MUTUALLY ASSURED DISRUPTION:
FRAMING CYBERSECURITY IN NUCLEAR TERMS

A National Committee on American Foreign Policy Report

By Simran R. Maker

January 2018

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 heads the Cybersecurity Initiative and the Middle East Initiative at the NCAFP. She focuses on addressing imminent challenges and evolving threats in these areas through her research and analysis as well as through closed-door conferences and roundtables with leading experts and practitioners.

Acknowledgments

The quality of this conference, and this report as a product thereof, are owed to the ten experts who so willingly and acutely provided insight on this important topic demanding greater attention, definition, and prioritization. We are utterly grateful to these panelists (listed in the "Participant List" at the end of the report) for taking time out of their busy lives to deliberate on these issues with us. Their candor and thoughtfulness made way for unique discussions and analyses. Rafal Rohozinski deserves a very special thank you as the Conference Chair. His endless conversations and guidance beforehand helped shape the topic and dialogues on this critical intersection of two important policy areas. Only his moderating during the conference could have so effectively directed the dialogue. We deeply value his support and look forward to continuing our work together.

The NCAFP would also like to thank all of our cyber donors for their generous support, which made this conference possible and helps us strengthen our Cybersecurity Initiative on an ongoing basis. In particular, we would like to thank Mr. John Bell and Ms. Edie Holbrook, both of whom demonstrate an unmatched commitment to our programs and are always eager to provide support in so many forms. We are indebted to you both. Thank you, also, to Mr. David Hunt, whose contribution greatly helped in arranging this session.

Again, we are tremendously grateful to all of you for your engagement, contributions, participation, support, and guidance, and we look forward to working with each of you again.

Images

January 2018

MUTUALLY ASSURED DISRUPTION:
FRAMING CYBERSECURITY IN NUCLEAR TERMS

A National Committee on American Foreign Policy Report

By Simran R. Maker

January 2018

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1

INTRODUCTION 4

I. EXCLUSIVITY OR ACCESSIBILITY: THE NUCLEAR AND CYBER CLUBS **6**

II. THE NUCLEAR-CYBER INTERPLAY: STRATEGIC AND TACTICAL CONSIDERATIONS **10**

A. On the Dangers of Analogy 10

B. On Deterrence 11

C. On Strategic Capabilities 13

D. On the Security of Nuclear Systems Against Cyber Attacks 13

E. On the Vulnerability of Civilian Infrastructure from Nuclear Versus Cyber Threats 14

III. ACROSS THE CHESSBOARD: ADVERSARIAL PLAYERS **16**

A. On the Russian Mindset 16

B. On the Chinese Mindset 17

C. On the North Korean Predicament 18

1. On North Korea's Use of Cyber Weapons **19**

2. On the Disruption of the North Korean Missile Program by Cyber Means **20**

IV. STRATEGIC LESSONS: LOOKING BACK AND THINKING AHEAD **21**

PARTICIPANT LIST 25

Executive Summary

The nuclear era began long before there was an awareness that international relations would be strategically and irreversibly shifted. The technology outpaced the policymaking and even the awareness or understanding of consequences. The cyber domain has similarly materialized in global affairs at lightning speed. While vastly different in material ways, both nuclear and cyber weapons are strategic capabilities that tilt the battlefield with a different calculus than traditional means of warfare.

Two facets particularly stand out and connect these otherwise isolated policy topics. One is the question of strategic continuance, for it is important that we examine the relevance of the strategic underpinnings of the nuclear era as they are shifting in the new cyber era. As policy thinkers and analysts, it is valuable to deconstruct and piece together shifts in the tectonic plates of the global order over the last few decades. In doing so, we must not ignore the technical shifts in capabilities, and so the other question is that of the intersection between cyber and nuclear capabilities, particularly on a tactical level. Both themes emerge, in different but equally relevant ways, throughout this analysis.

Today, cyber and nuclear capabilities are entangled in complex and dangerous respects that are not discussed or addressed often enough. Both domains – and the specialists, experts, engineers, technologists, policymakers, and practitioners associated with each – exist and operate in siloed spaces. This makes it particularly difficult to bridge the communities and make each aware of the threats against or concerns of the other. For this reason, such analysis is not only highly valuable, but critical.

The nuclear era spurred its own rules of the game – implicit and explicit – due to the existential risks deployment would pose to the entirety of mankind. Thus, even nations with very different interests came to follow a certain code of conduct, recognizing that all other interests were secondary to survival. This led to a decades-long continuance of the principle of Mutually Assured Destruction, which endured through the Cold War. While great powers such as the United States and the Soviet Union continued to push conflict to the brink in other domains, there remained a certain stability at the strategic level.

The stability of the nuclear era was further cemented due to the relatively high threshold for entry into the nuclear club, which allowed only a small and elite group of sophisticated countries in, vesting them with an element of control in balancing power. One of the most prohibitive barriers to entry was the lack of means – especially financially, with exorbitant costs linked to each step of nuclear development.

The threshold for entry into the cyber club is low. The comparison is especially stark when measuring cost as a barrier to entry. Technical know-how and expertise further tip the scales. Thus, cyberspace is relatively accessible for offensive purposes, with comparatively high prospects for success. Further, the infrastructure's basic insecurity along with the lack of an agreed-upon normative framework means the technology exists in a gray area – easily exploitable by states and individuals.

The evolution of cyber conflict has also led to a shift in strategic culture. Cyber and nuclear create and exist in very different strategic environments. Nuclear weapons favor revealing capabilities for the extension of stability, whereas cyber weapons favor concealing capabilities to maintain a degree of strategic surprise and offensive advantage. The fact that these realities now coexist – along with conventional weapons – represents the fundamental and distinct paradox of our day and age, often complicating interstate relations on multiple levels.

It is vital to ask if the nuclear age is then the right analogy, with all the questions it raises – about controlling weapons, deterrence, mutually assured destruction, the risks of proliferation, and the risks of destabilization. All the questions might be the same, but the answers vastly differ.

The emphasis here is on evaluating points of convergence or divergence in the strategic thinking of the nuclear and cyber eras. Is there significant overlap or are we now operating with two different road maps in two different dimensions? Do core principles still apply or must we work with a whole new set of assumptions? Can the same behavior be expected and can the known elements of defense and deterrence be accordingly extended? Deterrence has been an often confused and misunderstood concept in the bridge from nuclear to cyber – a point of departure, and thus, a critical place to begin.

