioned. The example of the United States' failure to harm ISIS is a great example of these limitations;[22] current adversaries often do not depend on cyber technology, while advanced enemies like China are prepared to meet the threat. Lindsay counters, "most imagined cyber weapons are useless, however, for communicating threats because they depend on secrecy to be effective."[23] The secrecy paradox makes it nearly impossible to communicate credibility and resolve in the domain.

Addressing scholars such as Lindsay, Kello notes, "skeptics dismiss these peculiar features of security in our times."[24] However, Kello misses the mark here, as scholars such as Lindsay are not dismissing the use of cyber tactics as dangerous but rather their probability of use and the actual utility of these measures in terms of coercive power. The cyber revolution point of view states that the digital realm is different and will drastically change how we interact on diplomatic, military, and even economic battlefields. Kello, perhaps the exemplar of this point of view, declares that "in contrast, the cyber domain is primarily a political and social plane subject to a wholly different interventions and behavior rules. We require separate concepts to capture their separate essences."[25]

Instead, E. Gartzke and J. R. Lindsay offer a well-articulated theory of deception in cyber operations that counters the utility of harm that Kello suggests.[26]

Adam P. Liff and Timothy J. Junio also evoke an interesting exchange regarding the cyber conflict domain.[27] Liff points out that the potential of cyberwar being lethal remains relatively low. Junio argues that because something is improbable does not mean that it is impossible, and therefore the study of potential ramifications of a cyberwar should not be dismissed. As Junio notes, the scenarios that militaries and governments analyze find that all-out cyberwar can and will be devastating if it ever plays out, therefore IR scholars must consider this when theorizing and conducting research on cyber conflict, especially keeping in mind that many of these operations are espionage.

Junio's warnings may be gaining traction as the Russians continue their more aggressive cyber actions, such as the critical infrastructure–killing CrashOverride, which can adapt to different systems that power advanced societies, a piece of technology first seen from the Russian state in Ukraine in 2015.[28] Although used on its regional rival Ukraine, the probability of it being used on the United States remains low out of fear of retaliation and differenes in control of critical infrastructure. Although troubling, restraint dynamics are still holding in terms of physical damage in the cyber realm between great powers.

David C. Gompert and Martin Libicki discuss the scenario of the United States and China initiating destructive cyber weaponry on the other as capabilities increase and the tensions over certain issues escalate.[29] The mythical coming cyberwar between China and the United States depends first on the issue escalating to war, which remains remote given that the United States' interest in the region are driven more by third parties than by its own national interest. The possibility for massive war exists, but it remains unlikely given the rising tide against great power war in the system. Regardless, the behavior of these two cyber powers in the digital realm will dictate the behavior of others for years to come.

The tempered relations between the United States and China in the cyber realm as a result of the Xi-Obama diplomatic meeting in 2015 may have at least stabilized relations between China and the United States. Reports by FireEye and other firms document a drastic decline in Chinese hacking activities, while others warn of more hidden efforts that are unobserved.[30] Whatever the result, the cooperation and leadership of both the United States and China is crucial to how the domain is governed internationally, and these two states should work together to temper the more aggressive Russia, which has yet to be adequately dissuaded from its continued espionage and information operations.

Chris Demchak and Peter Dombrowski declare that we are in the beginnings of a securitized "cyber-Westphalian age."[31] Due to the rise of more overt and dangerous cyber weaponry that states are sure to launch against one another, governments will come to a point where Internet borders will be drawn much as territorial boundaries were delineated as a result of the 1648 Treaty of Westphalia. If true, this revolutionary framework would harm information sharing and the cyber domain would be one of mistrust and conflict, results not witnessed since their initial publication.

While there is a great desire to establish boundaries in cyberspace, such a desire does not make for realistic policy. The Chinese and Russian governments are perhaps the leaders of this view of cyber sovereignty, as the free flow of dissident information is considered a threat to state survival. The Chinese Great Firewall and recent moves by the Putin administration to domesticate all servers with the ".ru" domain are examples of the attempts to secure Internet borders.[32] Yet the porous nature of the Internet and its architecture is proving that this is a near impossible task and that blame may be pointed at these states if unaffiliated hackers launch attacks from their borders, thus suggesting that our conception of cyber boundaries remains fluid. The work of Valeriano and Maness uses inductive theories and data collection to find that most state-initiated cyber incidents are either low-level disruptive techniques or long-term strategy espionage campaigns.[33] Of the 192 cyber incidents that can be attributed to states, only 25 (13 percent) are considered degradation techniques where physical destruction is the key goal and coercive intent is clear.[34] This backs up Rid's claim when he says, "cyber war has never happened in the past, it does not occur in the present, and it is highly unlikely that it will disturb our future."[35] As 87 percent of cyber incidents launched by states are either espionage or disruptions, it is here where the future of cyber conflict lies and where academics and policymakers must begin to focus.

