NEW FRONTIER IN DEFENSE: CYBERSPACE AND U.S. FOREIGN POLICY

A National Committee on American Foreign Policy Report

By Simran R. Maker

May 2017

About the Organization

The National Committee on American Foreign Policy (NCAFP) was founded in 1974 by Professor Hans J. Morgenthau and others. It is a nonprofit policy organization dedicated to the resolution of conflicts that threaten U.S. interests. Toward that end, the NCAFP identifies, articulates, and helps advance American foreign policy interests from a nonpartisan perspective.

About the Author

Simran R. Maker is in charge of the Cybersecurity Initiative at the NCAFP, where she manages, organizes, and runs cyber programs and conferences as well as produces research and reports. She is also responsible for the Middle East Initiative and selected other long-term projects at the organization.

Acknowledgments

The success of this conference would not have been possible without the forthcoming and candid participation of the ten experts involved (listed at the end of the report). Their observations and insights were invaluable. We are grateful to each of them and hope to work with each of them again. A special thanks goes to the Conference Chair, whose input and feedback was especially instrumental and whose wise counsel remains indispensable: Rafal Rohozinski.

The NCAFP would also like to thank all of our cyber donors for their generous and continued support, particularly our principal sponsor, John H. Bell, Jr. Last but certainly not least, Edythe M. Holbrook has been a valued asset as a tireless advocate and champion of the project, securing its funding from the inception. Her encouragement and enthusiasm have been irreplaceable.

Thank you all for your contributions, participation, support, and guidance along the way.

Images

All images used in this report are sourced from Public Domain and Creative Commons databases. In accordance with usage guidelines and licensing rules, each image is directly followed by details and proper attribution. The cover image is credited below.

Cover Image
This work, "Red Binary World" by Simran R. Maker is a derivative of "Green Binary Codes and World Map" by Oda Gerdes, used under CC0 1.0 Universal.

May 2017

NEW FRONTIER IN DEFENSE: CYBERSPACE AND U.S. FOREIGN POLICY

A National Committee on American Foreign Policy Report

By Simran R. Maker

May 2017

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

The cyber domain is a synthetic one – unlike any other domain of human conflict. It is not a natural extension of human battlegrounds. It was not a byproduct of any national or international institutions. It did not stem seamlessly from any predictable field. Nevertheless, now that it has arrived, it is inextricably linked to the future of international interaction – whether friendly or adversarial; cooperative or competitive.

Cybersecurity is much more than just information security. It is about the protection of all systems – tangible and intangible – that rely on online networks to function. The more connected we are, the more vulnerable we can be. Thus, it is absolutely paramount to simultaneously focus on the two fundamental sides of cybersecurity – as with any of the other domains: defense and offense. A nation must not only be able to safeguard its own cyber channels, but it must also be capable of countering with its own attacks – where deemed to be in its best interests.

The newness of this battlefield pits it in a purgatorial state of existing and not existing at the very same time. There is no Law of Cyberspace as there is a Law of the Sea. There is no prosecuting body like the International Court of Justice or the International Criminal Court. There are no international norms to govern or oversee cyber ethics. The cyber domain is yet a jungle; a void – where some nations will try to extend their normative behavior from other domains, only to be disappointed that their adversaries have not similarly handcuffed themselves.

Clearly, the general population is fascinated with the nexus of cybersecurity and politics. And it is an important theme for the population to begin to grasp and unpack. More urgently, it is an important subject for the policy community to grapple with – not just the "techies" or the cyber gurus; all of us.

The field is not only central because of the depth and breadth of the cyber domain; it is also significant because of growing cyber capabilities around the globe. Nations that are either unable or unwilling to challenge the U.S. in theaters of conventional warfare are commanding substantial attention in cyberspace. Countries are increasingly leveraging cyberspace as a short-of-war domain. The advantages abound for irregular and asymmetric warfare. Cyber activity also provokes a lower risk of attribution or retaliation than traditional domains. Concrete evidence is more difficult to compile and verify. Some states, like the U.S., are reticent to publicly attribute attacks. A large portion of cyber attacks, in fact, thread the needle between disruption and destruction – sometimes skewing the cost-benefit calculus for retaliation. This renders cyber attacks an effective tool for disruptive tactics – for both political and economic means.

At the same time, some experts frame cyber threats in terms of cyber opportunities. Perhaps cyberspace presents a new sphere of opportunity with all the room for innovation and growth. Maximizing such potential, harnessing these prospects, and driving greater modernization could prospectively lead to a cyber sector workforce that propels America to the next level of security and prosperity alike. There certainly is a need for it.

§

When grappling with issues of such significance to national security, working within the right framework is essential. First and foremost, cybersecurity must be couched in the overarching foreign policy agenda.

It must be understood as a foreign policy tool. The relationship between U.S. foreign policy and cybersecurity is not only bidirectional; it is interdependent. A shift in America's foreign policy posture can have significant implications around the globe – in multiple regions, on multiple levels, in multiple dimensions. Now cybersecurity inarguably stands as one of these dimensions.

Therefore, a grave part of the problem is the misunderstanding and wrongful prioritization of threats. Yet again, this circles back to the underlying truth that cyber activity is merely a tool – an extension – of the differing foreign policy agendas of different nations. It is vital to unpack the overarching foreign policy postures of threat actors in order to gain a more lucid view of their cyber intentions. Only then can the U.S. properly forecast and anticipate what form the corresponding threats emerging from each country will assume, in order to optimally prepare and defend against each of them.

In terms of understanding cyber threats on a macro level, a few nuances must be observed. Cyber threats are all too often generalized into the black or white categories of cyber crime or cyber war. Such an oversimplification not only distorts the types of threats themselves, but it also vastly misses the nuances of intent that play a role in shaping how the threats will manifest or metamorphosize. Somewhere on the sliding scale, there are three gray areas holding enormous weight and factoring in intent: *cyber espionage* – which can be political or commercial in nature, always with an element of spying; *cyber subversion* – which often relies on the manipulation of information to have an undermining effect; and *cyber sabotage* – which generally involves a level of physical destruction with the goal of obstruction.

As a country, we do not have a cyber problem. We have a China problem; a North Korea problem; an Iran problem; a Russia problem. And cyber attacks will not be the only tool used to achieve our adversaries' goals.

Defensively, we have it all wrong. We have been destruction-focused, worrying about the protections in place for our physical and critical infrastructure. The Russians are on to something with their emphatic turn towards information warfare. Even the Chinese are more active in this realm. North Korea, too, has shown signs of leaning more towards info wars, as evidenced by the 2014 Sony Pictures Hack. By misunderstanding which playground our adversaries are playing on, we have handicapped ourselves and limited our vantage point. Had we been more cognizant of this, we would have seen that the Russian hack of the U.S. elections was actually quite unsurprising. Did we learn nothing from Russia's test drive of similar tactics with the Ukraine elections? We have been ignoring the smoke signals for too long. But we can no longer afford to do so.

As this report stresses, we must ultimately frame the cyber debate within the larger foreign policy debate. This inherently leads us back to the most elementary question – one that lies at the very root of foreign policymaking since the beginning of time: Who are our most dangerous adversaries? As far as nation-states go, the list is fairly straightforward in the present era – though the sequence of the list may well be cause for debate. Today, no list would be complete without an examination of China as a competitor; North Korea as an instigator; Iran as a challenger; and Russia as an opponent.

§

The strongest practical recommendation must be a greater emphasis on credible deterrence. One major attitudinal shift has had a tangible impact: over the last few administrations, there has been a move away from tolerating the theft of intellectual property – a threat that has been labeled "the greatest

transfer of wealth in history" by General Keith Alexander, the first Commander of the U.S. Cyber Command. There should similarly be less tolerance with other cyber targeting.

To combat these traditional adversaries, more needs to be done to collaborate with traditional allies that can also be cyber allies. Only in working with international partners, can cyber norms be created and carried out in a meaningful way. Cyber cooperation must continue to be a pillar in any policy conversation on cybersecurity. In this domain, however, a word of caution might be necessary. Traditional partners may be dressed differently; and expected adversaries may take different forms. Washington can expect the same players to arrive at the cyber ball, but it must not be too shortsighted – lest it miss a threat masquerading as a non-threat.

To reach a sounder understanding, a valuable lesson can be drawn from the operational tendencies of USCYBERCOM: the comingling of "adversary experts" – or area specialists – with the sea of technical experts. Area experts are an integral component in shaping response options within the military. Their presence enables a more consistent campaign of actions, particularly when it comes to deterrence. In this way, decision-makers can connect the dots between what will be possible and what will be effective. This is a paradigm that must be underscored and applied to other elements of the cybersecurity effort, especially as cyber specialists come to terms with the fact that their world is just a molecule in the foreign policy universe.

Moreover, while Cyber Command has begun to formalize and institutionalize mechanisms for capacity building, this is a focus that must continue to be prioritized across the board. Rhetoric about capacity building must be met with the appropriate investments and resources. Across the government, systems need to be upgraded, protocols need to be streamlined, and encryption needs to be standardized. Threat scenarios should be built out and prepared for, so that there is never again a simple attack that catches the government totally off guard – as with the White House and DoS attacks of 2014. As such, technical experts and policymakers need to exchange ideas on what short and long-term digital transformations look like. They need to discuss how to scale security benefits so they extend to departments that would not traditionally be expected cyber targets – like the Office of Personnel Management.

These feats should not be left solely to the military. There must also be a continuing role for the private sector. Across the last few administrations, there has been a consensus of sorts, but there might be a shift in direction under the new administration. Where President Obama was distinctly cautious not to over-militarize the issue of cybersecurity, the current administration might be altering the approach so that cyberspace falls more squarely under the purview of the military. It will be crucial to keep the private sector involved, and even to allow it to take the lead in improving cybersecurity solutions when called for.

What cannot be disputed is the key role the private sector has played thus far, and the central role it will – and must – continue to play going forward. It would be an error of judgment to siphon off the private sector from the problems of the government. American corporations are still American, with a vested interest in sustaining cybersecurity for the nation writ large. The current administration has floated the idea of compartmentalizing the private sector from the public sector in this domain, but this would actually be an oversight with unforeseeable implications. While there is unquestionably a need for certain cyber knowledge to remain classified to only the highest guardians of U.S. defense, individual companies within the private sector may have capabilities that are not always readily available to large bureaucracies within the government. They also have greater latitude for trial and error operations,

affording them the leeway to arrive at the best solutions through a process of deduction – something that government actors cannot always afford to experiment with.

Nevertheless, these recommendations (and others interwoven below) will be far less effective if the overarching dialogue on cybersecurity is not framed properly. Accordingly, this is the most crucial takeaway. What has been stressed throughout this analysis is that cybersecurity must be couched within the larger foreign policy discourse. It is vital to address one when addressing the other. Cyber defenses can be improved and cyber offenses can be upgraded, but the best way to further the country's cybersecurity is to ameliorate and better manage America's relationships with the very adversaries that become threat actors in cyberspace. This cannot be emphasized enough: We do not have a cyber problem. We have a China problem. A North Korea problem. An Iran problem. A Russia problem.

The discussion on cyber issues can be extensive and varied, but within the context of foreign policymaking, we must reflect on how advancing technology affects the business of statecraft. Just as the evolution of media revolutionized state-to-state politics on the global stage, current developments are reorganizing the way we receive information and perceive subjects – arguably in a much swifter, less noticeable way than ever before. But the cycle of change itself is not new. With each new connective technology, the world has gotten metaphorically flatter – for the average citizen: more accessible; more comprehensible; more immediate; more relevant. In this more connected world, cybersecurity matters more than ever before. Society has greatly benefited as technology has become more advanced and everything has become more networked, but it is also more vulnerable for these very same reasons.

II. INTRODUCTION

On February 2, 2017, the National Committee on American Foreign Policy (NCAFP) led a cybersecurity conference entitled **New Frontier in Defense: Cyberspace and U.S. Foreign Policy**. The objectives of the daylong conference were manifold: to analyze the global shifts in the cybersecurity arena – particularly on a nation-state level; to examine the current threat landscape – identifying vulnerabilities and weaknesses; to consider U.S. progress – assessing both offensive and defensive capabilities; and to chart the course forward – acknowledging achievements and areas in need of further action or prioritization.

The conference was broken down into three concentrated roundtable discussions: (1) The Evolving Cybersecurity Threat Landscape; (2) Short of War: Lessons of the Russia Hack of the American Elections; and (3) Cyberspace and U.S. Foreign Policy: Assessing Achievements and Prioritizing Action.

The NCAFP was fortunate to be joined by some of the most eminent experts in this cutting-edge field. Ten accomplished thought leaders and practitioners shared their personal and professional views – from government and policymaking institutions; academia and think tanks; private sector and technology firms. We were also fortunate to have a keynote address by an influential journalist who has long studied cybersecurity advances and policy decision-making within the U.S. government and in various parts of the world.

The conference followed Chatham House Rules in order to allow free and open discussion without attribution. While this binds the participants from divulging the identity or specific affiliation of those present, it was agreed that key themes and valuable insights could be integrated into a report. Accordingly, the report that follows draws from noteworthy points at the NCAFP conference, while also adding context from external research.

The chapter following the introduction frames the subject at hand and contextualizes the discussion ahead – first in terms of the growing need for attention to this area, and second, in terms of the current political climate. The next chapter more closely examines the evolving cybersecurity threat landscape, aligning with the conference before delving slightly deeper into a bit of background on a few key countries demanding further examination. The subsequent chapter extends the country theme with a deeper analysis of the Russian hack of the 2016 American elections – a vital topic that demands its own separate analysis. Finally, the last chapter provides a broad view of progress and success in this arena, blended with a flowing discussion of related recommendations. By no means does this report contain all the answers; but it does, however, pose several important questions while highlighting potential ideas to enhance America's cybersecurity.

III. The Current Context

A. Why Cybersecurity Matters, More Now Than Ever

The cyber domain is a synthetic one – unlike any other domain of human conflict. It is not a natural extension of human battlegrounds. It was not a byproduct of any national or international institutions. It did not stem seamlessly from any predictable field. Nevertheless, now that it has arrived, it is inextricably linked to the future of international interaction – whether friendly or adversarial; cooperative or competitive.

INFORMATION CAN BE CONSIDERED THE ORIGINAL WEAPON.

In military doctrine, the four traditional domains – land, sea, air, and space – all became fair game when we moved into the fourth generation of warfare. As the lines continued to further blur – between each of these domains; between state and nonstate actors; between combatants and civilians – we began to mark the fifth generation of warfare. The most interesting change here is the acknowledgment of the weaponization of information in warfare. In some ways, information can be considered the original weapon, but formally recognizing its role adds depth to a certain understanding of warfare. As we live through different iterations of hybrid warfare, cybersecurity becomes a pivotal element in controlling the flow of information.

THE MORE CONNECTED WE ARE, THE MORE VULNERABLE WE CAN BE.