While it may not be the perfect term, it lends a few valuable characteristics to cyber thinking. Of course, cyber deterrence is closely tied to political (and technical) attribution – a task that is less mysterious with nuclear weapons. Yet, there remains a facet of retaliation that serves the function of credible deterrence even in cyber conflict.

The elusive question is: what would it take to create credible deterrence in the cyber realm – where there is no visible count of warheads as in the nuclear realm, where there is no magical missile detection or catchall missile defense? The U.S. military, policymakers, and experts are still grappling with this question and there is not yet a clear-cut answer. As the thinking continues to evolve and refine, it is worth highlighting the disparity between the growing number of offensive cyber incidents and the lack of substantial responses to them. It is, in fact, difficult to name a significant cyber incident in the post-Stuxnet era where the offender paid a serious price. North Korea (and Russia) know this.

Undoubtedly, the strategic impacts of cyber use are not as well defined as nuclear use, wherein the calculus is straightforward and the effects as well as the consequences are unambiguous. When a state is deciding whether to deploy nuclear weapons, the decision makers unquestionably know there will be an equal response with devastating force. Retaliation does not come with a question mark, but an exclamation point. With cyber capabilities, on the other hand, the effects and the response to those effects are blurry and the calculus is complex.

One of the key fears surrounding any discussion on cyber and nuclear weapons is the security of the latter from attacks using the former. Theoretically speaking, this is a justified concern, as all systems using any type of computer software are subject to cyber attacks and manipulation. In fact, nuclear systems have always been vulnerable to attackers to some degree; cyber attacks simply present a new means, not a new challenge. Ultimately, nonetheless, the weakest link is the human behind the system.

Russia stands as a pivotal player in both the nuclear and cyber clubs. Despite much posturing over the years, Russia has refrained from actually using nuclear weapons with good reason. Russia is highly cognizant of the different factors at play in different conflicts with different adversaries. With the near enemy, central considerations are always the proximity and the likelihood for blowback and fallout. With the far enemy, Russian brass is well aware of the retaliation and escalation that would lead to mutually assured destruction. The story is different in the cyber domain, allowing the astute nation greater creativity and freedom. Russia has always been masterful at information operations with both external conflict and internal persuasion. Cyberspace merely facilitates an extension of this aptitude. And cyber operations harness a far wider array of options – both traditional and hybrid. This is Russia's gray area and it is becoming quite comfortable here.

China is another major player in both the nuclear and cyber clubs. With quite a different modus operandi than Russia, it is imperative to deconstruct China's approach on each track. Does Chinese doctrine form any explicit links between nuclear and cyber capabilities? Or, are the two treated as separate and distinct? Where Russia often lives in the gray area of hybrid operations, China conducts integrated and broad military operations. Cyber means are typically part and parcel with modern day

joint operations and seldom separated tactically or strategically. The goal is to get a head start with all the tools necessary to fight what China sees as the wars of the future: informatized wars.

It is worth recalling that China's motives in the cyber dimension have most frequently been fueled by a perceived imbalance when it compares itself to superpowers and competing nations. This has been especially true in terms of economic growth, which lends itself to cyber espionage – mainly in the corporate world. Yet this has not entirely precluded China from also pursuing space, civilian, or military targets – especially in seeking out information on adversary's policies, key personnel, and operational protocols. It all goes back to the integrated approach embedded in China's operational psyche.

North Korea's nuclear and cyber realities in this hybrid age deserve a closer look as well. On the nuclear front, the possession of such endangering weapons in the hands of a rogue state has been cause for concern from a U.S. standpoint – not to mention the risks of destabilization on the Korean peninsula and the fallout to the region, or the risks of proliferation to other rogue states and nonstate actors.

North Korea is also an interesting point of discussion when studying cyber as a full-scope weapon. Kim Jong-un seems astutely aware of this. Assessing some of North Korea's previous cyber attacks (such as the 2014 Sony Pictures hack) demonstrates an awareness of the advantages to using cyber means over conventional weapons or modes of attack. The latter would almost certainly guarantee retaliation. The North Koreans have calculated that cyber is in fact a great short-of-war weapon.

Cyberspace stands as its own domain for conflict to manifest, but it simultaneously impacts traditional domains and strategic thinking in unprecedented ways. This is especially palpable in the nuclear realm. The coinciding existence of these two strategically impactful elements of national security creates an uncertain environment that is still being explored and analyzed. This new era cannot – must not – be left to the wayside. It can irreversibly impact interstate relations, balance of power, and global stability.

Times have changed alongside priorities. The safeguards we took for granted may or may not be able to prevent nuclear proliferation, and we may yet see more aspirants or copy-cats to come. The emphatic lesson here is that while the nuclear problem lives on, the principles deriving from nuclear security may in fact be dying. In other words, nuclear threats may continue to remain paramount – making this a global security challenge we have not yet left behind.

The reduction of certainty has only been exacerbated by the tenuous nature of operating in the 'Wild West' of cyberspace, where no clear rules have ever existed. In fact, we seem to be living in an era where experimentation prevails and rules writ large are designed and adjusted casually for individual states' convenience, rather than formalized and cemented for mass observance. The absence of rules in the cyber domain has been a significant and complicating factor for both the nuclear and cyber spheres.

As cyberspace has become a fundamental dimension of modern life, it has touched every other facet of the current world order. It has altered the operating environment as well as the strategic culture that for decades underpinned global stability and security – from the nuclear to the conventional domain.

Where the nuclear era was defined by a degree of transparency, cyberspace is inherently opaque and invisible. It is tricky business to navigate through this dark space without any radar on what our adversaries are doing, how fast they are traveling, which direction they are going, or what their destination is. Add to this the reality that nuclear systems – facilities, weapons, command and control – could all be targets on the cyber highway. What is needed is greater communication and clarity in order to steer clear of everything from accidents and exploitations to provocations and incitements.

Introduction

On October 12, 2017, the National Committee on American Foreign Policy (NCAFP) led a cybersecurity conference entitled **Mutually Assured Disruption: Framing Cybersecurity in Nuclear Terms**. The objectives of the daylong conference centered around examining the overlap between the nuclear and cyber eras – both on strategic and tactical levels.

The nuclear era began long before there was an awareness that international relations would be strategically and irreversibly shifted. The technology outpaced the policymaking and even the awareness or understanding of consequences. The cyber domain has similarly materialized in global affairs at lightning speed. While vastly different in material ways, both nuclear and cyber weapons are strategic capabilities that tilt the battlefield with a different calculus than traditional means of warfare.