An example of these coercive cyber operations with the intent to physically degrade systems also evoke negative responses from states. Stuxnet, where the United States (and likely Israel) corrupted the Iranian nuclear program's networks and centrifuges, was a blatant attempt to discourage the Islamic Republic from pursuing a nuclear weapon and to degrade its capabilities. The attempt failed and a compromise was later agreed on, but this coupled with other recent coercive cyber events such as Shamoon (2012) and the Ukrainian power grid hack (2015) suggest there is limited ability to coerce in the cyber realm and that we should see fewer of these actions in the future.

Regarding the threat from nonstate actors, the use of the Darknet as a method to spread ideology and recruitment is limited, as Moore and Rid demonstrate.[36] Access issues, the need to install external software, and problems in utilizing the Darknet and Tor networks through mobile phones limit the use of technology as a recruitment or communication tool.[37] Cyber as a threat, therefore, may be inflated, and what we actually may be seeing are low-level actions as states and nonstate actors learn that conflict in cyberspace may be somewhat limited, even as a tool for activism or terrorism.[38]

Another issue that muddles strategic calculations is that the cyber domain presents the problem of attribution, where states can claim plausible deniability when accused of being behind an act of malicious activity on an adversary in cyberspace. Rid and Buchanan propose a new way of thinking for attributing cyberattacks, as finding the source of the attack can sometimes be laborious, time consuming, and even impossible. We must also look at motives, behavioral patterns, and linguistic attributes of the malicious code. A more nuanced way to "name and blame" could further limit state action in the cyber realm and make the Internet less conflictual and more manageable. This challenge is seen in the U.S. intelligence community's evidence that Russia was without a doubt behind the espionage and information campaign during the 2016 presidential elections.[39] Russia has aggressively denied these allegations, and Moscow has remained relatively unpunished for its actions.[40]

With empirical evidence and logical theories that move away from predictions of cyber doom and worst-case scenario thinking, the growing cyber security scholarship is finding patterns of nonescalatory and restrained behavior from the major cyber powers in the international system. There is also a demonstrated lack of capability and intent to use cyber means for harm by nonstate actors.[41] Cybercrime is an issue that states and private actors should surely be addressing, but these actions fall outside the scope of the analysis in this chapter. However, with the upsurge in disruptive cyber operations and the development of degradation weapons by Russia, is this relative period of restrained behavior ending?

The Cyber Battlefield

Coercion as a Strategy

The work of Valeriano and Maness,[42] Maness and Valeriano,[43] and Valeriano, Jensen, and Maness[44] show that restraint is the strategic underpinning of how many states confront cyber actions because the coercive potential of cyber actions is quite limited. In cyberspace, restraint from geopolitical actors is interpreted as concern for escalating costs; avoiding costly and time-consuming coercive actions in the cyber realm because the potential to change behavior is weak; or unintended consequences of action, such as civilian harm, which in cyberspace might lead to spillover effects into other domains. Therefore, in the macro sense, states willingly restrain their operations in cyberspace due to strategic, normative, or lack of utility concerns, sometimes in combination.

Why is there restraint in cyberspace? Some answers include: (1) the reproducibility of tactical cyber weapons are not one-shot weapons, and they can be replicated prone to usage by the enemy if released into the wild; (2) cyber weapons are not simple to design: Stuxnet took years, along with the entire U.S. intelligence apparatus (plus help from Israel) and hundreds of millions of dollars and it still largely failed; (3) the chances of collateral damage (and thus blame) are high, since these weapons are not surgical; (4) there is high potential for diffusion of the conflict by dragging in third parties through alliances or friendship bonds; and (5) there is potential blowback since cyber weapons used to great effect will demand repercussions. None of these points alone will ensure restraint, but combined they create the outcome we currently observe.

In a comprehensive study of cyber actions as a coercive tool, Valeriano, Jensen, and Maness look at 192 cases of state-initiated cyber actions between rival states.[45] Using the Dyadic Cyber Incident and Dispute Dataset (vol. 1),[46] strategic intent is categorized into four types: disruptions, signaling espionage, breakout espionage, and degradations. Disruptions are low-cost, low-pain forms of signaling in order to harass a target into changing their decision calculus. These are usually website defacements with the intention of intimidation through propaganda or Distributed Denial of Service (DDoS) campaigns that target civilians and force the target to concede. The Russian campaigns against Estonia in 2007 and Georgia in 2008 are prime examples of disruptive efforts. Signaling espionage is when states intend to manipulate perceptions in the target government and the civilian populations about vulnerabilities, coercing them to rethink their decision-making calculus. These types of espionage campaigns are usually found in regional disputes such as South Korea and North Korea, India and Pakistan, or Israel and Iran. Breakout espionage is more based on long-term strategies where the intent is to alter the balance of information and capabilities by stealing military secrets or intellectual property. The near decade-long espionage launched by China against the United States and other developed countries is an example of this type of espionage. Degradations are high-pain, high-cost operations where the intent is to degrade or destroy critical capabilities via digital means.[47] The Shamoon wiper campaign on Saudi Arabia or the famed Stuxnet worm launched by the United States and Israel are prime examples of this type of espionage.