Cybersecurity, nevertheless, is much more than just information security. It is about the

protection of all systems – tangible and intangible – that rely on online networks to function. The more connected we are, the more vulnerable we can be. Thus, it is absolutely paramount to simultaneously focus on the two fundamental sides of cybersecurity – as with any of the other domains: defense and offense. A nation must not only be able to safeguard its own cyber channels, but it must also be capable of countering with its own attacks – where deemed to be in its best interests. The newness of this battlefield pits it in a purgatorial state of existing and not existing at the very same time. There is no Law of Cyberspace as there is a Law of the Sea. There is no prosecuting body like the International Court of Justice or the International Criminal Court. There are no international norms to govern or oversee cyber ethics. The cyber domain is yet a jungle; a void – where some nations will try to extend their normative behavior from other domains, only to be disappointed that their adversaries have not similarly handcuffed themselves.

THE CYBER DOMAIN IS YET A JUNGLE; A VOID – WHERE SOME NATIONS WILL TRY TO EXTEND THEIR NORMATIVE BEHAVIOR FROM OTHER DOMAINS, ONLY TO BE DISAPPOINTED THAT THEIR ADVERSARIES HAVE NOT SIMILARLY HANDCUFFED THEMSELVES.

And perhaps it is this freshness or this lack of clarity that attracts so many people – who would otherwise not be interested in defense and security issues – to the subject of cybersecurity. Readers flocked to stories on Russia's attempts to interfere with the 2016 U.S. elections. Over two-and-a-half million readers perused the New York Times coverage of the topic. Follow-up stories have been spotted on the smallest of blogs and the largest of newspapers – even several weeks after the conclusion of the election. The coverage has only been amplified with the ongoing Federal Bureau of Investigation's (FBI) probe into the reach of the Russians. Clearly, the general population is fascinated with the nexus of cybersecurity and politics. And it is an important theme for the population to begin to grasp and unpack. More urgently, it is an important subject for the policy community to grapple with – not just the "techies" or the cyber gurus; all of us.

NATIONS THAT ARE EITHER UNABLE OR UNWILLING TO CHALLENGE THE U.S. IN THEATERS OF CONVENTIONAL WARFARE ARE COMMANDING SUBSTANTIAL ATTENTION IN CYBERSPACE. COUNTRIES ARE INCREASINGLY LEVERAGING CYBERSPACE AS A SHORT-OF-WAR DOMAIN. THE ADVANTAGES ABOUND FOR IRREGULAR AND ASYMMETRIC WARFARE.

The field is not only central because of the depth and breadth of the cyber domain; it is also significant because of growing cyber capabilities around the globe. Nations that are either unable or unwilling to challenge the U.S. in theaters of conventional warfare are commanding substantial attention in cyberspace. Countries are increasingly leveraging cyberspace as a short-of-war domain. The advantages abound for irregular and asymmetric warfare. Cyber activity also provokes a lower risk of attribution or retaliation than traditional domains. Concrete evidence is more difficult to compile and verify. Some states, like the U.S. are reticent to publicly attribute attacks. A large portion of cyber attacks, in fact, thread the needle between disruption and destruction – sometimes skewing the cost-benefit calculus for retaliation. This renders cyber attacks an effective tool for disruptive tactics – for both political and economic means.

At the same time, some experts frame cyber threats in terms of cyber opportunities. Perhaps cyberspace presents a new sphere of

opportunity with all the room for innovation and growth. Maximizing such potential, harnessing these prospects, and driving greater modernization could prospectively lead to a cyber sector workforce that propels America to the next level of security and prosperity alike. There certainly is a need for it.

B. The Political Environment

In order to turn rhetoric into reality, the new administration must build an overarching cyber vision with an acute understanding of the systems in place, their strengths and weaknesses, and the overall cyber threat landscape. Given that cybersecurity now connects to all aspects of governance, cyber priorities must stand upon an intricate understanding of threats as well as capabilities. Only then can meaningful action be taken to shape a cohesive and comprehensive cyber strategy.

The president has conscientiously emphasized the need for greater attention to America's cybersecurity programs – on the campaign trail and in the early days of the presidency alike. President Trump has himself called for a unified overhaul of the country's cyber defenses, stipulating the need for more effective cyber measures in both the private and public sectors. The center stage placement of these issues is an encouraging sign.

The next few months will be a crucial period of watchful waiting. All eyes should be on actions taken – both operationally as well as politically. Thus far, there are two starting points that may foreshadow the general direction ahead: (1) the much-anticipated Cyber Executive Order (EO) and (2) the White House's first Budget Blueprint to Congress.

Drafts of the Cyber EO emerged within weeks of the inauguration, but nothing was finalized and signed until May 2017. The signed order lays out concerns and tackles them in more technical and specific terms. The aim remains the same: to explicitly assign responsibilities for protecting and securing the federal government, the country's critical infrastructure, and the American people from cyber attacks. The basics are not ignored, as engendering greater modernization and resilience are major priorities along with recommendations for better shared security protocols and procedures. These are long overdue efforts that direly need to be seen to fruition before any other measures can prove effective. It is not just the mindset that needs to be upgraded, after all; it is also the technology and systems.

The EO carefully spells out the need for vulnerability and capability considerations across the board. In a shift from previous drafts, the final order sets hard deadlines and deliverables, tasking key agency heads on crucial areas. Full reports are demanded for necessary steps such as risk management reviews of federal networks, critical infrastructure checks, situation analysis on electricity disruption, safeguards against distributed threats jeopardizing internet safety, and scenario analysis on defense and industrial base resilience.

> **"AS A HIGHLY CONNECTED NATION, THE UNITED STATES IS ESPECIALLY DEPENDENT ON A GLOBALLY SECURE AND RESILIENT INTERNET AND MUST WORK WITH ALLIES AND OTHER PARTNERS TOWARD MAINTAINING [THIS]."**
> **– CYBER EXECUTIVE ORDER, MAY 2017**

Perhaps one of the most meaningful enhancements is also one of the most subtle: paying due attention to America's cyber relations with other international actors. There are entirely new and rather promising, if brief, points on international cooperation and competition. In one aspect, the order declares: "As a highly connected nation, the United

States is especially dependent on a globally secure and resilient internet and must work with allies and other partners toward maintaining [this].” Articulating this here is not the same as making a passing comment in a speech. This cements more of an overall ideology about America’s priorities for cyberspace. Cooperation is only one side of the coin, nevertheless. As such, broadening the scope of international considerations is fundamental. To that end, agency heads for key government divisions are now required to submit holistic reports directly to the president “on their international cybersecurity priorities, including those concerning investigation, attribution, cyber threat information sharing, response, capacity building, and cooperation.”

On workforce development, there is a sharp awareness that international watchfulness will be a telling indicator of America’s continued competitive advantage in the cyber arena. To note, the order calls for monitoring “the workforce development efforts of potential cyber peers in order to help identify foreign workforce development practices likely to affect long-term United States cybersecurity competitiveness.” In fact, the broad attention given to the cyber workforce, emphasizing future generations, is a welcome change. It is not only crucial to patch vulnerabilities and build capabilities for the near future; it is equally imperative to ensure resilience into the far future. What better way to do so than to start reaching the next generation now? They must be interested, prepared, and focused now, in order to be involved later – in both the private and public sectors. Recognizing this and dedicating resources to such a purpose is incredibly important.

Private sector cyber companies have long been proposing better training programs to ready the next generation of cyber professionals. In fact, this is one area of professional services where the number of openings overwhelms the number of job applicants. A focused method to filling this void could do tremendous good in leveling out some of the unemployment issues the country is currently facing, while also bringing the economy back to the forefront of the global service and technology sectors – ones that the U.S. was a longtime leader in, but other advancing countries are now quickly closing in on. This very topic will poke its head later in this report and was a distinct point of discussion during the conference. The U.S. Cyber Command has been implementing and advocating such training programs at a very early level of education in hopes of incentivizing and training the next generation of cyber professionals for the private and public sectors.

While private sector collaboration is not off the table yet and while there seems to be an openness to cooperation with the private sector, it plays nowhere as central of a role now as it did in previous discussions or drafts. This could be an error at the risk of over-militarizing the nation’s cyber concerns. Not to be shortchanged, this discussion is further expanded in the final chapter.

With that said, the EO does not come without its flaws. There are more than a few, but one essential discussion missing here is the turn to adversaries – recognizing, identifying, and disrupting them.

Another consideration is that the new order may place too much of the ultimate responsibility for cyber oversight within the White House. This raises several questions and warrants deeper consideration on the pros and cons of such a move. Will this politicize cybersecurity issues? Will it ensure a cohesive strategy and standardize norms? Will it guarantee the uniform execution of priorities in cyberspace?

IT IS NOT ONLY CRUCIAL TO PATCH VULNERABILITIES AND BUILD CAPABILITIES FOR THE NEAR FUTURE; IT IS EQUALLY IMPERATIVE TO ENSURE RESILIENCE INTO THE FAR FUTURE. WHAT BETTER WAY TO DO SO THAN TO START REACHING THE NEXT GENERATION NOW?

Shifting from the Cyber Executive Order to the Budget Blueprint, one can see greater clarity, purpose, and alignment between President Trump's first federal budget and his emphatic demands for a better overall national cybersecurity strategy. Cybersecurity is a running theme in several sections – including in the introductory *Management* section on "making government work again." Intelligently, the plan recognizes cyberspace as the next frontier in defense, listing it side by side with the traditional domains of land, sea, air, and space. One can interpret much from where and how the cyber realm is couched. The issue appears numerous times – most obviously in connection with the Department of Defense (DoD) and the Department of Homeland Security (DHS). It is also reassuring to see it linked to the Department of Justice (DoJ), the Department of the Treasury (DoTr), and the National Aeronautics and Space Administration (NASA).

The greatest specificity is allowed in the DHS outline. The budget "[s]afeguards cyberspace with $1.5 billion for DHS activities that protect Federal networks and critical infrastructure from an attack. Through a suite of advanced cybersecurity tools and more assertive defense of Government networks, DHS would share more cybersecurity incident information with other Federal agencies and the private sector, leading to faster responses to cybersecurity attacks directed at Federal networks and critical infrastructure." With a drastically smaller allotment, but a similarly strong and specific assignment, "The FBI would devote resources toward its world-class cadre of special agents and intelligence analysts, as well as invest $61 million more to fight terrorism and combat foreign intelligence and cyber threats and address public safety and national security risks that result from malicious actors' use of encrypted products and services." Compared to the DHS request, this stands out as quite a hefty ask for pennies in the bank. Both are a step in the right direction, nonetheless.

What is spelled out is just as revealing as what is left out. There are several additional departments that should also be linked to cybersecurity, identifying the need for protection and defense in these areas. For instance, there is no mention of cybersecurity related to the Department of Energy (DoE) or the Department of Transportation (DoT) – both key to safeguarding critical infrastructure, insomuch as that remains a high-level national concern.

Another vital but absent point is the need for the protection of personnel records from cyber attacks such as hacking. The federal government was witness and victim to the lifting of millions of identities and records in the 2015 Office of Personnel Management (OPM) data breach. While such records now have more sophisticated encryption, the road should not end there in protecting the identities of the millions of Americans that dedicate their lives to public service. Personnel records are an imperative asset for the federal government to dutifully protect, but this responsibility is not addressed in the roadmap. In fact, cyber issues are generally framed mainly as some sort of large scale defense or attack scenario throughout the report – nudging readers and reviewers towards assumptions, instead of laying out definitions or specifying scope. Take that with a grain of salt, though. None of this is entirely unusual at the start of a new administration – when many policy areas will initially be unfamiliar territory.

On the topic of personnel, another essential point must be addressed here. It is becoming more urgent that the president focuses his immediate attention on identifying and appointing the right cyber visionaries and experts to office. While it is still quite early in the term, several senior positions for cybersecurity remain vacant. There have been no Trump appointments for the central positions of Federal Chief Information Officer and Federal Chief Information Security Officer, for example. For the moment, it seems these

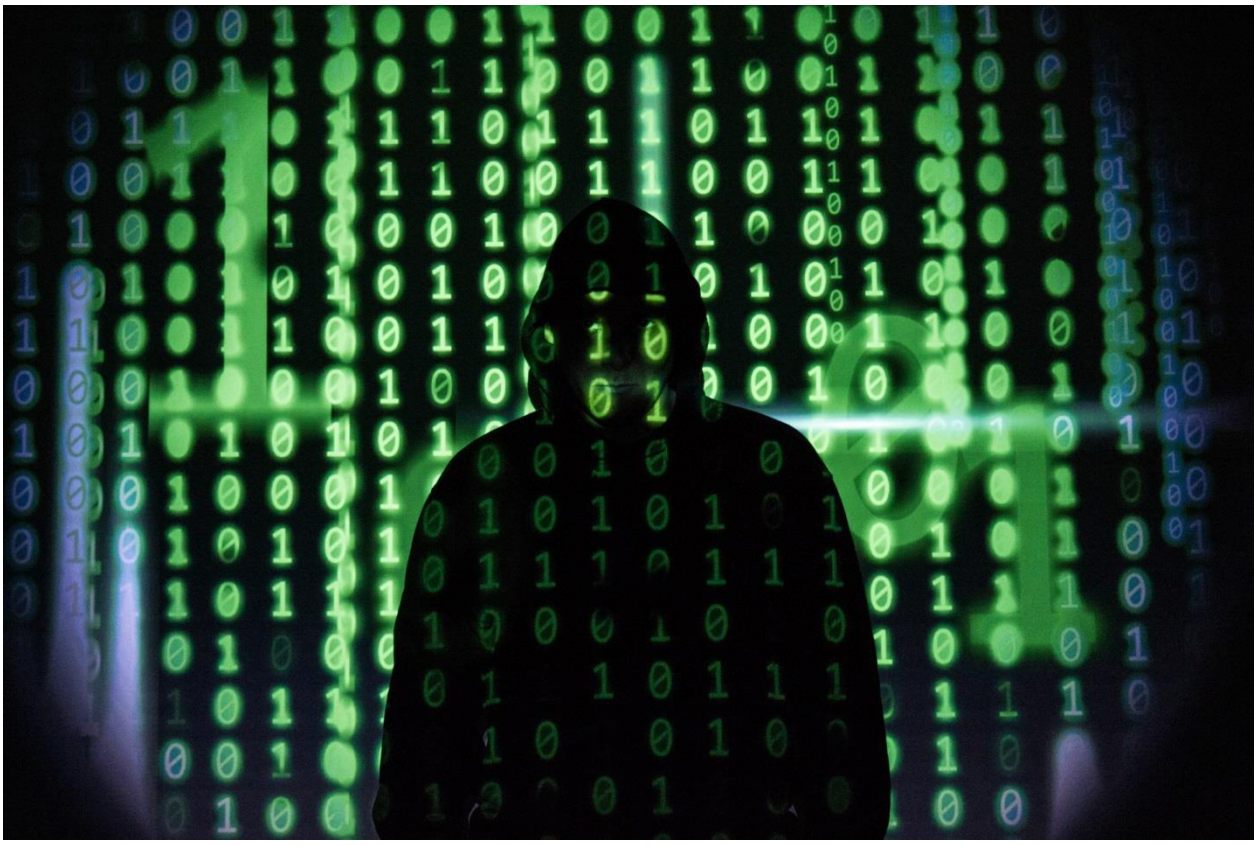
duties are being outsourced. Temporary external advisers can be helpful as the administration works to learn the lay of the land and pinpoint the best candidates for longer-term roles. There is, needless to say, a wealth of brilliant cyber experts that do not hold official titles. Ultimately, however, these roles need to be clarified and solidified instead of remaining ad hoc. Otherwise, the ambiguity could prove damaging down the road.