Nuclear weapons changed the strategic culture and interface among nation states. Where it was previously in a state's interest to hide its offensive capabilities, the advent of nuclear weapons reversed this logic for the purpose of deterrence. As states began to reveal their nuclear capabilities, the impacts reverberated for balance of power, global and regional stability, and the international order itself. It also created a certain distance in conflict decisions. Nuclear states were no longer held captive by the nearness of traditional battlefields. The threat of nuclear destruction was often sufficient to pause a conflict, or at least limit its uncontrollable escalation.

We have been operating in a world with these strategic assumptions since the Cold War. War by traditional means has not been erased. Yet mutually assured destruction continues to be a controlling parameter for battles and proxy conflicts in great power politics. The subtle arrival of the cyber era introduces different variables to the calculus. Now there is a return to concealing capabilities, without eliminating the distance element.

The strategic capabilities of states that can swiftly, covertly, and effectively maneuver in cyberspace are yet to be fully recognized. And the magnitude of their impact is yet to be fully realized. We are at a critical juncture to address and frame these issues now, while we still have the power to shape the discourse and the decision-making. There are lessons to be learned from all the nuclear era surprises that played out on the international stage. There are also important questions to be extended. Is this a reversal or a continuation of the strategic operating environment cemented during the rise of nuclear weapons? Or, is it an entirely different dimension altogether? Is it a coincidental or deliberate reality that several of the nuclear powers sit at the top of the cyber domain with the greatest capabilities, command, and control? Is cyber changing the decision calculus for conflict engagement, provocation, and/or aversion?

These are some of the critical debates and discussions that must be urgently addressed in order to keep the United States one step ahead in the cyber race, tactically and strategically, while also protecting its nuclear capabilities. While the era of mutually assured destruction is not yet to be archived, the new era of mutually assured disruption has already arrived.

With this understanding, the discussions at the conference aimed to explore the scope and effects of the emergent cyber era alongside the enduring nuclear era, and to begin building towards an understanding of the implications of this unique crossroads.

The conference was structured to have three sessions, including a keynote address and two concentrated roundtable discussions: "Strategic Lessons: From the Nuclear Era to the Cyber Domain" and "A New Decision Calculus: Real World Scenarios & Implications." Bringing together some of the

most knowledgeable experts in the two often-siloed fields of cyber and nuclear security was the key to effectively addressing such topics. Ten experienced thought leaders and practitioners from both ends of the spectrum shared their personal and professional insights – from government and policymaking institutions; academia and think tanks; private sector and technology firms. We were very fortunate to be able to tie the two main roundtable sessions together with a keynote address by a distinguished journalist who has been closely examining cybersecurity issues and policymaking, with an emphasis on the nuclear connection.

All of the roundtables followed Chatham House Rules in order to allow free and open discussion without attribution. While this binds the participants from divulging the identity of those making specific points, 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 independent research and analysis where relevant.

The chapter following the introduction ("Exclusivity or Accessibility: The Nuclear and Cyber Clubs") frames the subject at hand and contextualizes the discussion ahead. It probes some of the unique characteristics of the nuclear club in contrast with the cyber club, particularly in terms of exclusivity and accessibility. The next chapter ("The Nuclear-Cyber Interplay: Strategic and Tactical Considerations") delves deeper into a few of the most consequential issues when considering these two arenas – from strategic capabilities to bidirectional impact. The subsequent chapter ("Across the Chessboard: Adversarial Players") sets forth key observations on the mindsets of three focal adversaries in each arena and in the emerging hybrid space – namely, Russia, China, and North Korea. The final chapter ("Strategic Lessons: Looking Back and Thinking Ahead") pulls together some of the more pressing considerations and ideas drawn from the preceding analysis and the discussions at the conference. This report does not claim to have all the answers, but it poses some central questions and draws attention to some important issues to be grappled with if we are to live in the space between the nuclear era we knew and the cyber world we are beginning to know.

I. EXCLUSIVITY OR ACCESSIBILITY: THE NUCLEAR AND CYBER CLUBS

There are more than a few ways to frame a discussion on cyber issues alongside one on nuclear issues. The focus here is not on the analogy between the two as weapons in their own right – a debate that has had its moment in the limelight in many academic and policy circles. Here we explore two other facets connecting these otherwise isolated policy topics. One is the question of strategic continuance, for it is important that we examine the relevance of the strategic underpinnings of the nuclear era as they are shifting in the new cyber era. As policy thinkers and analysts, it is valuable to deconstruct and piece together shifts in the tectonic plates of the global order over the last few decades. In doing so, we must not ignore the technical shifts in capabilities, and so the other question is that of the intersection between cyber and nuclear capabilities, particularly on a tactical level. Both themes emerge, in different but equally relevant ways, throughout the analysis that follows.

Today, cyber and nuclear capabilities are entangled in complex and dangerous respects that are not discussed or addressed often enough. Both domains – and the specialists, experts, engineers, technologists, policymakers, and practitioners associated with each – exist and operate in siloed spaces. This makes it particularly difficult to bridge the communities and make each aware of the threats against or concerns of the other. For this reason, dialogues like this are not only highly valuable, but critical.

The nuclear era spurred its own rules of the game – both implicit and explicit – because of the existential risks deployment would pose to the entirety of mankind. Thus, even nations with very different interests came to follow a

certain code of conduct, recognizing that all other interests were secondary to survival. This led to a decades-long continuance of the principle of Mutually Assured Destruction, which endured through the Cold War. While great powers such as the United States and the Soviet Union continued to push conflict to the brink in other domains, there remained a certain stability at the strategic level.

The stability of the nuclear era was further cemented due to the relatively high threshold for entry into the nuclear club, which allowed only a small and elite group of sophisticated countries in, vesting them with an element of control in balancing power. One of the most prohibitive barriers to entry was the lack of means – especially financially, with exorbitant costs linked to each step of nuclear development.