Of the 192 cyber incidents recorded for the years 2000–2014, 25 are degradations, 30 are breakout espionage incidents, 70 are signaling espionage, and 67 disruptions are coded.[48] There is evidence for restraint by even the most capable states. Only 13 percent of cyber incidents have the intent to degrade, while the rest are lower-level and usually nonescalatory espionage and disruption campaigns. Furthermore, only nine incidents in the recorded data evoke a concessionary behavioral change from the target, eight of these being degradations and one being a breakout espionage campaign. Therefore, cyber as a successful coercive tool is quite sparse, coming in at 4.6 percent.

There seems to be more utility in the cyber realm in espionage and disruptions, which although not often compellent in changing behavior could change the strategic calculus of states in other ways and aid in coercion overall. The connection between cyber espionage and disruption, on the one hand, and information operations on the other means that the spread of disinformation might be the future of cyber operations. harks harkens back to Russian reflective control strategies of the past and will continue to be the future unless targeted societies are on guard to ward off disinformation.

There have been calls in the United States for more tit-for-tat retaliations in response to cyber aggression. David Sanger notes in the *New York Times* how the Obama administration deliberated on how to respond to the Chinese hacking of the Office of Personnel Management (OPM hack) in 2015, "in a series of classified meetings, officials have struggled to choose among options that range from largely symbolic responses . . . to more significant actions that some officials fear could lead to an escalation of the hacking conflict between the two countries."[49] However, the Obama administration chose diplomacy, and the U.S. government refrained from responding to the OPM hack.[50] After the state visit to the United States in 2015, Chinese President Xi Jinping ordered the arrest of the People's Liberation Army (PLA) members supposedly responsible for the breach.[51] The United States also indicted foreign hackers as a matter of response in some cases. It has indicted five PLA members as well as seven Iranians for their actions on American networks.[52] Two members of the hacktivist group the Syrian Electronic Army are also on the FBI's most wanted list.[53] Early signs say that states such as Russia, China, and North Korea are becoming more brazen, yet how the United States will respond to the changing cyber landscape is still a mystery.

Restraint and Escalation

There have been extensive calls for the United States and other states to "hack back."[54] In fact, some private companies debate this position after they are infiltrated. Yet government operatives tend to understand something that private individuals do not—that the inner workings of a bureaucracy are complex and dangerous. Needlessly provoking an escalatory response in a domain where both sides are wholly unprotected and borderline incompetent could be strategic suicide, especially for a state so plugged-in as the United States.[55] The United States and its Western allies have restrained themselves from escalation for now, but as Russia, Iran, North Korea, and their proxies continue to bombard the electoral processes of these democracies, we could see more dangerous conformations over these matters.

As noted before, disruptions and espionage are what dominate the cyber battlefield and will continue to do so in the future. Cyber weapons intended to degrade are expensive and very often do not work in terms of strategic intent. We have been noticing a reduction in these types of cyber coercive actions and a rise in espionage and disruptions indicating that states are learning the utility of cyber tactics and setting up the battlespace of the future in the cyber domain. This future will see constant hackings that seem to be reported everyday as an intense demonstration of this and provide a stark reminder of the reality of how cyber technologies are used for effect by states and individuals alike. The question that few are asking is: When should you worry about the threat that comes from the cyber domain?

If the reality of cyber conflict is more restrained than many would suggest, we are left with the interesting question of what aspects of the cyber security discourse remain understudied. The obvious answer is the rise of digital espionage and disruptive information campaigns for political effect, either between or within governments. This does not mean that there is not a threat from the newly emerged fifth domain of warfare; this threat comes in the form of exploitations for information through cyber espionage.[56]

The year 2017 has brought many new questions about the stability of the cyber domain. The United States has yet to demonstrate any resolve or serious response to Russian hacking on its electoral process, and it remains to be seen if any active measures will be in place in time for the 2018 midterms. Russian hackers have sparked a crisis in the Middle East by hacking Qatari news agencies, spreading false information, and convincing other Gulf States of Qatar's complacency with terrorist groups, Iran, and Israel. North Korea is taking advantage of systems running on outdated operating systems, and the WannaCry campaign shows just how vulnerable important networks are worldwide.[57] Governments and the private sector need to promote proactive policies that limit these preventable actions in the future.

Data collected in the DCID dataset recording espionage campaigns should be taken as a representative sample under certain constraints. Espionage is a tactic meant to be hidden and not reported, but the issue is that in the cyber domain espionage operations by definition are overt in that they seek to change or steal information, actions that can be witnessed with accurate monitoring of systems. The fact still remains that we are depending on the reporting of these incidents by cyber governments and cyber security companies or actors such as Edward Snowden to release information. It should also be noted that much of the cyber espionage likely occurs outside the domain of rivalry and between friends as much as enemies. Economic targets are also likely prevalent, which would not be captured here.

Norms in the Cyber Realm

Now that we have a better sense of the cyber domain, there needs to be a deeper exploration of just what all of this means from the macro-level of a normative perspective. In this task the cyber security and foreign policy community has failed miserably. The reality of cyber espionage suggests there is a clear need for more rules in cyberspace. On this issue the Obama White House requested Congress to act after the OPM hack, and it sanctioned the Russian government as it was leaving office in December 2016.[58] One apparent goal after these data breaches should be to rethink how we store critical information. That the director of the OPM described their systems as a “hacker’s dream” in November 2014, and the fact that a mere spear-phishing email infiltrated the Democratic National Congress (DNC), should give us pause to rethink our reaction to this latest violation and the need for basic cyber hygiene.[59] Instead of operating in frameworks of violence and aggression, cyber security frameworks likely need to rethink the nature of access, the role of the state, and the purpose of aggression. A big part of the cyber future will rest on international norms and the will to enforce them, which seems imperiled as the United States retreats from its global leadership role.