Clearly, the Executive Order and the Budget Blueprint prove that cybersecurity is on the new president's mind and his agenda. With any new term, the first budget is indicative of focus and direction – a game plan of sorts. It is thus reassuring that cybersecurity seems to be an issue the president is not taking lightly. Now it would be beneficial to see continued emphasis on the area. To begin, a few urgent measures must be prioritized:

- a study plan that brings the president and his cyber team up to speed on imminent issues and dangers;
- a framework that maps the critical ways cybersecurity ties into the many functions of government;
- the development of an overarching whole-of-government plan;
- the filling of official cyber-related roles, including operational and political appointments; and
- the implementation of the Executive Order that clarifies the building blocks and overall approach to America's cyber strategy.

A few crucial questions remain hanging in the balance: Is there any set protocol governing cyber decisions? What are the channels for decision-making? How can other, less obvious, branches and departments of government be involved? Who are the intergovernmental liaisons? What is the chain of command? Who are the influencers? The effects of such vacuums and loose organization are damning to strategy formation above all. A disjointed approach may be counterproductive in such a wide new arena of defense strategy with such far-reaching impacts on every level of national security. These are just a few pivotal starting points.

IV. The Evolving Cybersecurity Threat Landscape



With all that has transpired in the geopolitical cyber domain over the last several months – and even the last few years, the current presidential transition provides a unique window to reassess both the United States' cyber stance as well as its overall foreign policy leanings. First and foremost, cybersecurity must be couched in the overarching foreign policy agenda. It must be understood as a foreign policy tool. The relationship between U.S. foreign policy and cybersecurity is not only bidirectional; it is interdependent. A shift in America's foreign policy posture can have significant implications around the globe – in multiple regions, on multiple levels, in multiple dimensions. Now cybersecurity inarguably stands as one of these dimensions.

KNOWN THREATS HAVE SCALED MUCH FASTER THAN OUR ABILITY TO ACT ON THEM.

Within this context, a consequential question becomes: What does that mean with the new president's "America First" outlook? In which direction will the new administration tread – towards a multi-stakeholder system or towards an individualistic approach cast by the strongest nation-states? Trust has been the basis of the multi-stakeholder framework. However, trust has become an expensive commodity in light of all the recent cyber activity and targeting by various countries. This is especially true taking an external view from within the United States.

Thus the multi-stakeholder order may be at risk of being challenged by a more nationalistic emphasis. Needless to say, there are at least two views on which avenue is more advantageous to the U.S. overall. On the one hand, one does not have to be an

internationalist to fathom how a multi-stakeholder system could greatly benefit America in the long run. Within the current global order, it allows the U.S. to take the reins in shaping global norms and behavior. On the other hand, an individualistic or nationalistic approach offers the potential of shorter-term gratification. While a competitive security environment in this new domain of warfare may not offer longer-term stability; it may, in fact, allow swifter independent action in safeguarding one's own homeland from a variety of cyber offensives. These questions and considerations will be paramount for the administration to cogitate upon – not only as it shapes the broader U.S. posture in the world, but also as it defines its cyber strategies more explicitly.

CYBER ACTIVITY IS MERELY A TOOL – AN EXTENSION – OF THE DIFFERING FOREIGN POLICY AGENDAS OF DIFFERENT NATIONS.

The reality is we live in a glass house, but we have the nicest rocks. America's cyber defenses are yet underdeveloped, making the country somewhat vulnerable in its glass house. Inversely, the nation's offensive cyber capabilities are far more advanced – giving us the firepower of highly lethal rocks. Offensive cyber capabilities constitute an ever-growing cache of weapons. They can encompass everything from data breaches to intrusions on critical infrastructure. They can be tangible or intangible, targeting physical structures or invisible ones. Among their many utilities, they are especially useful in stealing or leaking data, breaking into systems, and obtaining access to sensitive information. This also adds an element of leverage to such attacks, wherein sometimes the threat of releasing sensitive data or state secrets can be enough to sway the victim towards the perpetrator's objectives. Thus, offensive operations are often employed as manipulation tactics, ranging from intimidation to blackmail. The U.S. arsenal of such capabilities runs deep and wide, strengthened by the secrecy of its uses, methods, and attacks.

America's lack of defensive cyber capabilities is not a new problem. It has been a prevailing issue since at least the 1980s. The reach is greater now, but the technique and tactics have not drastically changed. Known threats have scaled much faster than our ability to act on them. While there may always be an element of vulnerability in the cyber domain, American defenses have far from caught up to the changing global threat landscape. One of the reasons there has been insufficient emphasis on this area of defense is the lack of resources and funding. Perhaps the more fundamental problem, though, is the country's lack of perspective in properly understanding its main adversaries in this realm. The U.S. has continued to focus on critical infrastructure protection – namely physical systems such as electric grids. Meanwhile, the threats have evolved dramatically and vary from adversary to adversary. In fact, critical infrastructure may not often be an attractive target.

CYBER THREATS ARE ALL TOO OFTEN GENERALIZED INTO THE BLACK OR WHITE CATEGORIES OF CYBER CRIME OR CYBER WAR. SUCH AN OVERSIMPLIFICATION NOT ONLY DISTORTS THE TYPES OF THREATS THEMSELVES, BUT IT ALSO VASTLY MISSES THE NUANCES OF INTENT THAT PLAY A ROLE IN SHAPING HOW THREATS WILL MANIFEST OR METAMORPHOSIZE.

Therefore, a grave part of the problem is the misunderstanding and wrongful prioritization of threats. Yet again, this circles back to the underlying truth that cyber activity is merely a tool – an extension – of the differing foreign policy agendas of different nations. It is vital to unpack the overarching foreign policy postures of threat actors in order to gain a more lucid

view of their cyber intentions. Only then can the U.S. properly forecast and anticipate what form the corresponding threats emerging from each country will assume, in order to optimally prepare and defend against each of them.

In terms of understanding cyber threats on a macro level, a few nuances must be observed. Cyber threats are all too often generalized into the black or white categories of cyber crime or cyber war. Such an oversimplification not only distorts the types of threats themselves, but it also vastly misses the nuances of intent that play a role in shaping how threats will manifest or metamorphosize. Somewhere on the sliding scale, there are three gray areas holding enormous weight and factoring in intent: *cyber espionage* – which can be political or commercial in nature, always with an element of spying; *cyber subversion* – which often relies on the manipulation of information to have an undermining effect; and *cyber sabotage* – which generally involves a level of physical destruction with the goal of obstruction.

THE DISTURBING TRUTH IS THAT ALL THREE GRAY AREAS CAN ULTIMATELY BE ELEMENTS OF A GRANDER CYBER WARFARE SCENARIO. THE CYBER DOMAIN IS UNIQUELY DYNAMIC AND FLUID IN THAT SENSE. THIS IS PRECISELY WHY DEFENSES MUST BE RAMPED UP BUT REACTIONS MUST BE SLOWED DOWN. THINK TWICE; RETALIATE ONCE.

The last of these is easily the most damaging and severe. The United States has not yet suffered any crippling attacks in the form of cyber sabotage, which would perhaps fall the closest to an overt act of war as we know it. The gravity of this type of attack – particularly if perpetrated or sponsored by a nation-state – would be such a blatant violation that the chances of resisting a retaliatory attack of some sort would be infinitesimal. It is doubtful the American public would allow such an attack to go unanswered even if the government wished to show strategic restraint. It is not that such attacks have not occurred in recent times; just that they run a dangerous line when targeting a strong state such as the U.S. Weaker states have endured attacks of cyber sabotage without posing nearly as great a risk of retaliation. The 2015 sabotage of the Ukrainian power grid was traced back to IP addresses within Russia in 2015, but not much could be done in the way of a counterstrike. The disturbing truth is that all three gray areas can ultimately be elements of a grander cyber warfare scenario. The cyber domain is uniquely dynamic and fluid in that sense. This is precisely why defenses must be ramped up but reactions must be slowed down. Think twice; retaliate once.

BY MISUNDERSTANDING WHICH PLAYGROUND OUR ADVERSARIES ARE PLAYING ON, WE HAVE HANDICAPPED OURSELVES AND LIMITED OUR VANTAGE POINT. HAD WE BEEN MORE AWARE OF THIS, WE WOULD HAVE SEEN THAT THE RUSSIAN HACK OF THE U.S. ELECTIONS WAS ACTUALLY QUITE PREDICTABLE.

As a country, we do not have a cyber problem. We have a China problem; a North Korea problem; an Iran problem; a Russia problem. And cyber attacks will not be the only tool used to achieve our adversaries' goals.

Defensively, we have it all wrong. We have been destruction-focused, worrying about the protections in place for our physical and critical infrastructure. The Russians are on to something with their emphatic turn towards information warfare. Even the Chinese are more active in this realm. North Korea, too, has shown signs of leaning more towards info wars, as evidenced by the 2014 Sony Pictures Hack. By misunderstanding which playground our adversaries are playing on, we have handicapped ourselves and limited our vantage

point. Had we been more cognizant of this, we would have seen that the Russian hack of the U.S. elections was actually quite unsurprising. Did we learn nothing from Russia's test drive of similar tactics with the Ukraine elections? We have been ignoring the smoke signals for too long. But we can no longer afford to do so.

THIS INHERENTLY LEADS US BACK TO THE MOST ELEMENTARY QUESTION – ONE THAT LIES AT THE VERY ROOT OF FOREIGN POLICYMAKING SINCE THE BEGINNING OF TIME: WHO ARE OUR MOST DANGEROUS ADVERSARIES? TODAY, NO LIST WOULD BE COMPLETE WITHOUT AN EXAMINATION OF CHINA AS A COMPETITOR; NORTH KOREA AS AN INSTIGATOR; IRAN AS A CHALLENGER; AND RUSSIA AS AN OPPONENT.

Ultimately, we must frame the cyber debate within the larger foreign policy debate. This inherently leads us back to the most elementary question – one that lies at the very root of foreign policymaking since the beginning of time: Who are our most dangerous adversaries? As far as nation-states go, the list is fairly straightforward in the present era – though the sequence of the list may well be cause for debate. Today, no list would be complete without an examination of China as a competitor; North Korea as an instigator; Iran as a challenger; and Russia as an opponent.

The China Problem

Just as China is a U.S. competitor in the conventional domains of land, sea, air, and space, so too is it a competitor in cyberspace. While there are certainly some military concerns with China in the Asia-Pacific region, tensions in the larger international arena tend to be more of an economic and political nature. This is not to say that one cannot bleed into the other very easily, but Beijing remains careful in its direct provocations of Washington. China's global ambitions for economic and political dominance frame its cyber battles with America.

CHINA'S GLOBAL AMBITIONS FOR ECONOMIC AND POLITICAL DOMINANCE FRAME ITS CYBER BATTLES WITH AMERICA.

Extending these motives from conventional to unconventional tools of statecraft, it makes sense that China has displayed a growing fondness for cyber espionage in recent years – particularly related to economic interests. The FBI has investigated countless cases of alleged Chinese sponsorship or state action within U.S. jurisdiction. Chinese cyber espionage habitually seems to target American corporations, with distinct commercial and competitive interests. Notable instances include Chinese involvement in cyber spying cases with United States Steel Corporation, Westinghouse Electric Co., Alcoa Inc., Allegheny Technologies Inc., and even The Boeing Company. While cyber espionage can be quite disruptive to economic security and competitive advantage – with the theft of intellectual property and trade secrets, such attacks likely will not invite the wrath of the entire American defense system. Such

economic cyber espionage thus seems to offer a slightly safer bet for competitors like China – as far as calculated risks go.

For years, Washington has stood by quietly – hesitating to attribute many attacks to Beijing in sharp terms, at least publicly. Instead, private warnings were the preferred mechanism – to very little avail. Finally frustrated by the onslaught of such Chinese activity on American soil or against American entities, the DoJ took decisive measures in May 2014 by indicting five officers of the People's Liberation Army (PLA) – the Chinese military. The five were charged with hacking major American corporations or subsidiaries – particularly in the industrial sector, including Alcoa Inc. (a leading aluminum producer), Westinghouse Electric Co. (a prominent nuclear power producer), Allegheny Technologies Inc. (an alloys and metals supplier), SolarWorld Industries America Inc. (a solar technology company), and U.S. Steel (the country's oldest steel manufacturer). The DoJ was convinced that Beijing was after critical data that would enable Chinese corporations to be more competitive with its materials exports into the U.S. This series of operations allegedly covered data breaches of everything from trade secrets and technology blueprints to internal corporate strategy and import/export plans. These were not isolated instances of China's incursions into the intellectual property of American companies for economic gain. They just so happened to be the instances that the courts made an example of. In fact, the indictment itself claims that China's government has been supporting or sponsoring such intrusive espionage since at least 2006.

Nevertheless, this magnetism towards economically advantageous cyber attacks has not been mutually exclusive from the translation of traditional espionage into cyber activity. State secrets and personnel information remain strategic targets for Beijing. This cements the thievery of inside information from the U.S. government as a focal part of China's agenda – especially as a rising power directly challenging U.S. dominance. In April 2015, a security engineer at the Office of Personnel Management unearthed a shocking data breach during a routine check on the office's digital network. The engineer detected an uncharacteristic pattern of data flowing out of OPM to an unaffiliated domain name: www.opmsecurity.org. Further investigation led to the discovery of well-concealed malware that circuitously enabled a hacker to remotely access OPM's servers and the millions of personnel records they stored.

Initial reports wrongly estimated that the infiltration was limited to just 4 million files – still a jarring number. It was later confirmed that the numbers and the impact were abundantly higher. The personal data of nearly 22 million government employees was hacked, and the fingerprints of nearly 6 million of those were exposed. Though only ten or so computers were corrupted with malware, some of these were integral components of the entire OPM network. One that was particularly hazardous was the "jumpbox" – the administrative server with access to all of the other servers. Thus, mountains of sensitive information were obtained. Data from background investigations and security clearance applications was compromised. Social security numbers were taken. Spousal and family information was accessed. Sealed drug and criminal records were opened. But one of the most tangible consequences was also one of the least foreseeable. Since the cyber incursion included vast records of an array of different levels and types of staff across the government, it was now possible to distinguish cover identities from real staff assignments. This meant it was now possible to deduce the identities of U.S. intelligence operatives, agents, and spies working undercover around the world. Such revelations could damage foreign relations, hinder mobility, limit entry and exit access in the form of visas and permits, and drastically decelerate or even retrogress covert operations. Above all, it could pose a direct and immediate danger to these brave men and

women carrying out their missions. Wisely, entities within the U.S. intelligence community recalled several of their operatives working on foreign soil in the wake of the cyber intrusion that may have potentially imperiled their identities.