CYBER AND NUCLEAR CAPABILITIES ARE ENTANGLED IN COMPLEX AND DANGEROUS RESPECTS THAT ARE NOT DISCUSSED OR ADDRESSED OFTEN ENOUGH. BOTH DOMAINS – AND THE SPECIALISTS, EXPERTS, ENGINEERS, TECHNOLOGISTS, POLICYMAKERS, AND PRACTITIONERS ASSOCIATED WITH EACH – EXIST AND OPERATE IN SILOED SPACES. THIS MAKES IT PARTICULARLY DIFFICULT TO BRIDGE THE COMMUNITIES AND MAKE EACH AWARE OF THE THREATS AGAINST OR CONCERNS OF THE OTHER.

With the growth of cyber, we have seen a new era and a new environment taking shape. The emergence of cyberspace as a domain for human activity towards the end of the Cold War essentially added a new dimension to interstate relations.

Notably, cyberspace is a sphere outside of state regulation. The internet itself is outside the formalized system of institutions that have historically been tasked with regulating communications and related technology. The global digital economy is built on its foundation, which leads to a cascade of mutual dependencies and vulnerabilities.

The dark secret of the internet is that it was built for resilience, not security, and it still operates in this way. Any steps to secure the internet today are fundamentally just patches. This is not simply a theoretical assessment; we have seen the effects of this play out on the front pages of major newspapers over the past decade. We have witnessed large scale losses of data by multinational corporations such as Equifax as well as government divisions like the Office of Personnel Management. We have also witnessed more sophisticated and enduring attacks against critical infrastructure, threatening to alter the very ways in which modern society operates – in Ukraine, for instance.

Unlike with the nuclear club, the threshold for entry into the cyber club is low. The comparison is especially stark when measuring cost as a barrier to entry. Where a sizable nuclear program can cost billions of dollars for materials, production, delivery systems, and maintenance, cyber offensive programs can cost as little as a few computers. Technical know-how and expertise further tip the scales, as the physics and engineering required for nuclear programs is far more difficult to acquire, cannot be self-taught or easily transferred, and thus remains in rare supply. Cyber tools are far easier to learn and the knowledge is far more easily available on a foundational level. All of this makes cyberspace relatively accessible for offensive purposes, with comparatively high prospects for success. Further, the infrastructure's basic insecurity along with the lack of an agreed-upon normative framework means the technology exists in a gray area – one that is easily exploitable by states and individuals.

The evolution of cyber conflict has also led to a shift in strategic culture. Cyber and nuclear create and exist in very different strategic environments. Nuclear weapons favor

revealing capabilities for the extension of stability, whereas cyber weapons favor concealing capabilities to maintain a degree of strategic surprise and offensive advantage. The fact that these realities now coexist – along with conventional weapons – represents the fundamental and distinct paradox of our day and age, often complicating interstate relations on multiple levels.

Nuclear systems have vulnerabilities through the cyber dimension, especially when it comes to supply-chain attacks such as Olympic Games. Cyber systems are also uniquely vulnerable to nuclear impacts. Beyond the blanket effects nuclear weapons would have on all systems through radiological or blast impacts, there is also the risk of electromagnetic pulses (EMPs). One of the less discussed and more serious considerations when it comes to North Korea's development of thermonuclear weapons is precisely their ability to generate and utilize EMP capabilities. EMPs, in fact, are looking like a more probable use of North Korean nuclear capabilities.

Unlike the mass-scale use of nuclear weapons that we fear being deployed towards the loss of lives and the destruction of cities or infrastructure, EMPs can be uniquely employed with precise application to critically damage or disable civilian infrastructures across a wide area and for a very long period of time. This is particularly true for systems dependent on electrical infrastructure, which is not a small category in modern society. For instance, there are a few highly critical points along the Eastern seaboard of the United States that are dependent on large scale transformers, which cannot be replaced easily. Damaging these – especially simultaneously – would effectively cripple a large portion of the Eastern portion of the U.S., with consequences rippling across other regions of the country that are closely dependent for security and economic activity. Given the lag time to rebuild, if the magnitude of the attack is high enough, growth and livelihood could be compromised for several years. Thus, one argument is that the principal threat of North Korean progress with nuclear development is not mass use of the weapons in a traditional sense, but rather their advanced ability to generate EMPs for harm.

Perhaps one of the unintended consequences of this discovery, if North Korea goes in this direction, is that it could inadvertently lower the threshold for other aspiring nuclear states, for whom developing a large-scale arsenal is not an achievable goal – the kind we saw during the Cold War era for deterrence purposes and the kind we traditionally see with nuclear powers. If destruction can be so impactful with alternate uses, however, massive arsenals will no longer be necessary to disrupt modern society. Impacts would reach across interconnected categories ranging from food security to the broader digital economy.