Norms are expected modes of appropriate behavior for international actors, often invoking how things should be rather than how they might operate in current contexts.[60] When norms are present and adhered to, these international actors are constrained from acting outside of these normative structures.[61] Existing international norms can and, based on our empirical evidence, are being developed by states and institutions to deal with cyber conflict. The good news is that we have had no major operations that include death or destruction of physical equipment outside of a few examples, which suggests that the wider trend in cyber security is to invoke stability and safety according to the norms advocated by the G20. There is a norm of nonaction in terms of cyber conflict.

There have been recent strides made in norm creation where many governments, including Russia and China, along with Western liberal democracies, developed structures and systems to contain the threat of cyber harm. A prime example is the norms created at the November 2015 G20 summit. Three crucial norms were established by countries representing the world's twenty largest economies: "first, no country should intentionally damage the critical infrastructure of another state or impair the use of critical infrastructure that provides services to the public; second, no country should take actions intended to impair the Computer Security Incident Response Team (CSIRT) of another country from responding to cyber incidents and that such CSIRTs should be not be used to do harm online; and third, countries should cooperate with requests from other states to investigate cybercrimes and mitigate malicious cyber activity emanating from their territory."[62]

These aspiring norms stem from the United Nation's (UN) newly created Group of Government Experts (GGE), a collection of cyber security experts from a variety of nation-states.[63] Furthermore, a centerpiece of the agreement between the United States and China crafted during Xi Jinping's state visit in September 2015 was that the two states vowed not to hack each other's intellectual property or critical infrastructure.[64]

The prime reason for these developing norms is that limitation of harm to civilians is an accepted practice in international affairs. Most would recognize the need to limit harm to these groups; even those states that are suggested as possibly violating these norms (such as the United States and Israel) go out of their way to demonstrate concern for civilian victimhood. The limitation on harm to critical systems fits into this normative construct since the prime impact would be on civilians rather than the military. The military could be burdened with repair and containment of disasters, but the main targets would be civilians if a nuclear or conventional power plant were targeted, suggesting that the reason for the acceptance of this limitation is generated out of concern for the rights of individuals.

The true paradox of the digital world is that, while society fears the cyber threat,[65] the reality is that we are actually extremely trusting of the digital infrastructure we have created.[66] Governments and especially the private sector continue to put more and more of their services and inventory online, even in the face of the threat of digital losses. Governments are also turning to cloud computing and blockchains to keep their sensitive information more secure.[67] Contrary to what Roger Hurwitz argues, we place more trust in the Internet than anything in recent memory.[68] We trust it with our connections, our private contacts, our banking, our personal lives, our work lives, even our romantic lives. Yet we fear the digital domain? Instead it has become obvious that there is an abnormal amount of confidence in our digital institutions. This confidence may be unwarranted given how vulnerable a digitally connected state is, yet all digital technology is vulnerable, and resilience is the key to surviving the coming era of low-level Internet-based attacks and probes. This increase in usage of digital systems and cloud computing seems perplexing in the context of increasing surveys that suggest there is much distrust in the Internet by individuals and corporations.[69]

Like traffic laws, a basic understanding of how things work and what limitations there are in digital interactions is for the good of all. Of course, there will be violators, but everyone needs to understand the rules of the road first. Even China and Russia appear to be willing to work within some system of norms, despite protestations to the country by those who would seek escalation. Russia and China's position on the devolution of ICANN makes sense and demonstrates their own need to participate in Internet governance given the importance of digital connectivity to society.

While many may scoff at the idea of norms,[70] in their basic sense they can be effective means to control the basic behaviors of the majority of actors.[71] Of course, there will always be deviants, but as long as we have clear systems of norms, deviancy will be seen as just that—out of the norm. It must be recognized that this is a developing norm. It is in danger of disruption every day since limiting civilian harm is an outcome of the lack of total war. The taboo of chemical weapons operates under the same conditions.[72] No one case of deviancy should destroy a model and norm, but it can surely harm it.

To reinforce a norm of cyber safety, states must be willing to make hard choices in order to make it difficult to even attempt to launch cyber operations. Our digital world is insecure because states and corporations have not made a significant effort to reform and reorganize how we provide computer security. To reform how critical infrastructure is run would be a massive project that no one really is willing to undertake. Most states do not have any functional cooperation between government and private industry for low-level cyber infiltrations. We need more cyber hygiene (internal training on how to deal with potential threats), a reformulation of the critical infrastructure that runs important systems, and greater cooperation between the public and private sectors. Anything less would be irresponsible.