STRATEGIC AND POLICY LEVEL REFLECTIONS ARE INDISPENSABLE IN THE AFTERMATH OF SUCH A CYBER CAMPAIGN. THESE DELIBERATIONS MUST WRESTLE WITH SOME INESCAPABLE QUESTIONS OF GREAT GRAVITY: WHAT OTHER UNANTICIPATED TARGETS ARE POTENTIALLY BEING EYED BY FOREIGN ACTORS? HOW COULD THREAT SCENARIO ANALYSIS BETTER ENCOMPASS SUCH LESS CONVENTIONAL OR EXPECTED TARGETS? HOW COULD THREAT DETECTION BECOME MORE AIRTIGHT?

As a matter of course, U.S. officials and President Obama were all reticent about attribution. Citing diplomatic sensitivity, there was a characteristic hesitation to admonish a state actor at first. There was no public announcement by the White House. There was no public accusation. There was no public punishment. No example was made of China. In fact, in the last days of the Obama presidency, ABC News' White House Correspondent grilled the Press Secretary about the lack of public response following the OPM hack. The Press Secretary confirmed "that there was no public announcement about our response," but kept reverting to the fact that he could not "speak to what response may have been initiated in private."

On the very face of it, this was a rather perspicacious attack. Beijing likely had a sense of President Obama's hesitation to rock the boat with attribution. This likely lowered the risk calculus and made the hack more appealing. Moreover, the choice of target itself was shrewd. At the time, the Office of Personnel Management would not likely be categorized as a high value target. So, no one saw the attack coming. There was no preparedness plan; no heightened encryption. There were no countermeasures; no safeguards in place. After all, who would want to steal the files on a random assortment of staffers in various government offices? A patient and strategic adversary, that's who. In actuality, OPM does have to ward off hacks more frequently than one would think. However, they have generally been smaller scale attempts that are rather common for any large digital network. This was a different ball game altogether.

Unquestionably, strategic and policy level reflections are indispensable in the aftermath of such a cyber campaign. These deliberations must wrestle with some inescapable questions of great gravity: Why were personnel records not deemed vital enough to be better guarded? How was the Office of Personnel Management overlooked as a target? What other unanticipated targets were potentially being eyed by foreign actors? How could threat scenario analysis better encompass such less conventional or expected targets? How could threat detection become more airtight? But those are not the only questions to be answered and those are not the only thought exercises that matter. The technical conversations would be just as crucial. After all, the technical safeguards are the real barriers to such intrusions. For example, in this and other instances, an easy roadblock would have been the use of multi-factor authentication. Not to be conflated with two-step verification, multi-factor authentication is a heightened mechanism for enhanced security whereby system access is granted only after users prove their identities in multiple ways – frequently requiring the physical insertion of a unique chip card.

OPM has indeed invested time and resources towards improving its cybersecurity since June 2015, beginning with an articulation of fifteen

new measures for modernizing systems, protecting identities, and instituting better cyber practices across the board. It also made information and tools for recourse available to anyone directly or indirectly affected by the data theft. Within OPM and throughout the federal government, all these important discussions happened after the OPM hack; it is a shame they did not happen before. That is the true significance of the OPM attack: its unforeseeable nature irreversibly changed the direction of strategic and policy thinking as well as technical rationale. There is now a growing understanding that in cyberspace, nothing is off limits except that which is offline.

THAT IS THE TRUE SIGNIFICANCE OF THE OPM ATTACK: ITS UNFORESEEABLE NATURE IRREVERSIBLY CHANGED THE DIRECTION OF STRATEGIC AND POLICY THINKING AS WELL AS TECHNICAL RATIONALE. THERE IS NOW A GROWING UNDERSTANDING THAT IN CYBERSPACE, NOTHING IS OFF LIMITS EXCEPT THAT WHICH IS OFFLINE.

A few months after this hack and a little over one year after the DoJ indictments, in September 2015, President Barack Obama and President Xi Jinping announced the U.S.-China Cyber Agreement – the first of its kind. The majority of the mutually accepted conditions align with two main principles: to intensify cyber cooperation and to curtail cyber provocations. The White House released an official communiqué summarizing some of the core tenets of the agreement. Promising language detailed that neither government would conduct or allow cyber espionage or cyber theft geared towards gaining a competitive advantage commercially – with an emphasis on intellectual property, including trade secrets. While this was a noteworthy step in the right direction, it is somewhat concerning that the language on curbing offensive cyber activity seems to have been so narrowly crafted and limited to only the commercial sector. Does this mean China has a ready loophole when conducting other types of cyber espionage against or within America – if it targets the public sector or government instead of the commercial sector or corporations?

Aspects of proposed cooperation are articulated in greater detail. Both countries will "mitigate malicious cyber activity emanating from their territory." They will respond to each other's requests for information and assistance in a prompt and reasonable manner. The governments will cooperate in fulfilling requests to investigate cybercrimes including the collection and sharing of evidence – within the confines of their national laws, needless to say.

Marking the long-term nature of the cooperative agreement, China and America additionally decided to work together on global standards "to further identify and promote appropriate norms of state behavior in cyberspace within the international community." To implement all of this, the two committed to maintaining an ongoing joint dialogue for further discussions and regular bilateral meetings. For this, each nation was to designate certain high-level defense, intelligence, and foreign affairs officials as part of their respective teams.

"THERE IS NO NATIONAL SECURITY WITHOUT CYBERSECURITY." –PRESIDENT XI JINPING

Cyber relations with Beijing have been positively affected since the agreement. Still, much distance remains to be bridged between the two powers. The differences in their core principles and ideologies pose several obstacles. Washington will not follow in Beijing's footsteps with the government's obsessive control over information disseminated or even allowed into view for its citizens. China has essentially

created such a tight gridlock of information control within the country that analysts have even coined a term for it: The Great Firewall of China. This path should certainly not be a model for the U.S. Au contraire, information freedom is a key principle and value of Western civilization, particularly in America. Nevertheless, there is one thing America could do well to learn from China's President Xi Jinping as cooperation continues: "There is no national security without cybersecurity."

The North Korea Problem

This work, "Electric North Korea" by Simran R. Maker is a derivative of "Korea North Korea War" by Gerd Altmann, used under CC0 1.0 Universal.

The North Korean cyber threat must be framed by the constrictions of Pyongyang's current reality – which is less fluid than with any other threat actor. Because of its place on the global stage, because of its limited international ties, because of its own vulnerability, the North Korean regime treads carefully – but not necessarily lightly – in cyberspace. Yet, this new domain has opened up a realm of offense that the regime recognizes to be advantageous to its unique quandaries. Conventional warfare is a difficult domain, as the world would not sit idly by. Nuclear development has been advancing swiftly in accordance with the stated goals of the Kim Jong-un regime, continuing the trajectory of his predecessors. Nonetheless, developing nuclear weapons is one thing; employing them is wholly another. If he is a rational actor, Kim Jong-un must be fully aware of the self-threatening risk to ever actually launching a first strike against any Western countries directly. Thus, this avenue of offense and deterrence seems to be more survival insurance – at least rationally speaking.

CYBERSPACE OFFERS THE COVER OF DARKNESS FOR LIMITED OPERATIONS, AND HAS THUS BECOME AN INCREASINGLY ATTRACTIVE ARENA FOR NORTH KOREAN FOUL PLAY. GIVEN THE GEOPOLITICAL CONSTRAINTS ON OTHER DOMAINS OF NORTH KOREAN ACTIVITY – MILITARY, ECONOMIC, POLITICAL – THE NATION HAS BEEN FORCED TO RESORT TO ASYMMETRIC STRATEGIES AND OPERATIONS.

Cyberspace, however, offers the cover of darkness for limited operations, and has thus become an increasingly attractive arena for North Korean foul play. Within the present framework, one must internalize two critical truths that inherently guide the regime's cyber activities. First, given the geopolitical restraints on other domains of North Korean activity – military, economic, political – the nation has been forced to resort to asymmetric strategies and operations. This, of course, fits perfectly with the dynamics of weaker actors facing stronger states as adversaries. Second, due to

the suffocating fears of retaliation – ranging from direct military confrontation to economic sanctions, most of the nation's cyber attacks are never claimed publicly. This enables the regime to conduct attacks in a somewhat safer space, with the added advantage of difficult attribution in many cases. This is not to say Kim Jong-un is not capable of commanding more lethal cyber attacks. In fact, the more recent attacks signal growing cyber reach and capabilities.

Within this 'tread carefully' model, the country has more often than not stuck to operations targeting its sworn enemy and neighbor, South Korea. In more recent years, nonetheless, the regime has more boldly ventured to conduct disruptive attacks against what it views as South Korea's prime protector: America. It is worth noting, however, that as attacks against South Korea have been drastically ramped up in recent times, attacks against America have not followed such a straight line upwards – perhaps, again, due to a fear of retaliation from the current global superpower.

Consider the upward trajectory in the impact of attacks on South Korea from 2013 to 2017. While the North has and will always continue to deny responsibility for cyber attacks, the March 2013 Dark Seoul instance is nearly undeniable. The media and banking sectors were hacked and infected with malware linked to a remote access tool. The hard drives of thousands of computers were wiped simultaneously, while servers were blocked and networks went down. The impact was detrimental, but not necessarily lethal, to media, banking, and financial operations – specifically at two major media outlets and three major banks. The attack may have been routed through IP addresses in China, to make attribution and detection less straightforward. Yet, the level of sophistication pointed to a government-sanctioned mission, rather than a lone hacker. Moreover, some of the targets had been explicitly threatened by Kim Jong-un in prior statements. The accompanying on-screen messages – images of a skull and a warning that this was the beginning of a movement – were thought to further support these allegations. Eventually, Seoul released its findings: "An analysis of cyber terror access logs, malicious code, and North Korean intelligence showed that the attack methods were similar to those used by the North's Reconnaissance General Bureau, which has led hacking attacks against South Korea." The Ministry of Science provided further evidence that, it believed, was strongly indicative of an attack perpetrated by Pyongyang.

Similar, but less sophisticated attacks had been conducted in previous years – notably in 2009, and again against the banking sector in 2011, according to investigations by the leading security software developer McAfee Inc. The trajectory was observably moving upwards. Most recently, the trend has been further solidified and targets have been further expanded with the 2017 attack on organizations in 31 different countries. The cyber security firm, Symantec, disclosed that its investigations uncovered digital evidence of malware and corrupting software remotely installed on computers around the world. Symantec is "reasonably certain" that a North Korean hacking group, Lazarus, is behind the attack. Those close to the inquiry have noted that "this represents a significant escalation of the threat" and an indication of the advancing sophistication of Pyongyang's cyber capabilities. As the investigation is still under way due to the recency of the attack, few details on targeted organizations or tactics are available at the moment. In typical fashion, Pyongyang denies any involvement. The FBI is still in the process of following leads and conducting a thorough inquest before providing any comment. Nonetheless, if such an attack was in fact perpetrated by North Korea, it reveals a strikingly intensified cyber campaign – in breadth and in depth.

Lazarus has emerged as a North Korean cybercrime outfit worth paying special attention

to. They have been implied in several attacks against South Korea, including many of the denial of service (DDoS) attacks and much of the cyber espionage since 2009. These same cyber criminals stepped up their game and launched a wiper attack against Sony Pictures in America – essentially wiping the data from thousands of hard disks after the theft of sensitive information. At the time, and for this particular case – perhaps to create a degree of separation and confusion – the group called itself the Guardians of Peace, ironically abbreviated as the "GOP". In one of the worst data breaches in corporate history, the unit hacked its way to accessing closely guarded inside information. The stolen data included intellectual property such as unreleased films and scripts, privileged communications such as executive level email exchanges, protected personnel information such as account data, usernames, and passwords, as well as personnel records such as employment details for thousands of Sony employees. Much of the acquired data was leaked or released to the public – though not all of it – causing irreparable harm to an industry leader like Sony.

WHAT MAKES THE SONY PICTURES HACK SO CENTRAL TO AMERICAN INTERESTS IS THE SUSPECTED MOTIVE. IT DID NOT TAKE MUCH READING BETWEEN THE LINES TO INTERPRET THE ATTACK AS ONE AGAINST A CORE VALUE OF AMERICAN IDEOLOGY: THE FREEDOM OF SPEECH.

Shaken by the reach of such state-sponsored cyber operations, an advanced cyber analytics firm (Novetta) formed a coalition with private industry partners to study the Sony case in greater depth. The project, Operation Blockbuster, aimed to better understand the group and the attack – from targeting to tactics, techniques, and procedures. In meeting these goals, the Novetta-led project has already proven valuable. The firm released its findings in a detailed technical report in February 2016. The case study encourages others to implement further protections to safeguard valuable proprietary information and trade secrets.

"THE WHOLE WORLD IS WATCHING HOW WE AS A NATION RESPOND. AND IF WE DON'T ACKNOWLEDGE THIS, IF WE DON'T NAME NAMES HERE, IT WILL ONLY ENCOURAGE OTHERS TO DECIDE 'WELL, THIS MUST NOT BE A RED LINE FOR THE UNITED STATES. THIS MUST BE SOMETHING THEY'RE COMFORTABLE WITH AND WILLING TO ACCEPT." –ADMIRAL MICHAEL ROGERS

Aside from the economic or privacy implications, and aside from the reach of the attack itself, what makes the Sony Pictures hack so central to American interests is the suspected motive. The attack took place within the context of the controversial upcoming release of the Sony film "The Interview" – a political satire about a journalistic duo recruited to assassinate Kim Jong-un during an interview, a storyline that he certainly felt was menacing to the security of the regime. In the months prior to the release of the movie, Kim Jong-un took some bold steps on the public stage. He not only called it a "wanton act of terror" and blamed President Obama for the ploy to encourage such plots; he also overtly threatened retaliation – even war – if the film ever saw the light of day. Thus, he saw Sony's announcements of the movie's release as an act of direct defiance and provocation, justifying the Sony hack as a short-of-war attack. On this side of the world, however, it did not take much reading between the lines to interpret the attack as one against a core value of American ideology: the freedom of speech.