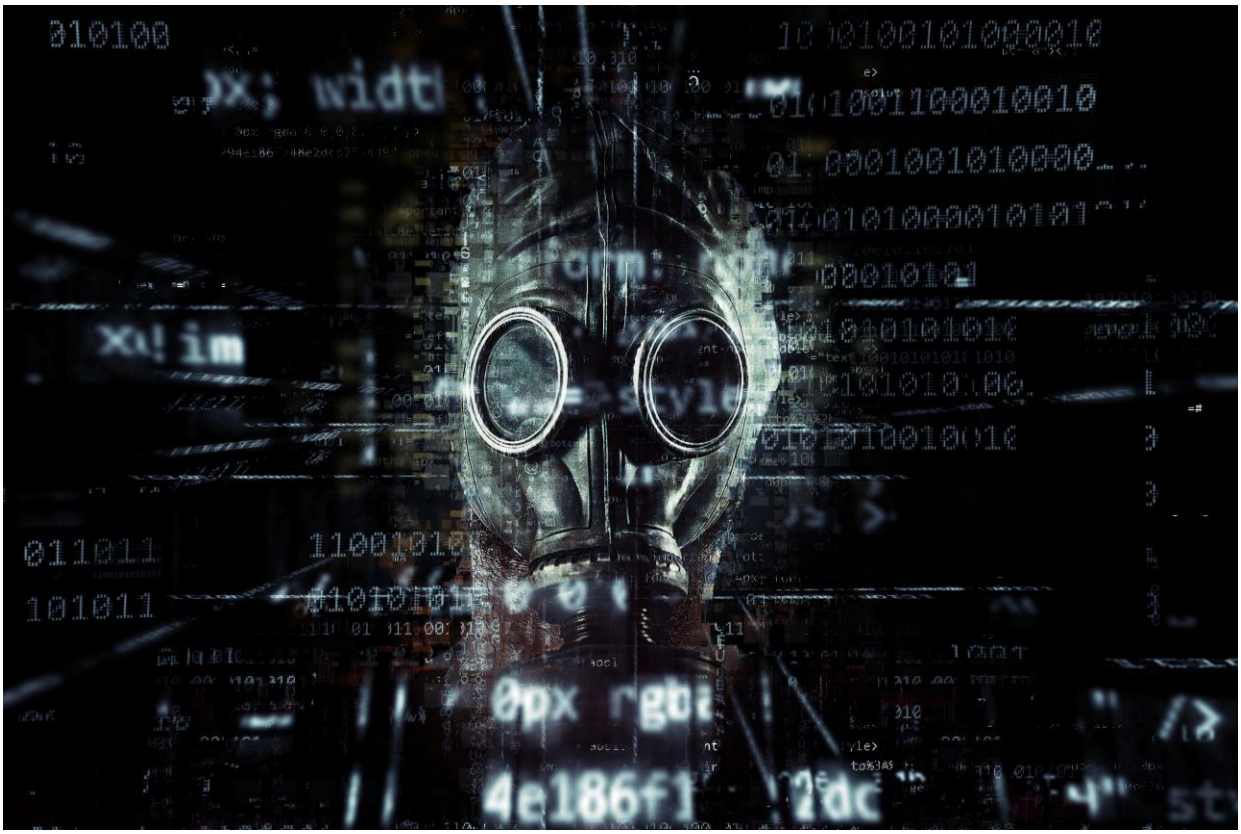
THE EVOLUTION OF CYBER CONFLICT HAS LED TO A SHIFT IN STRATEGIC CULTURE. CYBER AND NUCLEAR CREATE AND EXIST IN VERY DIFFERENT STRATEGIC ENVIRONMENTS. NUCLEAR WEAPONS FAVOR REVEALING CAPABILITIES FOR THE EXTENSION OF STABILITY, WHEREAS CYBER WEAPONS FAVOR CONCEALING CAPABILITIES TO MAINTAIN A DEGREE OF STRATEGIC SURPRISE AND OFFENSIVE ADVANTAGE. THE FACT THAT THESE REALITIES NOW COEXIST – ALONG WITH CONVENTIONAL WEAPONS – REPRESENTS THE FUNDAMENTAL AND DISTINCT PARADOX OF OUR DAY AND AGE, OFTEN COMPLICATING INTERSTATE RELATIONS ON MULTIPLE LEVELS.

There is, nonetheless, an upside to the existing capabilities associated with EMPs: they are also a potentially appealing response to North Korea and other rogue nuclear states (or aspiring states) by the U.S. and its partners. This response is certainly to be explored, as joint EMP-cyber operations versus such rogue states may turn out to be one of the best ways of

ensuring the weapons cannot be deployed or utilized.

In these ways, EMPs are an interesting factor that further complicate the dual cyber and nuclear eras we live in today. In short, cyber and nuclear have become entangled, and entangled quite precariously at that. We live in an age where we now have a clash of strategic cultures – of a simultaneous demand for concealment and revealment. We live in a time with a lowered threshold for the use of cyber weapons, and paradoxically, the development of nuclear ones.

II. THE NUCLEAR-CYBER INTERPLAY: STRATEGIC AND TACTICAL CONSIDERATIONS



A. On the Dangers of Analogy

As technologists and policymakers race to define and comprehend the way their worlds intersect in cyberspace, a multitude of analogies emerge. With its intangible nature – it cannot be seen or outlined or grasped – the innate tendency is to try to compare it to that which is familiar in the physical world. This takes a different form depending on one's vantage point. Much cyber terminology has been borrowed from medical jargon – malware, viruses, worms, and so forth. Legal experts try to apply concepts from the laws of war – sovereignty or proportionality, for instance – when trying to ascertain the rules of cyber conflict. However, the boundless nature of cyberspace overwrites and undermines the idea of sovereignty, with its borders and clearly marked territories.

From the vantage point of politicians, it is beneficial to utilize analogies that sound alarms and garner attention – whether to raise awareness or support and funding. Take the term 'Cyber Pearl Harbor,' stirring up images of one of the worst attacks in American history. The catchphrase has also been used in questioning if the 2017 Russian hacks equate to our Cyber Pearl Harbor. But we have not seen a Cyber Pearl Harbor. And if one has to ask, the answer is probably 'no.'

Beyond analogies between cyber weapons and conventional weapons, there is no shortage of comparisons to the nuclear era as well. Initially this seems to be a stretch of the imagination, but with alarmist visions abounding – of electric

grids shut down, nationwide blackouts, and Cyber Pearl Harbor, to name a few – it has become a hot topic of debate. Taking a step back, it is vital to ask if the nuclear age is then the right analogy, with all the questions it raises – about controlling weapons, deterrence, mutually assured destruction, the risks of proliferation, and the risks of destabilization. All the questions might be the same, but the answers vastly differ.

An entire book could be written on the myriad ways in which the two eras overall diverge, or the countless ways the weapons themselves differ operationally. It is relevant here to observe that the very origin stories and evolutionary trajectories of the two capabilities have been entirely in contrast to each other. This matters because it points to their reason for coming into existence – their raison d'être.

The emphasis here is not on analogies in a broad sense; rather, the focus is on evaluating points of convergence or divergence in the strategic thinking of the nuclear and cyber eras. Is there significant overlap or are we now operating with two different road maps in two different dimensions? Do core principles still apply or must we work with a whole new set of assumptions? Can the same behavior be expected and can the known elements of defense and deterrence be accordingly extended? Deterrence has been an often confused and misunderstood concept in the bridge from nuclear to cyber – a point of departure, and thus, a critical place to begin.

AN ENTIRE BOOK COULD BE WRITTEN ON THE MYRIAD WAYS IN WHICH THE TWO ERAS OVERALL DIVERGE, OR THE COUNTLESS WAYS THE WEAPONS THEMSELVES DIFFER OPERATIONALLY. THE VERY ORIGIN STORIES AND EVOLUTIONARY TRAJECTORIES OF THE TWO CAPABILITIES HAVE BEEN ENTIRELY IN CONTRAST TO EACH OTHER. THIS MATTERS BECAUSE IT POINTS TO THEIR REASON FOR COMING INTO EXISTENCE – THEIR RAISON D'ÊTRE.