Given there is likely a cyber norm against the use of harmful cyber activities against critical infrastructure and evidence of restraint in cyberspace due to both these normative concerns and strategic limitations, why do we fear this threat vector so much? There is little left to fear but the unknown. The unknown is scary. Do you know how the Internet works? Do you know how your bank accesses your money? Not knowing does not really signify vulnerability but rather a general misunderstanding of processes that are knowable. This would suggest there is an intense future need for research on threat construction, inflation, and the psychological impact of cyber security threat priming.

We can draw parallels between the cyber threat and the terror threat. In both instances, the fear comes from the unknown, the unexplored, and the imagined. With terrorism, we have seen a large industry spring up to deal with the terror threat, as vivid as it may be, and this process continues with the cyber threat. The reaction to terrorism has generally been counterproductive and damaging; it is troubling, then, to see the same path repeated with the industry springing up in the private sector and the military complex to meet the cyber threat.[73] The fact that we have seen little evidence of severe cyber actions must give us pause to question the narrative that a cyber threat is as dangerous as it is presented. Most companies have insurance and do not lose money from data breaches.[74] Sony Pictures was reimbursed the money it lost from the 2014 hack, and it can be posited that the movie *The Interview* was seen by more people due to the publicity.

Yet, this perspective does not preclude or minimize the potential massive impact cyber security has had on national security calculations. While significant escalation in the domain is rare, the proliferation of conflict after a digital violation is possible and more probable in the future. States like China and the United States made significant efforts to reformulate their strategic plans in the wake of the cyber threat. Vulnerability is endemic in cyber security and this reality prompts a reconsideration of future tactics and possibilities when confronted with major work.

While the course of major war might be enabled through cyber activities, it also must be remembered there is an international relations context to cyber disputes. These disputes are not unique to cyberspace but spillover from past disputes between states. It is tough to isolate a purely cyber incident; with this in mind, solving the potential for future cyberwar lies in solving the sources of disagreement between states so that we might avoid cyber doom scenarios. The future of cyberwar between the United States and China should be not be framed as a trap, but as a chance for two powers to manage and construct an international system that allows for digital connectivity to positive relations, rather than war.

The Unknown Cyber Future

Militarizing digital space leaves little room for civilian applications such as research, communication, education, and productivity. As a recent Brazilian report concludes, “the ‘capture’ of resources for cyber-security by the military has potentially dangerous implications for civil liberties more generally in the country.”[75] Given that we are in an era of cyber stability and peace, how do we encourage it to endure? The simplest way is to maintain that attacks by states and nonstate actors alike on civilian populations are off limits. Since in the digital world, there is no real barrier between civilian and government systems, this alone should maintain a level of safety for our digital future since almost any attack is likely to violate this critical line. This of course should be buttressed by greater investment in defenses and resiliency.

Going further, institutions need to be built that might enforce these norms of non-action and cyber protection, yet no one really seems willing to undertake this massive effort because we have yet to see evidence that massive attacks are driving us toward making a significant effort to prepare for what might be possible, even if unlikely. Within the United Nations, Russia, China, and other states have proposed potential frameworks with little success.[76] There is little trust in the United States to lead these efforts since the state is a leading actor in using cyber methods to infiltrate enemies, therefore other states and institutions must take the lead.[77]

Of course, the Internet and digital methods will be used for conflict in the future, but this does not mean it will be a critical or even an evident method of conflict. Like other technologies, cyber tactics will likely support and enhance other methods of violence rather than be the focus or dramatic example of a revolution in the conduct of military force. The Internet remains a sacred place for many, and by emboldening and upholding a norm of cyber safety we can maintain our shared digital futures. This is the key point: the digital life that has become so important should be the highest priority in that the potential avenues for research, education, commerce, and entertainment remain critical to our future.

This all bodes very well for our cyber future. Although the current state of the cyber realm remains questionable with Russian use of the cyber domain for political effect, and the retreat of the United States as a global leader on international issues, including the cyber domain, cyber as a tool for the military is quite limited. While the general fear is that the Internet will be the primary threat vector for future societies, this framework is a bit premature and primarily based on the lack of understanding of how cyberspace works. We fear what we do not understand. Cyberspace can be controlled, but it is a chronically unsafe environment that operates at a low level of intensity. This requires us to understand it, be aware of the possible escalation dynamics at hand in each conflict, and take in all the information possible—not just relying on one source or perspective. Given the convergence of the basics of espionage, restraint, and norms, even the most aggressive of states can be shown to be peaceful actors in our digital frontiers, even while being poked.