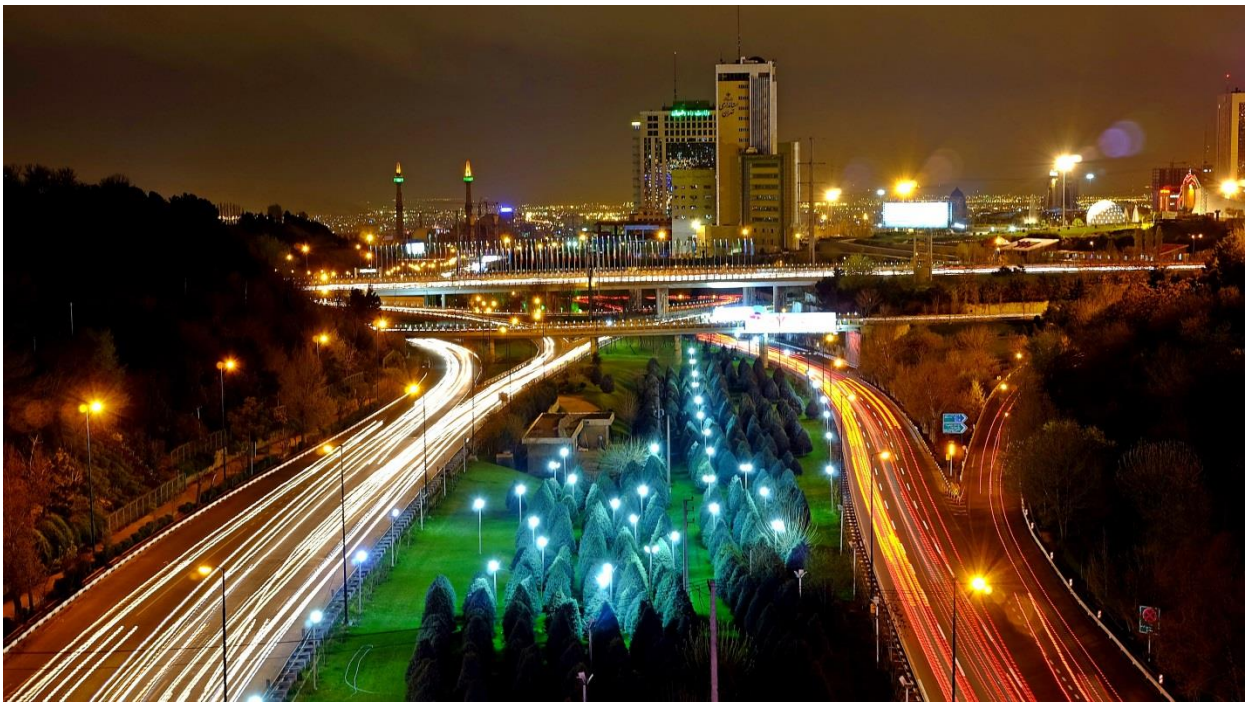
Initially, the American attribution problem reared its head again. The government followed its tendency not to overblow the problem publicly, and resorted to private scoldings. Sony – temporarily crippled from the breach and inclined to take threats of additional attacks seriously – postponed the movie's release. It was this act of seemingly succumbing to Pyongyang's intent to suppress free speech that was the final tipping point for President Obama. In a change of course, he garnered support for unprecedented countermeasures and a much stronger reaction than with any previous state-sponsored cyber intrusion. That same week, Obama also publicly named and shamed the North Korean regime for attempting to trample on deeply valued Western principles.

ALL IN ALL, THE TREATMENT OF THE SONY ATTACK ULTIMATELY SET A SOLID EXAMPLE – DESPITE THE CIRCUITOUS PATH TO THAT END. FUTURE ADMINISTRATIONS COULD BENEFIT FROM TAKING A PAGE OUT OF THAT BOOK. DETERRENCE IS NOT A CHAPTER TO BE TAKEN LIGHTLY.

While many senior officials in the Obama administration recounted the debate over attribution, it was an important example to set for future deterrence. Recognizing this, Admiral Michael Rogers (then head of the National Security Agency) recalled: "The argument I made was the whole world is watching how we as a nation respond […] And if we don't acknowledge this, if we don't name names here, it will only – I'm concerned – encourage others to decide 'Well, this must not be a red line for the United States. This must be something they're comfortable [with] and willing to accept.'" Obama's public statements were not his only way of showing Kim Jong-un this was not the case. He also promptly signed an executive order authorizing additional sanctions on North Korean officials and entities as the first step, leaving room for additional steps as necessary.

There were suspicions of subsequent U.S.-led covert acts against North Korea – such as internet shutdowns, but they were not publicly acknowledged by the administration. All in all, the treatment of the Sony attack ultimately set a solid example – despite the circuitous path to that end. Future administrations could benefit from taking a page out of that book. Deterrence is not a chapter to be taken lightly.

The Iran Problem



Iran has been acutely aware of the dormant potential in weaponizing cyberspace since at least the early 2000s – both, aware of the offensive potential against external actors and the defensive potential in protecting its own systems or suppressing dissident activity. Governmental bodies were formed as early as 2002 and 2003 to deal with issues related to online systems and technologies. The Committee to Prescribe Measures against Prohibited Internet Bases was formed in 2002 as a suppression tool, initially focused on blacklisting websites and filtering content. An early iteration of a cyber policy arm was established in 2003 – then known as the Supreme Council for Information Sharing Security. By 2005, the Supreme Council for Technological Innovation was founded and tasked with strategic policymaking, particularly for technological advancement. Despite being early to recognize the weight cyberspace would hold in the future, Iran's cyber institutions largely concentrated on censorship and suppression in those early years.

Today is a completely different story. Within a few short years, Iran's cyber arms became better organized, structured, and consolidated. Capabilities were widened beyond suppressive measures, to include divisions of highly trained cyber warriors to carry out offense. Separate programs centered on cyber defense have also been enhanced. Now, Iran's cyber operations fall under two divergent chains of command, thus taking shape differently from each other at times. First, there are cyber divisions and actors under the command of the Iranian Revolutionary Guard Corps (IRGC) – which includes Iran's elite cyber forces. Second, there are operations not directly under the government's command, but supported by it and carried out by groups like Hezbollah. The line between the two is still a line in the sand, nevertheless – making distinct attribution or verification a very gray area.

Tehran has been quick to learn and adapt, not slow to react to perceived threats or consequential global events. Though not the

only ones, two influential phenomena did directly trigger decision-makers to ramp up cyber programs: the movements emerging from the 2009 elections in Iran and the Arab Spring uprisings across the Middle East. Such events only amplified the centrality of cyberspace to Iranian leaders' national security calculus.

IRAN HAS BEEN ACUTELY AWARE OF THE DORMANT POTENTIAL IN WEAPONIZING CYBERSPACE SINE AT LEAST THE EARLY 2000S – BOTH, AWARE OF THE OFFENSIVE POTENTIAL AGAINST EXTERNAL ACTORS AND THE DEFENSIVE POTENTIAL IN PROTECTING ITS OWN SYSTEMS OR SUPPRESSING DISSIDENT ACTIVITY.

Put in the works immediately following these events, Ayatollah Khamenei soon announced the foundation of what would become the highest decision-making cyber division within the IRGC, the Supreme Cyberspace Council. Fully operational by 2012, it was to have oversight of all other cyber branches and ensure that a cohesive cyber strategy be observed throughout. The level of structure and the emphasis on a single integrated strategy together validate the clarity and specificity with which the nation shapes and shifts its cyber objectives.

As Tehran's cyber strategy has taken shape with greater definition in Tehran, the name of the game has become disruption and destruction. Unlike threat actors such as China, the commercial sector is not central to Iran's cyber intentions. Where corporations have been targeted, the motive seems to have been retaliatory or punitive for the most part. The February 2014 Yellowstone 1 attack on Las Vegas Sands Corporation is a case in point. On the heels of aggressive comments by CEO Sheldon Adelson – advocating that America drop a nuclear bomb in Iran to push back on its nuclear development – his company's operations were brought to a standstill by hackers linked to Iran. Hundreds of computers and servers critical to the operations of the gaming company were shut down; many were wiped clean. Telecommunications were interrupted so that phones stopped working. To note, not a penny was stolen. The chaos that ensued and the consequential financial costs to the American giant were enough to satisfy the perpetrators. This was an act of revenge, if not an attempt to punish and silence such inflammatory rhetoric against the regime. An earlier example shows continuity in the motive trend. From 2011 to 2012, the systems of three major American banks were repeatedly hacked – at JPMorgan Chase, Citigroup, and Bank of America. Analysts closely studying the attacks reported evidence suggesting these banks were chosen for their role in enforcing sanctions against Iran. The operations utilized DDoS attacks to flood the banks' networks with incoming web traffic, thus crippling their functionality – though not irreparably. There was no conclusive attribution – at least not publicly – following the series of attacks, but available data links the campaign to Iranian operatives or supporters.

AS TEHRAN'S CYBER STRATEGY HAS TAKEN SHAPE WITH GREATER DEFINITION, THE NAME OF THE GAME HAS BECOME DISRUPTION AND DESTRUCTION.

Such attacks are not always the standard modus operandi for Iran though. Tehran prefers cyber espionage and subversion to achieve its political ends. Along the same lines – and again distinguishing it from other threat actors – Tehran remains interested in sabotage and attacks on critical infrastructure. Expectably so, information warfare is also an integral part of the nation's cyber ploys – materializing in the theft of information and the spread of propaganda. All of this again points to the

manner in which cyber activity usually manifests as an extension of broader geopolitical realities – molded by both obstacles and objectives. This truth circles back to the fact that in order to better understand a country's potential cyber threats, its activities in this domain must be couched within a wider view of its overall foreign policy agenda. Like other states seeking to gain standing in the international order or assert a degree of regional power, Iran has turned to cyber offense as an extension of its doctrine of asymmetric warfare. It is not, in fact, an unfathomable derivation from other manifestations of such a strategy – ones that the country has historically relied on, such as the state-sponsoring of terrorism or the utilization of guerilla warfare.

LIKE OTHER STATES SEEKING TO GAIN STANDING IN THE INTERNATIONAL ORDER OR ASSERT A DEGREE OF REGIONAL POWER, IRAN HAS TURNED TO CYBER OFFENSE AS AN EXTENSION OF ITS DOCTRINE OF ASYMMETRIC WARFARE.

In general, the swift and intricate advancement of Iran's cyber programs suggests a certain anxiety about foreign threats – to which Iran's systems have been no stranger. Tehran seems particularly preoccupied with threats to its survival and endurance, but it is also concerned about challenges to its participation in the international order as the rising power it views itself as. As such, thorough contingencies have been implemented to defend against everything from attacks like Operation Olympic Games (or Stuxnet, as it is colloquially called), down to attacks that attempted to penetrate critical information via viruses like Duqu.

Iran is a foreign threat in its own right, nevertheless. The 2012 Saudi Aramco operation was dubbed the worst cyber attack the world had seen. Aramco is one of the world's oil and petrochemical giants, with customers in every corner of the world. The target was ripe; the virus was ready. In a wiper operation, 35,000 computers were infected with the Shamoon malware that wiped and destroyed the data and the systems. With the click of one cleverly disguised phishing link, a multitrillion dollar business was sent back to the dark ages. Essential operations – such as shipping, payments, contracts, fulfillment, and communication – were slowed to a halting pace. The entire IT infrastructure was essentially annihilated and rendered dysfunctional. Two weeks in, Aramco succumbed to distributing oil at no cost just to keep the barrels moving. It took five months for the company to finally come back online as fully operational. Immediately following the attack, a group identifying itself as the Cutting Sword of Justice claimed responsibility and cited Aramco's support of the Saudi royal family – and the regime's "crimes and atrocities" – as the reason it was targeted. There was consensus among intelligence analysts that this was an Iran-led operation. The world had been hit with a wake-up call, and the phone was not about to stop ringing.

THE SWIFT AND INTRICATE ADVANCEMENT OF IRAN'S CYBER PROGRAMS SUGGESTS A CERTAIN ANXIETY ABOUT FOREIGN THREATS – TO WHICH IRAN'S SYSTEMS HAVE BEEN NO STRANGER.

As conventional warfare between Israel and Iran has persisted – often in the form of proxy wars such as the Gaza conflict, Iran has endeavored to widen its offense and deepen its impact with cyber attacks against Israel. Exploiting the diversion of Israeli forces fighting Hamas, hackers have recurrently staged a series of cyber attacks on Israeli websites. Officials of the Israel Defense Forces (IDF) have somewhat downplayed the infiltrations as failed attempts; instead emphasizing the successful rate of deflection and prevention. During Operation

Protective Edge – the July 2014 campaign in Gaza – Israel reported an unprecedented rise in cyber activity. Some of these were simply distracting DDoS attacks on non-crucial websites; others led to leaked databases and personnel information to benefit Hamas. The IDF's cyber defense experts claim to have efficiently and effectively thwarted the attacks, but they were still caught off guard by the rapid intensification of capabilities that they attributed to Iran and Iran-sponsored hackers. Colonel N, the head of the cyber division, remarked that "[W]e saw attacks on a greater scale and on a more sophisticated level. A significant amount of thought and investment stood behind the attacks we saw." It was not just the sophistication, but the volume and coordination of the attacks that really tested his unit, he admitted. Iran had arrived in cyberspace. And it was willing and ready to take on its enemies – at least the near ones.

By March 2016, Iran's cyber warriors had further stepped up their game. A small dam just outside of New York City was hacked to be remotely controlled – perhaps as a demonstration of capabilities or a show of force. This particular cyber encroachment did not lead to any sort of catastrophic damage, but it did regenerate concerns about larger scale operations aimed at America's critical infrastructure. Senator Charles Schumer took the scare very seriously, interpreting the message in no vague terms: "They were saying that we can damage, seriously damage, our critical infrastructure and put the lives and property of people at risk." The dam attack prompted the DoJ to unseal an indictment for seven Iranians facing other cyber charges from 2011 to 2013. Further, Assistant Attorney General John Carlin publicly made the attribution to Iran: "We can tell the world that hackers affiliated with the Iranian government attacked U.S. systems, and we seek to bring them to justice for their crimes." He also disclosed prior instances of cyber targeting against the New York Stock Exchange and other important American institutions.

PERPETRATORS MUST BE MADE FULLY AWARE THAT THE UNITED STATES CAN TRACE SUCH CYBER TRANSGRESSIONS BACK TO THEM, AND IS PREPARED TO DEFEND ITS INFORMATION, INSTITUTIONS, AND INFRASTRUCTURE AGAINST FOREIGN OFFENSIVES.

Other than such sabotage efforts, the U.S. government has reported IRGC attempts to infiltrate government agency communications, including within the Obama administration. Such espionage has not typically been made a public spectacle, but perhaps keeping it quiet accomplishes nothing if more overt physical operations are still plotted. Moreover, Ayatollah Khamenei has not been shy to warn America about attacks against its critical infrastructure. In response, the willingness to make direct attributions in no uncertain terms is crucial. Perpetrators must be made fully aware that the United States can trace such cyber transgressions back to them, and is prepared to defend its information, institutions, and infrastructure against foreign offensives. At the end of the day, a cyber attack is still an act of war.

The Russia Problem

Of the foremost threat actors the United States faces, Russia is arguably the most actively engaged. This naturally aligns with Russia being one of the greatest U.S. challengers still today. Its foreign policy agenda frequently considers U.S. counterstrategies and countermoves. It makes sense, then, that Russia would behave similarly in the cyber domain, seeing it as an opportunistic arena for directly challenging the United States. What makes Russia's cyber campaigns unique is not just its arduously sustained efforts against America, but its choice of weapons and tactics. Moscow's simple strategy of information warfare has proven highly effective – particularly as Washington's detection and prevention networks often turn to focus on the nation's hard targets. The Cold War adversary has taken notice and taken advantage of the inadequate resources that the U.S. has devoted to the dominion of information warfare, both offensively and defensively. Some experts – especially those that have been acutely watching and analyzing the global cyber threat landscape – contend that information warfare is the most significant and most immediate hazard for the U.S. The real threat does not lie in the hack itself; it lies in the consequences of leaked information. In the view of these analysts, infrastructure can be fixed and sealed; information leaks cannot. Washington does not invest enough in this realm; it overemphasizes averting physical destruction at the cost of forestalling ideological disruption.