B. On Deterrence

Talk to someone not submerged in policy analysis, and 'deterrence' is just a word – easily interchangeable with 'hindrance' or 'discouragement.' Simple enough. In our world, though, it is a loaded word – historically packed with nuclear references. Recall that deterrence theory emerged during the Cold War within the framework of game theory. Where unilateral deterrence initially gave the U.S. the upper hand with a larger nuclear arsenal, the Soviets ultimately built up their own arsenal to give way to mutual deterrence. This was further cemented as second-strike capabilities advanced on both sides. In this era, retaliation and mutually assured destruction were the guarantors of stability via credible deterrence.

This concept has been pushed and squeezed into cyber jargon in recent years, where it takes on a slightly different meaning – not least because of the very dissimilar weapons and domains in which they operate. Some that have lived through Cold War struggles or witnessed them first hand in a policy role refuse to part with their ownership of the term 'deterrence,' but there may be some validity to its application in cyber conflict. While it may not be the perfect term, it lends a few valuable characteristics to cyber thinking. For instance, when mapping out a deterrence timeline it is valuable to extend the traditional 'left of boom' and 'right of boom' concepts to left or right of virtual boom. Of course, cyber deterrence is closely tied to political (and technical) attribution – a task that is much less mysterious with nuclear weapons. Yet, there remains a facet of retaliation that serves the function of credible deterrence even in cyber conflict. The key is to observe the context of use, as the meaning rests entirely in the context.

The cross-section of the cyber and nuclear eras returns us to the original question of deterrence. What is the primary value of traditional nuclear deterrence today, if any?

Who and what are we actually trying to deter, and how? The answers are not simple, but deterrence still has immense value in maintaining global nuclear security. There are four key principles with deterrence: (1) The U.S. must continue to demonstrate leadership and commitment to arms control and a nonproliferation regime, especially with nuclear weapons. Initiatives like START and NPT continue to hold great weight across the globe. (2) Deterrence can help prevent accidental or unauthorized access to and use of nuclear weapons. (3) Deterrence is still effective as a tool to avert strategic attacks on U.S. soil as well as against troops abroad or our allies and partners. Along these same lines, deterrence also discourages retaliatory or second-strike attacks. (4) If deterrence fails in any single instance, the U.S. and its partners must remain prepared to respond with strong military readiness in order to prevail in the conflict and then restore deterrence.

Additionally, there are at least two categorical approaches to nuclear deterrence: (1) deterrence by denial and (2) deterrence by entanglement. Deterrence by denial makes it so difficult and costly for adversaries that they are ultimately deterred from pursuing nuclear ambitions. Sanctions are a well-documented iteration of this approach – whether economic sanctions, military sanctions, or diplomatic sanctions. Deterrence by entanglement follows on the heels of the post-World War II era, in which states are now so deeply interconnected and mutual interests are so inextricably aligned, that causing destruction to an enemy may have boomerang effects on one's own state. Beyond human security, the global economy and natural environment are so widely shared that global nuclear fallout would not only affect the target but surrounding states and interconnected regions.

Two thorny issues with nuclear deterrence are the 'who' and 'how' – both of which have proven to shift over time. The states pursuing nuclear weapons and their respective means of acquiring materials or expertise have not remained static, consistent, or predictable. Iran's approach, for one, has been drastically divergent from North Korea's path. Of course, the U.S. has sufficient nuclear capabilities to deter longstanding threats such as China and Russia. We worry less, too, about our nuclear allies – others in the traditionally constructed nuclear club. However, there is no guarantee that some members of that club would never be inclined to proliferate their technology or expertise. There is also no guarantee that other states will not develop nuclear weapons of their own accord, without much regard for the U.S. or the nuclear club. One only has to look to India and Pakistan for an episode of this saga.

ADMIRAL MICHAEL ROGERS HAS SUMMED UP WHAT COULD BE THE FIRST NOTCH IN CYBER DETERRENCE THINKING: IT MUST BE MADE KNOWN, TO INDIVIDUALS AND STATES ALIKE, THAT ANYONE WHO PROVOKES OR CHALLENGES THE U.S. IN THE CYBER DOMAIN WILL FACE SERIOUS CONSEQUENCES. IF THAT IS NOT CLEARLY UNDERSTOOD AND RECOGNIZED, WE WILL HAVE FAILED AT OUR JOB.

A final murky area with deterrence is knowledge. In this current crossover environment of equal appeal between revealing and concealing any offensive capabilities, we are no strangers to denial and deception. Where the Cold War bipolarity kept the Soviet Union and the U.S. on track to reveal their pursuit of certain capabilities (even if not their depth) – whether in nuclear arms race or the outer space race, states today seem to calculate no real gain from revealing their pursuits during early development phases. Iran and North Korea are perfect examples.

A topic demanding further analysis is the question of which of these truths about nuclear deterrence can be cross-applied to cyber deterrence. Admiral Michael Rogers (Director of the National Security Agency and U.S. Cyber

Command) has summed up what could be the first notch in cyber deterrence thinking: it must be made known, to individuals and states alike, that anyone who provokes or challenges the U.S. in the cyber domain will face serious consequences. He has candidly remarked that if that is not clearly understood and recognized, we will have failed at our job. Today, we have accomplished much behind closed doors as a nation – in cyber offense and cyber defense – but when it comes to cyber deterrence, we still have some work to do.

C. On Strategic Capabilities

While nuclear force fits the traditional paradigm of a strategic weapon, cyber forces can also be strategic – depending on the means of attack and the targets themselves as well as the overarching objectives and the context or timing. The means and the target matter in determining efficacy to a great degree. For example, cyber methods were strategically effective in rolling back Iran's advancement of nuclear development via the use of Stuxnet. Similarly, the Russian hack of U.S. political parties' data was successful in generating strategic and psychological effects. In both cases, the precise timing and operational means were the formula for success in impacting the specified targets and meeting the strategic objectives. Had Operation Olympic Games against the Natanz uranium enrichment plant in Iran been conducted at a different time, it may not have been as impactful in sabotaging Iran's nuclear progress at the time – potentially even rendering the entire mission an abject failure. Had Russia hacked and leaked its data at a later date, it would perhaps seem less relevant to the media and the public – certainly having less front-page sway on voters ahead of the U.S. presidential election. It is worth noting that Russia is categorically masterful in its use of cyber tools towards strategic ends – especially in information warfare campaigns. This is not a coincidence of history if one observes the pattern of Russia's emphasis on information as a weapon throughout various generations of warfare.