Notes

1. ODNI, "Assessing Russian Activities and Intentions in Recent US Elections," accessed May 31, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.
2. Andy Greenberg, "The NSA Confirms It: Russia Hacked French Election Infrastructure." *Wired*, May 9, 2017, accessed May 30, 2017, https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/.
3. Patrick Wintour, "Russian Hackers to Blame for Sparking Qatar Crisis, FBI Warns," June 7, 2017, accessed June 12, 2017, https://www.theguardian.com/world/2017/jun/07/russian-hackers-qatar-crisis-fbi-inquiry-saudi-arabia-uae.
4. Debra Killalea, "Qatar Crisis: Saudi Arabia, Allies Issue 'Terrorism' List," *news.com.au*, June 10, 2017, accessed June 17, 2017, http://www.news.com.au/finance/economy/world-economy/qatar-crisis-saudi-arabia-allies-issue-terrorism-list/news-story/2b2d9a70ab78d0e943faa9d7919e9a58.
5. Al Jazeera, "Hackers 'to Leak' Emails of UAE Ambassador to US," *Aljazeera.com*, June 3, 2017, accessed June 15, 2017, http://www.aljazeera.com/news/2017/06/hackers-leak-emails-uae-ambassador-170603110132159.html.
6. Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The EvolvingNature of Cyber Power and Coercion*, forthcoming, Oxford University Press.
7. Patrick Smith, "As Trump Abdicates Global Leadership, Europe Moves to Fill in the Vacuum," *The Fiscal Times*, June 2, 2017, accessed June 15, 2017, https://www.thefiscaltimes.com/Columns/2017/06/02/Trump-Abdicates-Global-Leadership-Europe-Moves-Fill-Vacuum.
8. Abhinandan Mishra, "Concerns Deepen about Cyber Attack on Su 30, IAF Starts Inquiry," *Sunday Guardian Live*, June 4, 2017, accessed June 13, 2017, http://www.sunday-guardianlive.com/investigation/9670-concerns-deepen-about-cyber-attack-su-30-iaf-starts-inquiry?utm_content=buffer5c7a3&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer.
9. Chris Bing, "A Stolen Trump-Duterte Transcript Appears to be Just One Part of a Larger Hacking Story," *Cyberscoop*, May 31, 2017, accessed June 12, 2017, https://www.cyberscoop.com/apt-32-trump-duterte-hacking-xi-jinping-vietnam/.

10. Joe Uchill, "Symantec Increasingly Confident Ransomware Attack Linked to North Korea," *The Hill*, June 22, 2017, accessed June 6, 2017, http://thehill.com/policy/cybersecurity/334658-symantec-increasingly-confident-wanna-cry-linked-to-north-korea.
11. Miriam Dunn-Cavelty, "The Normalization of Cyber-International Relations," in *Strategic Trends 2015: Key Developments in Global Affairs*, ed. Oliver Thränert and Martin Zapfe (Zurich, Switerland, CSS, 2015), 83.
12. Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (New York: Oxford University Press, 2015).
13. Hans-Inge Lango, "Competing Theoretical and Conceptual Approaches to Strategic Cyber Security," in *Conflict in Cyber Space: Theoretical, Strategic, and Legal Perspectives*, ed. Karsten Friis and Jens Ringsmore (London: Routledge, 2016).
14. Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security* 38, no. 2 (2013): 7–40. Dale Peterson, "Offensive Cyber Weapons: Construction, Development, and Employment," *Journal of Strategic Studies* 36, no. 1 (2013): 120–124.
15. See Miriam Dunn-Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (New York: Routledge, 2008); Sean Lawson, "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats," Journal of Information Technology & Politics 10, no. 1 (2013): 86–103; Erik Gartzke, "The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth," *International Security* 38, no. 2 (2013): 41–73; Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 365–404; Mark Raymond, "Puncturing the Myth of the Internet as a Commons," *Georgetown Journal of International Affairs* (2013): 53–64; Charles Guitton, "Cyber Insecurity as a National Threat: Overreaction from Germany, France and the UK?," *European Security* 22, no. 1 (2013): 21–35.
16. See Adam Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies* 35, no. 3 (2012): 401–428; Derek Reveron, "An Introduction to National Security and Cyberspace," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek Reveron (Washington, DC: Georgetown University Press); David Betz, "Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed," *Journal of Strategic Studies* 35, no. 5 (2012): 689–711; Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst & Company, 2013); Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986–2012*, (Washington, D.C.: CCSA Atlantic Council); Brandon Valeriano and Ryan C. Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001–2011," *Journal of Peace Research* 51, no. 3 (2014): 347–360.
17. Valeriano, Jensen, and Maness, *Cyber Coercion*.
18. Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2017]): 44–71.
19. Brandon Valeriano and Alison Pytlak, "'Closing That Internet Up': The Rise of Cyber Repression," *Council on Foreign Relations Net Politics*, January 13, 2016, accessed May 30, 2017, https://www.cfr.org/blog-post/closing-internet-rise-cyber-repression.
20. Jon R. Lindsay and Lucas Kello, "Correspondence: A Cyber Disagreement," *International Security* 39, no. 2 (2014): 181–192.
21. Kello, "Meaning of the Cyber Revolution," 22.
22. David E. Sanger and Eric Schmitt, "US Cyberweapons, Used against Iran and North Korea, Are a Disappointment against ISIS," *New York Times*, June 12, 2017, accessed June 16, 2017, https://www.nytimes.com/2017/06/12/world/middleeast/isis-cyber.html.