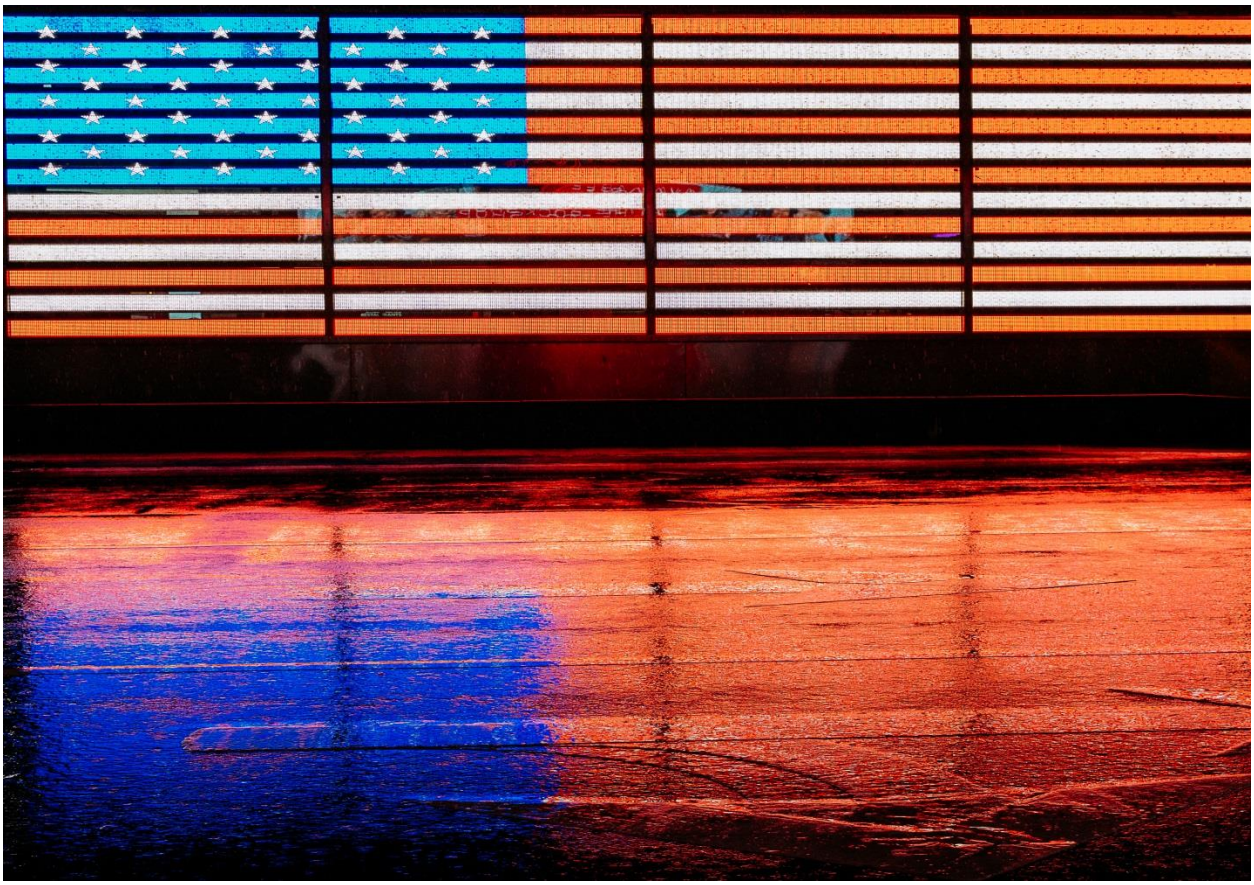
INFORMATION WARFARE IS THE MOST SIGNIFICANT AND MOST IMMEDIATE HAZARD FOR THE U.S. THE REAL THREAT DOES NOT LIE IN THE HACK ITSELF; IT LIES IN THE CONSEQUENCES OF LEAKED INFORMATION. INFRASTRUCTURE CAN BE FIXED AND SEALED; INFORMATION LEAKS CANNOT. WASHINGTON DOES NOT INVEST ENOUGH IN THIS REALM; IT OVEREMPHASIZES AVERTING PHYSICAL DESTRUCTION AT THE COST OF FORESTALLING IDEOLOGICAL DISRUPTION.

IT WOULD NOT BE A STRETCH TO SAY MOSCOW PURSUES A STRATEGY OF ANARCHY FROM WITHIN. LET THE LINES BETWEEN TRUTH AND LIES BE BLURRED. LET THE PEOPLE TURN AGAINST THEIR OWN GOVERNMENT. LET THE INSTITUTIONS IMPLODE. LET THE CHAOS ENSUE, PULLING AT THE STRINGS OF THE VERY FABRIC OF THE SYSTEM. IN A DEMOCRACY, THIS CAN BE A VERY DANGEROUS GAME OF DOMINOES INDEED.

To accomplish its objectives, Moscow turns to a diverse spectrum of tactics and techniques. Coercion is not a new modus operandi for former Soviet operatives. Flooding the populace with disinformation and propaganda is just one mechanism. Critical information leaks are another. Both can be equally destructive. Both can call into question the powers that be. It would not be a stretch to say Moscow pursues a strategy of anarchy from within. Let the lines between truth and lies be blurred. Let the people turn against their own government. Let the institutions implode. Let the chaos ensue, pulling at the strings of the very fabric of the system. In a democracy, this can be a very dangerous game of dominoes indeed.

So it echoes that the United States does not have a cybersecurity problem. It has a China problem; a North Korea problem; an Iran problem; and a Russia problem. There may indeed emerge other players that pose a serious or semi-serious threat to the U.S. in the cyber domain. Nonetheless, for now, the primary state threats line up synchronously with the primary cyber threats as an extension of one another. A watchful eye and careful vigilance will be the most imperative tools in containing these problems, reducing the threats, increasing deterrence, and detecting other potential cyber adversaries. Russia is the most active adversary in this realm, and thus the worst of the threats at the moment – deserving of its own focused discussion.

V. Short of War: The Russian Hack of the American Elections



Russia's recent display of cyber arrogance warranted its own special session at the conference. There are still far too many clouds hovering around what actually happened in the 2016 U.S. elections. How far was Moscow's reach? What was the actual intent for such cyber meddling? Was the Democratic National Committee isolated as a target, or was the Republican National Committee also attacked? There are more questions than answers. Yet, there is no limit to the speculation and the rumors.

One hears whispers everywhere about the DNC hack as if this was the first time Russia committed an act of cyber espionage in the United States, as if this was the first time Russia crossed the invisible line from the acceptable to the unacceptable. Has the cyber intrusion in late 2014 been forgotten? In a wave of strikes, the White House and the U.S. State Department were compromised. Indeed, the string of hacks may say more about the defensibility of Executive Branch systems than about the capabilities of foreign intruders. Only unclassified emails were breached at both the White House and the State Department. But these are some of the highest offices of the United States federal government. Unclassified systems still consist of sensitive material that is not public information such as confidential exchanges among the Joint Chiefs of Staff and the president's real-time schedule – the who, what, when, and where on the agenda of arguably the most powerful leader in the free world. Similarly, the State Department's

systems gifted the hackers with sensitive material shared with foreign intelligence agents over unclassified networks – including details on the Ukrainian crisis. Why such information exists on unclassified systems is a whole different mystery.

WASHINGTON HAD A CERTAIN RESPECT FOR MOSCOW'S CYBER CAPABILITIES AND WISHED TO ESTABLISH MUTUALLY AGREED UPON RULES OF ENGAGEMENT IN CYBERSPACE – A SORT OF NEW 'MOSCOW RULES'.

The compromised systems were temporarily unplugged in order to be secured and upgraded. In fact, such an attack was so unexpected and surprising, that there were no contingency measures in place. At the DoS, senior officials literally had to operate with Gmail accounts because there was no other way to communicate with their staffers once the systems were down. Investigations stretched across the Secret Service, the FBI, and other intelligence services, as it was internally viewed as a rather sophisticated spear phishing attack. The danger of such an attack is that it is so simple – more of a con than a burglary, if one were to analogize. A threat actor merely disguises an email so it appears to be generated internally or from a recognizable organization, and once the recipient clicks on the included link, the black magic begins.

At the outset, spokespersons for the White House and the State Department were cautious not to raise any red flags or sound any alarms, downplaying the breach as "activity of concern." The reasons for not directly attributing the attacks to Russia were largely political. Washington had a certain respect for Moscow's cyber capabilities and wished to establish mutually agreed upon rules of engagement in cyberspace – a sort of new 'Moscow rules'. There was also a lack of foresight, wherein Washington did not expect Moscow to later use its cyber weapons in a U.S. presidential election as the whole world was watching. Perhaps this is precisely what made it such an opportune target for Moscow.

The timing of the White House and DoS cyber attacks did not particularly prompt those in the know to be outspoken either – given the upcoming midterm elections. It was not very encouraging to later learn that the administration did not actually uncover the incursion itself, but was given a tip by a foreign intelligence partner. When it was finally aired to the public, talking points still only covered "suspicions" of Russian involvement. Not until much later was Russia ultimately identified as the architect of the hacks. For what it is worth, James Clapper (then the Director of National Intelligence) did comment on Russia's growing cyber activity in a February 2015 Senate hearing following the attack, calling the cyber threat posed by Russia "more severe than we have previously assessed." Still, such gentle language in a Senate hearing months later is not going to be the kind of strong, timely attribution that leads to credible deterrence.

A DEGREE OF TRANSPARENCY COULD HAVE ACTUALLY HELPED CURB MOSCOW'S CYBER PURSUITS. PUBLICIZING THE ATTACK AND OUTING RUSSIA WOULD HAVE JUSTIFIED IMMEDIATE SANCTIONS, WHICH IN TURN MIGHT HAVE DETERRED MOSCOW FROM ITS FUTURE CYBER ADVENTURISM – ESPECIALLY THE 2016 HACK OF THE U.S. ELECTIONS.

Everyone affected seemed to have a strong belief that the perpetrators were connected to Moscow, but it was a policy decision not to name or blame Russia publicly. The explanation provided was inadequate and insufficient, claiming it would have been more difficult to deal with Moscow on such issues if Russia was publicly humiliated. In retrospect, this was a

mistake. A degree of transparency could have actually helped curb Moscow's cyber pursuits. Publicizing the attack and outing Russia would have justified immediate sanctions, which in turn might have deterred Moscow from its future cyber adventurism – especially the 2016 hack of the U.S. elections.

This is necessary background. It is critical context. The DNC hack must be framed within this understanding – that Russia has not suddenly become so bold; it has always been moving in this direction. This also is not the first time that Moscow has used cyber aggression to meddle in the internal affairs of another independent nation. One only has to turn to the recent history of former Soviet-occupied states. The writing has been on the wall.

As early as 2007, Moscow staged a DDoS attack directed primarily at the government, media, telecommunication, financial, and banking sectors of Estonia – the breadth and depth of which necessarily trickled down to impact the general population as well. The provocation was not proportional to the cyber raid that followed. The Estonians were readying to relocate a World War II memorial for Russian soldiers – a site in Tallinn known as the Bronze Soldier. The Estonians believed they were simply exercising their autonomy in shifting a statue synonymous with years of oppression – a move they had rightly dreaded would instigate the Russians. To Moscow, this supposed recalcitrance presented an open invitation to disable connectivity and communications while crashing the internet of this very small, yet very internet-dependent country. It is not an exaggeration to claim Estonia is one of the most heavily wired countries, well ahead of the curve in 2007. Even then, routine daily tasks were transacted at the click of a button in the palm – parking passes, meal payments, banking transactions, news updates, and safety alerts, to name a few. The Estonian government was one of the few in the world that was already operationalizing online electoral processes such as voting. All of this sounds rather normalized and mundane in 2017. But pause and rewind ten whole years.

It was not just the country's connectivity that made the Estonian cyber invasion unique. This represented a watershed moment. It marked the first-ever simultaneous strike against so many critical sectors of one nation by another. In the words of Estonia's Minister of Defense at the time, Jaak Aaviksoo, "This was the first time that a botnet threatened the national security of an entire nation." And though he did not know this when he said that, he was right. The Estonian case demonstrated a sophisticated strategic cyber scheme with several stage-by-stage attacks – the likes of which had never been witnessed on the global stage. It ushered in a whole new era of cyber threats and security.

PERHAPS NO ONE TRULY BELIEVED THAT MOSCOW WOULD DARE TO VENTURE ACROSS SUCH LINES OF SOVEREIGNTY AGAINST ITS MOST CAPABLE ADVERSARY – THE UNITED STATES. AT ITS VERY CORE, THIS WAS A COLLECTIVE FAILURE OF IMAGINATION.

The 2014 Ukrainian election was another signpost of what was to come – perhaps an even more ominous case study for the United States. Days before the election, Russian operatives shut down the computer systems of the Central Election Commission in Ukraine. Ukrainian technicians were able to restore the systems just in time for the election, but the official website was hacked shortly thereafter displaying fake results. Perhaps no one truly believed that Moscow would dare to venture across such lines of sovereignty against its most capable adversary – the United States; but it was far more conceivable against a weaker state like Ukraine. At its very core, this was a collective failure of imagination.

The FBI first contacted the DNC about suspicious activity in the fall of 2015, again

based on a foreign intelligence tip. At this early stage, a mid-level FBI investigator was to collaborate with the DNC on the technology side. The IT official representing the party treated the message of caution with little regard, and invested negligible energy in further investigating. There was an absence of urgency in acknowledging, comprehending, or resolving this potentially calamitous cyber breach before it became a cyber catastrophe. The FBI followed up in April 2016, but again the matter was treated lightly.

SINCE CYBER STRIKES ARE NOT VISUAL, TANGIBLE ATTACKS, THEY DO NOT ELICIT IMMEDIATE, VISCERAL RESPONSES – IN THE WAY THAT A BOMB OR EXPLOSION WOULD.

Shockingly, President Obama was only briefed on the cyber invasion in June 2016. The unfathomable timeline here means that Russian cyber agents were in the servers of one of the two major political parties of the country for nine whole months before the American president was even alerted to their presence. Why had the Democratic National Committee not taken its own protection as seriously as its candidate, Hillary Clinton, had taken hers? There is, as of yet, no evidence that she herself was hacked; but, the emails of her campaign chairman, John Podesta, were indeed accessed. He could easily have avoided making himself vulnerable had he taken simple measures to encrypt his data – enabling two-factor authentication on email accounts or utilizing an external security key for two-step verification. By now, we should be past the failure of imagination problem on an individual level. The lack of emphasis on data security – by individuals of national importance – is truly alarming and crippling.