WHEN A STATE IS DECIDING WHETHER TO DEPLOY NUCLEAR WEAPONS, THE DECISION MAKERS UNQUESTIONABLY KNOW THERE WILL BE AN EQUAL RESPONSE WITH DEVASTATING FORCE. RETALIATION DOES NOT COME WITH A QUESTION MARK, BUT AN EXCLAMATION POINT. WITH CYBER CAPABILITIES, THE EFFECTS (AND THE RESPONSES TO THOSE EFFECTS) ARE MUCH MORE BLURRY AND THE CALCULUS IS MUCH MORE COMPLEX.

Undoubtedly, the strategic impacts of cyber use are not as well defined as nuclear use, wherein the calculus is straightforward and the effects as well as the consequences are unambiguous. When a state is deciding whether to deploy nuclear weapons, the decision makers unquestionably know there will be an equal response with devastating force. Retaliation does not come with a question mark, but an exclamation point. With cyber capabilities, on the other hand, the effects (and the responses to those effects) are much more blurry and the calculus is much more complex. The evolution of systems is also less static with cyber operations. Years can be spent gaining access to a system and monitoring a target system without any guarantee that all the reconnaissance will not be moot with a simple update to the system.

D. On the Security of Nuclear Systems Against Cyber Attacks

One of the key fears surrounding any discussion on cyber and nuclear weapons is the security of the latter from attacks using the former. Theoretically speaking, this is a justified concern, as all systems using any type of computer software are subject to cyber attacks

and manipulation. In fact, nuclear systems have always been vulnerable to attackers to some degree; cyber attacks simply present a new means, not a new challenge.

The complex and often age-old machinery of original nuclear systems is certainly vulnerable to the sophisticated cyber attacker. It is especially important to understand that most successful cyber attacks of any kind exploit vulnerabilities that have not yet been patched. In other words, known problems are the best way in.

It is important not to limit the range of cyber attacks to simply hacking – which is too often the restricting term used. Cyber attacks span a vast spectrum – from nuisance to espionage to data theft; and cyber operators have a divergent set of intentions and capabilities – from disruption to damage to destruction. We must also consider the way these factors intersect differently from state to nonstate actors.

THE U.S. MAY TODAY BE AT THE FOREFRONT OF CYBER TECHNOLOGIES, BUT THERE IS NO GUARANTEE IT WILL REMAIN SO IN THE LONG RUN. THIS IS A NEW KIND OF ARMS RACE – ONE THAT REVERBERATES ACROSS MULTIPLE DOMAINS AND MULTIPLE DIMENSIONS.

When zooming in on the threat to nuclear systems, it is perhaps helpful to boil all this down to two distinct waves: (1) disabling attacks – designed to hinder a nuclear system from functioning properly, and (2) enabling attacks – designed to facilitate activity such as a missile launch.

Moreover, the modernization of weapons poses its own challenges with new areas of potential weakness and new angles of potential intrusion. The greater the complexity of a system, the trickier the diagnosis of a vulnerability.

Ultimately, as is true with most cyber-enabled systems, the weakest link is the human behind the system. The weakest link is often not the system itself, but the human operator handling it. Several of the most sophisticated cyber attacks we have seen to date have taken advantage of the human being on the other end as the easiest point of access and the best attack vector.

A great deal of the cyber challenge lies in information security with threats of espionage, loopholes, and vulnerabilities. This is only complicated by the difficulties of instantly knowing if a system has been breached.

The U.S. may today be at the forefront of cyber technologies, but there is no guarantee it will remain so in the long run. This is a new kind of arms race – one that reverberates across multiple domains and multiple dimensions.

E. On the Vulnerability of Civilian Infrastructure from Nuclear Versus Cyber Threats

It has long been abundantly clear that civilian infrastructure is susceptible and vulnerable to nuclear attacks in the most destructive ways. What demands more clarity is the understanding of their vulnerability to cyber attacks – whether for destruction or disruption. We are nowhere near grasping the extent of the threat in the cyber realm. Still, there has been enough surveying to posit that critical civilian infrastructure could be catastrophically affected by cyber means.

Take EMPs as a point of discussion. Most civilian infrastructure has no safeguards against EMPs. Then there is the supply chain issue, wherein spare parts availability, procurement, and replacement could amplify the length of time, and thus, the effects of the damage as well. Further, like nuclear systems that often employ decades-old machinery, civilian

infrastructure is also susceptible to hidden legacy vulnerabilities. Not every node is readymade in the U.S. There would be a dependency for several parts to come from factories in states like China, which places recovery in potentially uncooperative hands. For these reasons access to quick replacements is a bigger problem than most would realize.

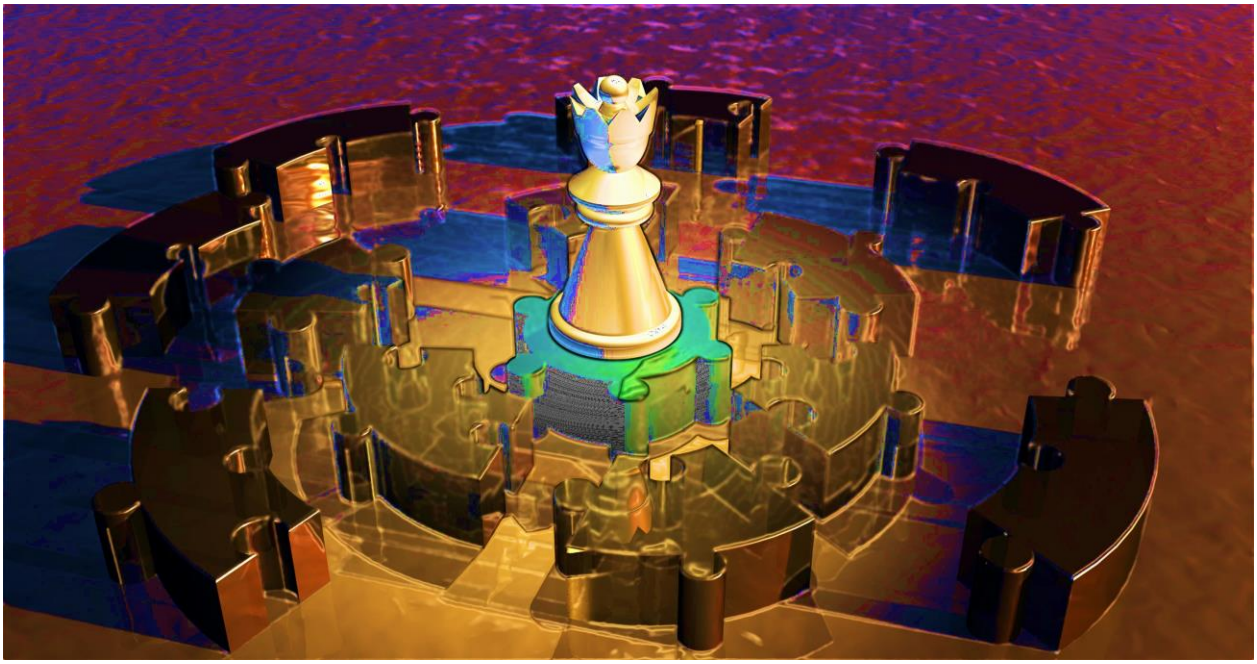
One key factor in the U.S. is that civilian infrastructure is frequently owned and/or operated by the private sector, with their own development, planning, and maintenance criteria. Legally, therefore, the U.S. government itself does not have much authority to implement certain cyber standards or protocols for protection and updates. Private ownership and operation similarly means that detection and monitoring are not uniform and cannot be mandated to be carried out in a certain way. For some corporations that do not believe cyber attacks are a major disruptive risk against such targets, the lack of tangible evidence might lead to lowered vigilance and a lack of awareness that malicious actors are even accessing their systems. Essentially, if there is no direct damage, there may be no vigilance toward potential intrusions and no emphasis on reinforcement, patches, or vulnerability protection. This only further elongates the list of government responsibilities, as defense infrastructure must now also account for the safety of civilian vulnerabilities to an extent.