23. Lindsay and Kello, "Correspondence: A Cyber Disagreement," 184.
24. Ibid., 188.
25. Kello, "Meaning of the Cyber Revolution," 192.
26. E. Gartzke and J. R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015): 316–348.
27. Timothy Junio, "How Probable Is Cyber War? Bringing IR Theory Back into the Cyber Conflict Debate," *Journal of Strategic Studies* 36, no. 1 (2013): 125–133. Adam P. Liff, "The Proliferation of Cyberwarfare Capabilities and Interstate War, Redux: Liff Responds to Junio," *Journal of Strategic Studies* 36, no. 1 (2013): 134–138.
28. Ellen Nakashima, "Russia Has Developed a Cyberweapon That Can Disrupt Power Grids, according to New Research," *Washington Post*, June 12, 2017, accessed June 14, 2017, https://www.washingtonpost.com/world/national-security/russia-has-developed-a-cyber-weapon-that-can-disrupt-power-grids-according-to-new-research/2017/06/11/b91b773e-4eed-11e7-91eb-9611861a988f_story.html?hpid=hp_hp-top-table-main_russiascyber-810a%3Ahomepage%2Fstory&utm_term=.86886b7491db.
29. David C. Gompert and Martin Libicki, "Cyber Warfare and Sino-American Crisis Instability," *Survival* 56, no. 4 (2014): 7–22.
30. FireEye, "Red Line Drawn: China Recalculates Its Use of Cyber Espionage," *FireEye*, June 20, 2016, accessed May 30, 2017, https://www.fireeye.com/blog/threat-research/2016/06/red-line-drawn-china-espionage.html.
31. Chris Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* (Spring 2011): 32–61.
32. Shaun Walker, "Russian Data Law Fuels Surveillance Fears," *The Guardian*, September 1, 2015, accessed February 14, 2015, http://www.theguardian.com/world/2015/sep/01/russia-internet-privacy-laws-control-web.
33. Valeriano and Maness, *Cyber War versus Cyber Realities*, 41.
34. Valeriano, Jensen, and Maness, *Cyber Coercion*.
35. Rid, *Cyber War Will Not Take Place*, xiv.
36. Daniel Moore and Thomas Rid, "Cryptopolitik and the Darknet," *Survival* 58, no. 1 (2016): 7–38.
37. Moore and Rid Cryptopolitik and the Darknet.
38. Raymond Puncturing the Myth, Moore and Rid Cryptopolitik and the Darknet.
39. ODNI, "Assessing Russian Activities and Intentions."
40. J. R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack," *Journal of Cybersecurity* 1: 1, 53–67.
41. Valeriano and Maness, Cyber War versus Cyber Realitieschap. 7; Moore and Rid, Cryptopolitik and the Darknet.
42. Valeriano and Maness, Cyber War versus Cyber Realities.
43. Ryan C. Maness and Brandon Valeriano, "The Impact of Cyber Conflict on International Interactions," *Armed Forces and Society* 42, no. 2 (2016): 301–323. Ryan C. Maness and Brandon Valeriano, "Cyber Spillover Conflicts: Transitions from Cyber Conflict to Conventional Foreign Policy Disputes?," in *Conflict in Cyberspace*, ed. Karsten Friis and Jens Ringsmose (New York: Routledge, 2016): 45–64.
44. Valeriano, Jensen, and Maness, Cyber Strategy.
45. Ibid.
46. Ryan C. Maness and Brandon Valeriano, "Coding Manual for v1.1 of the Dyadic Cyber Incident and Dispute Dataset, 2000–2014," unpublished manuscript, 2017.

47. Valeriano, Jensen, and Maness, Cyber Strategy.
48. Ibid.
49. David Sanger, "US Decides to Retaliate against China's Hacking," *New York Times*, July 31, 2015, accessed May 24, 2017, https://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html.
50. Ellen Nakashima, "U.S. Decides against Publicly Blaming China for Data Hack," *Washington Post*, July 21, 2015, accessed August 3, 2015, https://www.washingtonpost.com/world/national-security/us-avoids-blaming-china-in-data-theft-seen-as-fair-game-in-espionage/2015/07/21/03779096-2eee-11e5-8353-1215475949f4_story.html?postshare=5111437568103665.
51. Ellen Nakashima. "Chinese Government Has Arrested Hackers It Says Breached OPM Database," *Washington Post*, December 2, 2015, accessed February 22, 2016, https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html.
52. Michael S. Schmidt and David E. Sanger, "5 in China Army Face U.S. Charges of Cyberattacks," *New York Times*, May 19, 2014, http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html?_r=0. David E. Sanger. "U.S. Indicts 7 Iranians in Cyberattacks on Banks and a Dam," *New York Times*, March 24, 2016, accessed March 27, 2016, http://www.nytimes.com/2016/03/25/world/middleeast/us-indicts-iranians-in-cyberattacks-on-banks-and-a-dam.html.
53. Federal Bureau of Investigation, "Syrian Cyber Hackers Charged," *FBI.gov*, March 22, 2016, accessed April 1, 2016, https://www.fbi.gov/news/stories/2016/march/two-from-syrian-electronic-army-added-to-cybers-most-wanted/two-from-syrian-electronic-army-added-to-cybers-most-wanted.
54. Carl Franzen, "Should US Companies be Allowed to Hack China in Revenge? New Report Says Yes," *The Verge*, May 22, 2013, accessed May 23, 2017, https://www.theverge.com/2013/5/22/4356196/report-tells-congress-companies-should-hack-back.
55. Adam Elkus, "No Patch for Incompetence: Our Cybersecurity Problem Has Nothing to Do with Cybersecurity," *War on the Rocks*, June 23, 2015, accessed August 9, 2015, http://warontherocks.com/2015/06/no-patch-for-incompetence-our-cybersecurity-problem-has-nothing-to-do-with-cybersecurity/.
56. Matt Murphy, "War in the Fifth Domain," *The Economist*, July 1, 2010, accessed June 7, 2015, http://www.economist.com/node/16478792.
57. Uchill Symantec Increasingly Confident Ransomware Attack Linked.
58. APM, "White House Presses for New Cyber Laws after Vast Hack," *AFP, Yahoo News*, June 5, 2015, accessed June 24, 2015, http://news.yahoo.com/white-house-presses-cyber-laws-vast-hack-203123226.html.
59. David E. Sanger, Julie Hirschfield Davis, and Nicole Perlroth, "U.S. Was Warned of System Open to Cyberattacks," *New York Times*, June 5, 2015, accessed July 1, 2015, http://www.nytimes.com/2015/06/06/us/chinese-hackers-may-be-behind-anthem-premera-attacks.html.
60. M. Finnemore and D. B. Hollis, "Constructing Norms for Global Cybersecurity," *American Journal of International Law* 110, no. 3 (2016): 425–479.
61. M. Finnemore and K. Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (1998): 887–917.