With that said, the DNC hack and subsequent release of information was certainly the boldest demonstration of cyber interference in the internal affairs of the United States. This was an act of directly meddling in U.S. domestic politics. The implications of the infringement do not stop at the gate of the Democratic National Committee; they extend to the entire democracy. And so the national reaction matters. Thus began the long debate on how Obama should reply. Other than talks of attribution, there were internal discussions on a soft retaliation – disclosing details on Putin's finances around the world, for instance, or his financial ties to oligarchs. Ultimately, such ideas were sidelined due to a lack of conviction in their potential for having any real impact. President Obama, a Democrat, was also hesitant to come off as taking sides in the 2016 election. He worried that a harsh public position on the hacks may unfairly boost Hillary Clinton – or worse, cost her, if his role was perceived as interfering. Of all the factors weighed in internal discussions with his closest advisers, one that stands out is Obama's fear of provoking Moscow to up the ante and actually manipulate the polls themselves come Election Day.

Since cyber strikes are not visual, tangible attacks, they do not elicit immediate, visceral responses – in the way that a bomb or explosion would. So ultimately, there was no real public pressure or demand for the Obama administration to counter with decisive action. Only in the final week of his presidency did Obama turn to sanctions – a case of too little; too late. This was an attack against the integrity of U.S. electoral politics, and the answer should have been swifter and stricter.

A BULLET IS FIRED, A BOMB EXPLODES, A MASSACRE OCCURS, AND THERE IS AN UNIGNORABLE NEED FOR AN IN-KIND REPRISAL. IN THE CYBER DOMAIN, THERE IS NO FINGER ON THE TRIGGER; NO ON-OFF SWITCH. CYBERSPACE OPERATES ON A THERMOSTAT. THE HEAT CAN BE TURNED UP OR TURNED DOWN TO ADJUST FOR CALCULATIONS AND RETALIATIONS.

In many ways, the debate within the halls of the White House is emblematic of why cyber attacks have come to be the perfect short-of-war weapon. They are not like assaults by conventional weapons. A bullet is fired, a bomb explodes, a massacre occurs, and there is an unignorable need for an in-kind reprisal. In the cyber domain, there is no finger on the trigger; no on-off switch. Cyberspace operates on a thermostat. The heat can be turned up or turned down to adjust for calculations and retaliations. This also makes deterrence a very different problem in cyber warfare than in conventional warfare. The populace may impel the government with demands for a proportional retaliation to some spectacular and tangible act of war; whereas a cyber act may not even be a blip on the public's radar.

This is not to say that there should always be an equal and opposite reaction for every cyber action. An eye for an eye would leave the whole world blind. Instead, Washington must continue finding its place in the cyber domain as it has in more traditional domains. This will be a long process, but one that the country's cyber defenders must not shy away from. If what the U.S. really desires is cyber supremacy, it will have to temper that with channels of cooperation and mutual deterrence. There will be times when it is in the best interest of the nation to act and react with a strong cyber offense. There will also be times when Washington will need to prove that it is willing and able to demonstrate restraint. As it has proven time and time again, America may garner greater respect if it can heighten global awareness of both its cyber abilities and its cyber restraint. In simple terms, the key to deterrence will be a consciousness – for our adversaries and others – that there are actions we can take that we choose not to take; that our cyber offense can be a devastating force, but we will put deep thought into when it is warranted and how it is employed.

VI. Cyberspace and U.S. Foreign Policy: Assessing Achievements and Prioritizing Action

The threats described in this report paint a rather grim picture of the world for the United States. But threats are only half the story; progress is the other half. As a nation, the U.S. has actually come quite far in adapting to the evolving cybersecurity threat landscape. Cybersecurity has continued to become a more prominent concern for American presidents since the days of Bill Clinton, and a much more nuanced comprehension has emerged since then. Where it was initially pegged as a tangential issue, it has now become more centralized on the left and right sides of the aisle. This appreciation for the vast reach of cyberspace and the deep implications of cybersecurity is in itself quite an achievement. Alongside progress, one must also weigh recommendations for further improving the state of the nation's cybersecurity. Replicate what has worked; amend what has not.

The strongest practical recommendation must be a greater emphasis on credible deterrence. One major attitudinal shift has had a tangible impact: over the last few administrations, there has been a move away from tolerating the theft of intellectual property – a threat that has been labeled "the greatest transfer of wealth in history" by General Keith Alexander, the first Commander of the U.S. Cyber Command.

POLICY SILENCE MAY ENCOURAGE WORSE SUCH ATTACKS IN THE FUTURE.

There should similarly be less tolerance with other cyber targeting. An example of this would be Iran's hack of the New York dam. Though no substantial damage was done in that instance, policy silence may encourage worse such attacks in the future. Accordingly, naming and shaming state sponsors or individual hackers has unquestionably had a positive effect and must be continued. Where they previously

thought they could go unnoticed or untouched, they must now tread more carefully. However, the weightiest impact has come from the threat of direct punishment in the form of sanctions and similar policy shifts. China is a strong case in point. Beijing only came to the table to discuss compromises and concessions when it realized the Obama administration's strategic patience had worn thin and the president's team had begun preparing an unprecedented sanctions package against Chinese corporations and individuals – namely those that benefited from the government's cyber thefts. The tangibility of the sanctions threat is what ultimately laid the groundwork for the execution of the U.S.-China cyber agreement – which seems to be working more so than not, in the year and a half since its signing. The PLA's state-sponsored espionage, for instance, has been detected at a far lower rate than previously.

Still, with cyber offense as a tool of foreign policy, it cannot be treated in isolation. The punishment must fit the crime. In other words, the response must speak to the motives of the cyber culprit, if any tangible effects are to be expected. If cyber activity was an economic tool for Beijing, there will have to be economic incentives to keep Chinese cyber spies at bay – in the same way that economic penalties proved a practical solution. How policies align in the new administration matters profoundly for the future of the agreement and the relationship writ large. There is certainly scope for crafting comparable agreements elsewhere. When it comes to deterrence, a similarly tailored approach would be beneficial to apply to other threat actors as well. Deconstructing the national goals of other adversaries will be the key to determining the best course for their treatment in the cyber domain.

While such recent accomplishments have directly curtailed the number of cyber attacks, there is ample room for improvement when it comes to mitigating risk. On this front, the United Nations Group of Governmental Experts (GGE) 2015 report was a stride forward. The GGE report was designed to specifically address international norms, and was accordingly called the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. What emerged was a negotiated understanding on cyber threats and acceptable responses among 20 leading countries – from norms and principles to rules and confidence-building measures. While this is not the be-all and end-all of cyber struggles, the significance of such a convention lies in the precedent it sets for formalized rules of global cyber engagement going forward. Now these rules must be cohesively implemented and enforced, and Washington could benefit from taking the lead.

DECONSTRUCTING THE NATIONAL GOALS OF OTHER ADVERSARIES WILL BE THE KEY TO DETERMINING THE BEST COURSE FOR THEIR TREATMENT IN THE CYBER DOMAIN.

In fact, more needs to be done to collaborate with traditional allies that can also be cyber allies. Only in working with international partners, can cyber norms be created and carried out in a meaningful way. Cyber cooperation must continue to be a pillar in any policy conversation on cybersecurity. In this domain, however, a word of caution might be necessary. Traditional partners may be dressed differently; and expected adversaries may wear different masks. Washington can expect the same players to arrive at the cyber ball, but it must not be too shortsighted – lest it miss a threat masquerading as a non-threat.

Managing competing priorities across borders continues to be challenging, yes, but there is a ray of light in the operational paradigm that national cyber defenses have taken within the United States. A major achievement was the foundation of a unified command and control

center: U.S. Cyber Command (USCYBERCOM). Established at the directive of the Secretary of Defense in 2009, Cyber Command was operational by 2010 – housed within U.S. Strategic Command (USSTRATCOM). A prominent part of its Mission Statement entrusts USCYBERCOM to "conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure U.S./Allied freedom of action in cyberspace and deny the same to our adversaries." Its *Focus Statement* also confers it with the duty of "unif[ying] the direction of cyberspace operations." Fusing these responsibilities within a single command center was a significant leap forward.

Given the nature of its focus and the era in which it was instituted, Cyber Command has attracted a whole new generation of talented tech-savvy young Americans with a sense of patriotic duty. In fact, much of the technical expertise is on a junior level in terms of rank and seniority. Commanding officers at USCYBERCOM seem to be prudently aware of the enormous potential to be tapped. They have started making great progress with the next generation. Other units operating in the cyber arena could benefit from learning this lesson. America's forces need to be more active with younger generations and seize all that they have to offer in the way of technical skills and an aptitude for cyber problem-solving.

TRADITIONAL PARTNERS MAY BE DRESSED DIFFERENTLY; AND EXPECTED ADVERSARIES MAY WEAR DIFFERENT MASKS. WASHINGTON CAN EXPECT THE SAME PLAYERS TO ARRIVE AT THE CYBER BALL, BUT IT MUST NOT BE TOO SHORTSIGHTED – LEST IT MISS A THREAT MASQUERADING AS A NON-THREAT.

Though subtle, one of the most valuable lessons to be drawn from the operational tendencies of USCYBERCOM is the comingling of "adversary experts" – or area specialists – with the sea of technical experts. Area experts are an integral component in shaping response options within the military. Their presence enables a more consistent campaign of actions, particularly when it comes to deterrence. In this way, decision-makers can connect the dots between what will be possible and what will be effective. This is a paradigm that must be underscored and applied to other elements of the cybersecurity effort, especially as cyber specialists come to terms with the fact that their world is just a molecule in the foreign policy universe.

USCYBERCOM's potential, nevertheless, has yet to be maximized. Due to the complex bureaucracy within the Department of Defense, Cyber Command is sometimes excluded from discussions focusing on issues that could be related to cybersecurity, such as certain aspects of counterterrorism. Another constricting factor can be that the DoD is an organization biased towards action, operating in an environment where policymakers may favor restraint. The view within Cyber Command is not necessarily what one would expect, in fact: the military does not have to lead the cybersecurity effort, and probably should not; but it can and must help sustain it. This makes it incredibly important for policymakers and military leaders to jointly craft responses to cyber threats and attacks – so that the best possible decision on action or restraint is reached in each instance.

While Cyber Command has begun to formalize and institutionalize mechanisms for capacity building, this is a focus that must continue to be prioritized across the board. Rhetoric about capacity building must be met with the appropriate investments and resources. Across the government, systems need to be upgraded, protocols need to be streamlined, and encryption needs to be standardized. Threat scenarios should be built out and prepared for, so that there is never again a simple attack that

catches the government totally off guard – as with the White House and DoS attacks of 2014. As such, technical experts and policymakers need to exchange ideas on what short- and long-term digital transformations look like. They need to discuss how to scale security benefits so they extend to departments that would not traditionally be expected cyber targets in cybersecurity – like the Office of Personnel Management.

These feats should not be left solely to the military. There must also be a continuing role for the private sector. Across the last few administrations, there has been a consensus of sorts, but there might be a shift in direction under the new administration. Where President Obama was distinctly cautious not to over-militarize the issue of cybersecurity, the current administration might be altering the approach so that cyberspace falls more squarely under the purview of the military. It will be crucial to keep the private sector involved, and even to allow it to take the lead in improving cybersecurity solutions when called for.

What cannot be disputed is the key role the private sector has played thus far, and the central role it will – and must – continue to play going forward. It would be an error of judgment to siphon off the private sector from the problems of the government. American corporations are still American, with a vested interest in sustaining cybersecurity for the nation writ large. The current administration has floated the idea of compartmentalizing the private sector from the public sector in this domain, but this would actually be an oversight with unforeseeable implications. While there is unquestionably a need for certain cyber knowledge to remain classified to only the highest guardians of U.S. defense, individual companies within the private sector may have capabilities that are not always readily available to large bureaucracies within the government. They also have greater latitude for trial and error operations, affording them the leeway to arrive at the best solutions through a process of deduction – something that government actors cannot always afford to experiment with.

Government research labs were once responsible for the development of revolutionary new technology such as the first supercomputer and Arpanet – the predecessor to the modern internet. Now, the private sector is often where innovation begins, especially in the fields of technology and cyberspace. Privately owned firms attract some of the top experts in the field and furnish them with the top tools of the trade. The fact that they cater not only to government clients, but also to an array of small and large profit-driven corporations forces them to operate efficiently and deliver tangible real-time solutions. The level of specialization and the ever-growing competition also drive the creation of new methodologies and constant updates to the industry's best practices. In fact, as the private cyber sector continues to shape itself, there will be lessons learned that carry over to government as well. For instance, several firms are now focused on risk mitigation, an area of concern for the nation's cyber warriors. Removed from government bureaucracy, private cyber firms are also well poised to act instantaneously and with fewer limitations. Attesting to all this, the DNC hack was ultimately traced back to Russia by a private cyber threat intelligence firm, CrowdStrike. Thus, in many ways, it is not just the international order and the evolving cyber threats that have influenced and shaped the cyber domain; it is also the private sector.

Nevertheless, recommendations (such as those mentioned above) will be far less effective if the overarching dialogue on cybersecurity is not framed properly. Accordingly, this is the most crucial takeaway. What has been stressed throughout this analysis is that cybersecurity must be couched within the larger foreign policy discourse. It is vital to address one when addressing the other. Cyber defenses can be improved and cyber offenses can be upgraded, but the best way to further the country's

cybersecurity is to ameliorate and better manage America's relationships with the very adversaries that become threat actors in cyberspace. This cannot be emphasized enough: We do not have a cyber problem. We have a China problem. A North Korea problem. An Iran problem. A Russia problem.

The discussion on cyber issues can be extensive and varied, but within the context of foreign policymaking, we must reflect on how advancing technology affects the business of statecraft. Just as the evolution of media revolutionized state-to-state politics on the global stage, current developments are reorganizing the way we receive information and perceive subjects – arguably in a much swifter, less noticeable way than ever before. But the cycle of change itself is not new. Remember the introduction of the radio? It irrefutably modernized our global interconnectedness. Remember the arrival of the television? It indubitably altered the way we understood global politics in real time. Remember the advent of the 24-hour news cycle? It inarguably laid the foundation for the 'instant society' we live in today.

With each new connective technology, the world has gotten metaphorically flatter – for the average citizen: more accessible; more comprehensible; more immediate; more relevant. In this more connected world, cybersecurity matters more than ever before.

Society has greatly benefited as technology has become more advanced and everything has become more networked, but it is also more vulnerable for these very same reasons.

CYBER DEFENSES CAN BE IMPROVED AND CYBER OFFENSES CAN BE UPGRADED, BUT THE BEST WAY TO FURTHER THE COUNTRY'S CYBERSECURITY IS TO AMELIORATE AND BETTER MANAGE AMERICA'S RELATIONSHIPS WITH THE VERY ADVERSARIES THAT BECOME THREAT ACTORS IN CYBERSPACE. WE DO NOT HAVE A CYBER PROBLEM. WE HAVE A CHINA PROBLEM. A NORTH KOREA PROBLEM. AN IRAN PROBLEM. A RUSSIA PROBLEM.

The final consideration is that of leverage. Where do we have it? How do we use it – currently and going forward? Who has leverage against us? How do we balance against that? Washington must bear in mind that competition and conflict will abound in any domain – that is a fact of nature. Limited resources restrict growth, which in turn confines space for dominance. This is the international order – whether on land, in the sea, in the air, or in space. It remains so in the realm of ones and zeroes.

GLOSSARY OF HELPFUL TERMS

Breach / Data Breach: The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information[1]

Code / Coding: One or more commands or algorithm(s) designed to be carried out by a computer[2]

Criminal Syndicates: groups of criminals, closely or loosely affiliated, involved in some kind of organized crime[3]

> ***Organized crime***: refers to those self-perpetuating associations of individuals who operate internationally for the purpose of obtaining power, influence, monetary and/or commercial gains, wholly or in part by illegal means, while protecting their activities through a pattern of corruption or violence[4]

Critical Infrastructure: The systems and assets, whether physical or virtual, so vital to society that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters[5]

Cyber Attack: Cyber attacks are socially or politically motivated attacks carried out primarily through the Internet. Attacks target the general public or national and corporate organizations and are carried out through the spread of malicious programs (viruses), unauthorized web access, fake websites, and other means of stealing personal or institutional information from targets of attacks, causing far-reaching damage[6]

Cyber Coercion: the use, or threat of use of cyber force against an adversary in an attempt to compel them to take a desired action or not take an undesired action[7]

Cyber Crime / Cyber Criminals: normal crimes—such as financial crimes and terrorism—carried out through the internet; sophisticated attacks against computer hardware and software[8]

---

[1] "Glossary," NICCS, last modified January 17, 2017, accessed March 24, 2017, https://niccs.us-cert.gov/glossary#D.
[2] "Glossary," Code.org, last modified February, 2017, accessed March 24, 2017, https://code.org/curriculum/docs/k-5/glossary
[3] "Crime Syndicate," English Oxford Dictionaries, last modified 2017, accessed March 24, 2017, https://en.oxforddictionaries.com/definition/crime_syndicate
[4] "International Organized Crime," The United States Department of Justice, last modified June 2, 2015, accessed March 24, 2017, https://www.justice.gov/criminal-ocgs/international-organized-crime.
[5] "Glossary," NICCS, last modified January 17, 2017, accessed March 24, 2017, https://niccs.us-cert.gov/glossary#D.
[6] "Information Management," The NEC Group, last modified 2017, accessed March 24, 2017, http://www.nec.com/en/global/solutions/safety/info_management/cyberattack.html.
[7] Clinton M. Woods, ""Implementing Cyber Coercion," *Institutional Archive of the Naval Postgraduate School* (March, 2015): 7. Accessed March 24, 2017. http://calhoun.nps.edu/bitstream/handle/10945/45277/15Mar_Woods_Clinton.pdf?sequence=1
[8] "Cybercrime," Interpol, last modified 2017, accessed March 24, 2017, https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

Cyber Readiness: the process of integrating security measures across an entire system or infrastructure that continuously monitors not only threats, but incoming and outgoing activity across the network[9]

Cyber Terrorism / Cyber Terrorists: A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda[10]

Cyber Vandalism: a type of malicious behavior that involves damages to computers and data in various ways, and potentially disrupting businesses. Typical computer vandalism involves the creation of malicious programs designed to perform harmful tasks such as erasing hard drive data or extracting login credentials[11]

Cyber War(fare): Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks[12]

Dark Web / Deep Web: the Deep Web is a general term that refers to anything on the internet that cannot be accessed with a conventional search engine (Google, Bing, Yahoo), unlike the Surface Web; the Dark Web is a small portion of the Deep Web that has been intentionally hidden, and cannot be accessed with a standard Web browser (Internet Explorer, Google Chrome, etc.).[13]

> ***Surface Web***: anything on the internet that can be indexed by a typical search engine like Google, Bing, or Yahoo.

DDoS: The disabling of a targeted website or Internet connection by flooding it with such high levels of Internet traffic that it can no longer respond to normal connection requests. The targeted site may crash while trying to respond to an overwhelming number of connections requests or it may be disabled because all available bandwidth and/or computing resources are tied up responding to the attack requests.[14]

---

[9] "Cyber Readiness – What is It and Why You Need It," TSI, last modified February 5, 2015, accessed March 24, 2017, http://tsisupport.com/cyber-readiness-what-is-it-and-why-you-need-it/

[10] "Keyword Index and Glossary of Core Ideas," Berkman Klein Center for Internet and Society at Harvard University, last modified August 7, 2012, accessed March 24, 2017, https://cyber.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas#Cyber_Terrorism

[11] "Computer Vandalism," Kaspersky Labs, last modified 2017, accessed March 24, 2017, https://usa.kaspersky.com/internet-security-center/threats/computer-vandalism#.WNV-GlUrLct

[12] "Cyber Warfare," Rand Corporation, last modified March 22, 2016, accessed March 24, 2017, http://www.rand.org/topics/cyber-warfare.html

[13] "Clearing Up Confusion – Deep Web vs. Dark Web," BrightPlanet, last modified March 27, 2014, accessed March 27, 2017, https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/.

[14] "Keyword Index and Glossary of Core Ideas," Berkman Klein Center for Internet and Society at Harvard University, last modified August 7, 2012, accessed March 27, 2017, https://cyber.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas#DDoS_Attack

Decryption: The process of converting encrypted data back into its original form, so it can be understood.[15]

Disinformation Campaigns: the spread of false information which is intended to mislead, especially propaganda issued by a government organization to a rival power or the media.[16]

Encryption: Converting data into a form that cannot be easily understood by unauthorized people.[17]

Espionage: the process of obtaining information that is not normally publicly available, using human sources (agents) or technical means (like hacking into computer systems). It may also involve seeking to influence decision-makers and opinion-formers to benefit the interests of a foreign power.[18]

Firewall: A hardware/software device or a software program that limits network traffic according to a set of rules of what access is and is not allowed or authorized.[19]

Hacking / Hackers: advanced computer users who spend their time searching for vulnerabilities in IT systems, usually to gain access to information for which they are unauthorized.[20]

Hacktivism: The nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends. These tools include web site defacements, redirects, denial-of-service attacks, information theft, web site parodies, virtual sit-ins, virtual sabotage, and software development. Individuals who perpetrate these kinds of political acts are known as "Hacktivists."[21]

Hybrid War(fare): a type of warfare widely understood to blend conventional/unconventional, regular/irregular, information and cyber warfare. [22]

Identity Theft: The exploitation by malevolent third parties of unwarranted access to clients' or consumers' identities. Often the result of lax data security or privacy measures.[23]

---

[15] "Glossary," NICCS, last modified January 17, 2017, accessed March 27, 2017, https://niccs.us-cert.gov/glossary#D

[16] "Disinformation," Oxford English Dictionaries, last modified 2017, accessed March 27, 2017, https://en.oxforddictionaries.com/definition/disinformation

[17] "Glossary," NICCS, last modified January 17, 2017, accessed March 27, 2017, https://niccs.us-cert.gov/glossary#D

[18] "Espionage," MI5 – The Security Service, last modified 2017, accessed March 27, 2017, https://www.mi5.gov.uk/espionage

[19] "Glossary," NICCS, last modified January 17, 2017, accessed March 27, 2017, https://niccs.us-cert.gov/glossary#D

[20] "Keyword Index and Glossary of Core Ideas," Berkman Klein Center for Internet and Society at Harvard University, last modified August 7, 2012, accessed March 27, 2017, https://cyber.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas#Hacker

[21] "Keyword Index and Glossary of Core Ideas," Berkman Klein Center for Internet and Society at Harvard University, last modified August 7, 2012, accessed March 27, 2017, https://cyber.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas#Hacktivism

[22] "Hybrid war – does it even exist?" NATO Review, last modified May 7, 2015, accessed March 27, 2017, http://www.nato.int/docu/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm

Information Warfare (IW): a form of comprehensive warfare, which may include any combination of military and non-military techniques, such as cyber attacks, with political, military, or economic objectives.[24]

Internet Service Provider (ISP): A company that offers access to the Internet, and may also provide add-on services such as web hosting, electronic mail, virus scanning, SPAM filtering, etc.[25]

Malware: Software that compromises the operation of a system by performing an unauthorized function or process.[26]

Phishing: A criminally fraudulent, digital form of social engineering meant to deceive individuals into providing sensitive information.[27]

Ransomware: a type of malware that prevents the use of a computer, holding the computer or certain files "ransom." All types of ransomware will ask the user to do something, usually pay money, before re-gaining access to their computer, although there is no guarantee that access will be restored. [28]

Remote Access Tool / Trojan (RAT): Remote Access Tool is a piece of software used to remotely access or control a computer. This tool can be used legitimately by system administrators for accessing the client computers, but when used maliciously, they are termed Remote Access Trojans.[29]

Spyware: Software that is secretly or surreptitiously installed into an information system without the knowledge of the system user or owner.[30]

Subversion: A general term that refers to actions designed to undermine the military, economic, psychological, or political strength or morale of a governing authority. [31]

---

[23] "Keyword Index and Glossary of Core Ideas," Berkman Klein Center for Internet and Society at Harvard University, last modified August 7, 2012, accessed March 27, 2017, https://cyber.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas#Identity_Fraud.2FTheft

[24] "Toward a Functional Model for Information Warfare," Central Intelligence Agency – Library, last modified June 27, 2008, accessed March 27, 2017, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/97unclass/warfare.html.

[25] "Keyword Index and Glossary of Core Ideas," Berkman Klein Center for Internet and Society at Harvard University, last modified August 7, 2012, accessed March 27, 2017, https://cyber.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas#Internet_Service_Provider

[26] "Glossary," NICCS, last modified January 17, 2017, accessed March 27, 2017, https://niccs.us-cert.gov/glossary#D

[27] "Glossary," NICCS, last modified January 17, 2017, accessed March 27, 2017, https://niccs.us-cert.gov/glossary#D

[28] "Ransomware," Microsoft – Malware Protection Center, last modified June, 2016, accessed March 27, 2017, https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx

[29] "Remote Access Tool," InfoSec Institute, last modified April 24, 2014, accessed March 27, 2017, http://resources.infosecinstitute.com/remote-access-tool/#gref

[30] "Glossary," NICCS, last modified January 17, 2017, accessed March 27, 2017, https://niccs.us-cert.gov/glossary#D

[31] "Subversion," *DOD Dictionary of Military and Associated Terms* (March 2017): 231, accessed March 27, 2017, http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf

Threat Actor: An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities, also known as a threat agent. [32]

Virus: A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.[33]

Wiper Attack: attack perpetrated with a specific type of malware that erases data from victims' computer drives.[34]

Zero-Day: A zero-day vulnerability, at its core, is a flaw. It is an unknown exploit in the wild that exposes a vulnerability in software or hardware and can create complicated problems well before anyone realizes something is wrong. In fact, a zero-day exploit leaves NO opportunity for initial or pre-emptive detection.[35]

---

[32] "Glossary," NICCS, last modified January 17, 2017, accessed March 27, 2017, https://niccs.us-cert.gov/glossary#D

[33] "Glossary," NICCS, last modified January 17, 2017, accessed March 27, 2017, https://niccs.us-cert.gov/glossary#D

[34] "Wiper Malware Poses Destructive Threat," SecurityIntelligence, last modified January 21, 2015, accessed March 27, 2017, https://securityintelligence.com/wiper-malware-poses-destructive-threat/

[35] "What is a Zero-Day Exploit?" FireEye, last modified 2017, accessed March 27, 2017, https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html

National Committee on American Foreign Policy's (NCAFP)

2017 CYBER CONFERENCE

NEW FRONTIER IN DEFENSE: CYBERSPACE AND U.S. FOREIGN POLICY

Thursday, February 2, 2017

PARTICIPANTS LIST

PANELISTS

Mr. Dmitri ALPEROVITCH
Co-Founder & Chief Technology Officer
CrowdStrike

Ambassador Rosemary A. DICARLO (Ret.)
President
National Committee on American Foreign Policy

Mr. Robert K. KNAKE
Whitney Shepardson Senior Fellow
Council on Foreign Relations

Mr. Rafal ROHOZINSKI
Co-Founder & Principal
SecDev Group

Dr. Adam SEGAL
Ira A. Lipman Chair in Emerging Technologies & National Security & Director of the Digital & Cyberspace Policy Program
Council on Foreign Relations

Mr. Ian WALLACE
Co-Director, Cybersecurity Initiative
New America

Brigadier General Jennifer G. BUCKNER
Deputy Commander of Operations
Cyber National Mission Force at U.S. Cyber Command

Mr. Jason HEALEY
Senior Research Scholar
School of International & Public Affairs at Columbia University

Ms. Angela MCKAY
Director, Government Security Policy & Strategy
Trustworthy Computing at Microsoft

Mr. David E. SANGER
Chief Washington Correspondent
The New York Times

Dr. Michael SULMEYER
Director, Cyber Security Project
Belfer Center for Science & International Affairs at Harvard University

PARTICIPANTS

Mr. John H. BELL, Jr.
Consultant
Lagoda Investment Management

Dr. Erica D. BORGHARD
Assistant Professor & Executive Director
Grand Strategy Program, U.S. Military Academy

Dr. Aaron F. BRANTLY
Assistant Professor & Cyber Policy Fellow
The Army Cyber Institute, U.S. Military Academy

Mr. John V. CONNORTON, Jr.
Secretary & Trustee
National Committee on American Foreign Policy

Mr. Jonathan M. CONRAD
Chairman, CEO, & Founder
AdmieMobile

Mr. Ken CREARY
Member
National Committee on American Foreign Policy

Mr. Armando FRANCO
CEO
International Investment Risk Advisors

Ms. Edythe M. HOLBROOK
Member
National Committee on American Foreign Policy

Mr. Richard R. HOWE
Executive Vice President & Treasurer
National Committee on American Foreign Policy

Mr. Jeppe T. JACOBSEN
PhD Candidate
Danish Institute for International Studies

Mr. Justin KOSSLYN
Product Manager
Jigsaw at Google

Captain Jourdan A. KURTZ
Executive Assistant to the Deputy Commander (Operations)
Cyber National Mission Force at U.S. Cyber Command

Ms. Simran R. MAKER
Project Associate
National Committee on American Foreign Policy

Ms. Hatice U. MORRISSEY
Trustee
National Committee on American Foreign Policy

Dr. George D. SCHWAB
President Emeritus
National Committee on American Foreign Policy

Prof. Mike URETSKY
Professor, Information Systems
New York University

OBSERVERS

Mr. Isaiah A. FISHER
Intern
National Committee on American Foreign Policy

Ms. Melissa J. SALYK-VIRK
Intern
National Committee on American Foreign Policy

Mr. Nicole A. SOFTNESS
MPA Candidate, International Security Policy
School of International & Public Affairs at Columbia University

Mr. Stephen WHITTAKER
Program Coordinator & Assistant to the President
National Committee on American Foreign Policy

National Committee on American Foreign Policy

320 Park Avenue, 3rd Floor • New York, NY 10022
Phone: (212) 224-1120 • Fax: (212) 224-2524
contact@ncafp.org • www.ncafp.org