62. Christopher Painter, "G20: Growing International Consensus on Stability in Cyberspace," *State.gov*, December 3, 2015, accessed March 13, 2016, https://blogs.state.gov/stories/2015/12/03/g20-growing-international-consensus-stability-cyberspace.
63. United Nations Office for Disarmament Affairs, "GGE information Security," 2015, accessed March 14, 2016, http://www.un.org/disarmament/topics/informationsecurity/.
64. The White House, "Fact Sheet: President Xi Jinping's State Visit to the United States," *Whitehouse.gov*, September 25, 2015, accessed April 1, 2016, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.
65. Bruce Stokes, "Extremists, Cyber-Attacks Top Americans' Security Threat List," *Pew Research Center*, January 2, 2014, accessed June 7, 2015, http://www.pewresearch.org/fact-tank/2014/01/02/americans-see-extremists-cyber-attacks-as-major-threats-to-the-u-s/.
66. Brandon Valeriano, Ryan C. Maness, and Sean Lawson, "The Economics of the Cyber Security Threat: The Concept of Cyber Shrinkage and Framing Loss," 2017, under review.
67. Willaim D. Eggers, "Better Faster, Cheaper. Cloud Computing in Government Explodes," *Governing.com*, January 31, 2011, accessed March 2, 2016, http://www.governing.com/blogs/bfc/cloud-computing-government-explodes.html.
68. Roger Hurwitz, "Depleted Trust in the Cyber Commons," *Strategic Studies Quarterly* 6, no. 3 (2012): 20–45.
69. NCCGroup, Trust in the Internet Survey, 2015, accessed April 1, 2016, https://whodoyou.trust/globalassets/documents/trust-in-the-internet-survey-paper.pdf. Mary Madden and Lee Raine, "Americans' Attitudes about Privacy, Security, and Surveillance," *Pew Research Center*, May 20, 2015, accessed March 29, 2016, http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/. Erica Ho, "Almost Everyone Doesn't Trust the Internet," *Time*, July 23, 2012, accessed April 1, 2016, http://newsfeed.time.com/2012/07/23/almost-everyone-doesnt-trust-the-internet/.
70. See Valeriano and Maness, Cyber War versus Cyber Realities.
71. Finnemore and Hollis, Constructing Norms; Valeriano and Maness, Cyber War versus Cyber Realities: Chapter 8.
72. R. M. Price, *The Chemical Weapons Taboo* (Ithaca: Cornell University Press, 1997).
73. J. E. Mueller, *Overblown: How Politicians and the Terrorism Industry Inflate National Security Yhreats, and Why We Believe Them* (New York: Simon & Schuster, 2006).
74. Valeriano, Maness, and Lawson, Cyber Skrinkage.
75. "Deconstructing Cyber Security in Brazil: Threats and Responses." *Igarape Institute*, December 1, 2014, accessed July 6, 2015, http://www.igarape.org.br/en/?s=deconstructing+cyber+security.
76. Tim Maurer, "Cyber Norm Emergence at the United Nations: An Analysis of the UN's Activities Regarding Cyber-security," *Belfer Center Discussion Paper 2011-11*, September 2011, accessed May 5, 2014, http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf. Alex Grigsby. "The UN GGE on Cybersecurity: What Is the UN's Role?" *Council on Foreign Relations*, April 15, 2015, accessed June 7, 2015, http://blogs.cfr.org/cyber/2015/04/15/the-un-gge-on-cybersecurity-what-is-the-uns-role/.
77. Henry Farell, "Promoting Norms for Cyberspace," *Council on Foreign Relations*, April 2015, accessed June 7, 2015, http://www.cfr.org/cybersecurity/promoting-norms-cyberspace/p36358.