FOR SOME CORPORATIONS THAT DO NOT BELIEVE CYBER ATTACKS ARE A MAJOR DISRUPTIVE RISK AGAINST, THE LACK OF TANGIBLE EVIDENCE MIGHT LEAD TO LOWERED VIGILANCE AND A LACK OF AWARENESS THAT MALICIOUS ACTORS ARE EVEN ACCESSING THEIR SYSTEMS. ESSENTIALLY, IF THERE IS NO DIRECT DAMAGE, THERE MAY BE NO VIGILANCE TOWARD POTENTIAL INTRUSIONS AND NO EMPHASIS ON REINFORCEMENT, PATCHES, OR VULNERABILITY PROTECTION.

With the growing number of important and interdependent urban hubs relying on cyber connectivity to operate smoothly, it is too early to categorically exclaim that cyber is not in fact a strategic threat to civilian infrastructure.

If there is a bright side, it is that a cyber attack on civilian infrastructure would not be as existential or as severe as a nuclear attack on the same. People will not die by the thousands. It will not be nuclear Armageddon. But that does not mean it is not a grave threat that comes with the potential for massive disruption and destruction.

III. ACROSS THE CHESSBOARD: ADVERSARIAL PLAYERS



This work, "3D Chess & Moving Parts" by Simran R. Maker is a derivative of "Puzzle, Lady, Chess Piece" by PIRO4D used under CC0.

A. On the Russian Mindset

It would be imprudent not to place a magnifying glass on Russia in such a discussion, since it stands as a pivotal player in both the nuclear and cyber clubs. Several questions loom large here, but a few key inquiries take precedence. First, we must dissect how Russian thinking on nuclear and cyber doctrine have evolved since the end of the Cold War. Next, we must inspect some of the doctrinal pillars shared by both domains.

From a military perspective, there are a few tenets worth highlighting. One key concept for the Russian brass is that of 'equal security,' wherein strategic stability and balance of forces can only be achieved by quantifying and leveling out the number and types of weapons on both sides. This is particularly true in the nuclear sphere, as the U.S. has witnessed time and time again. In the Cuban Missile Crisis, reducing Russian missiles in Cuba depended precisely on an equal show of faith with U.S. missiles being reduced in Turkey. This strict adherence to the 'equal security' principle in the nuclear arena begs the question: how do we establish equal security in the cyber domain, especially given that this domain favors covert and concealed capabilities?

The way Russians have historically viewed information operations is divided into two parts that translate loosely to 'information technical' and 'information psychological.' Today, we can easily see the integration of the two elements in Russian thinking.

A revealing prioritization of concerns surfaced at a recent meeting aimed at furthering information security talks with the Russians. The Russian's top concern was escalation models in the cyber domain, followed by civilian infrastructure second, definitions third, and codes of conduct fourth. Interestingly, industrial espionage was tenth on the list, all the way at the bottom below counterterrorism.

THIS STRICT ADHERENCE TO THE 'EQUAL SECURITY' PRINCIPLE IN THE NUCLEAR ARENA BEGS THE QUESTION: HOW DO WE ESTABLISH EQUAL SECURITY IN THE CYBER DOMAIN, ESPECIALLY GIVEN THAT THIS DOMAIN FAVORS COVERT AND CONCEALED CAPABILITIES?

Area studies experts focusing on Russia translate Russia's perception of information warfare by the military as activity carried out with the overlapping priorities of damaging systems, processes, resources, and infrastructure. The secondary objective is undermining political and social systems, while destabilizing the government and society writ large. Finally, there is an intent to tilt or coerce the targeted opponent's decision-making calculus to Russia's advantage.

If one were to postulate a scenario against the U.S., the first step would be intensifying pressure with the use of information – as leverage, for instance. The aim would be to try to disorient the country's political leadership first. The next hypothetical step would be conducting cyber operations while simultaneously deploying special operations units. Then Russia could default back to classic military operations and large scale information operations across the country as a final blow. This is one possible way for things to play out, knowing Russia's proclivity for hybrid multi-stage multi-dimension attack plans. This is not to say every instance will resemble this option, nonetheless.

RUSSIA HAS ALWAYS BEEN MASTERFUL AT INFORMATION OPERATIONS. CYBERSPACE MERELY FACILITATES AN EXTENSION OF THIS APTITUDE. AND CYBER OPERATIONS HARNESS A FAR WIDER ARRAY OF OPTIONS – BOTH TRADITIONAL AND HYBRID. THIS IS RUSSIA'S GRAY AREA AND IT IS BECOMING QUITE COMFORTABLE HERE.

Despite much posturing over the years, Russia has refrained from actually using nuclear weapons with good reason. Russia is highly cognizant of the different factors at play in different conflicts with different adversaries. With the near enemy, central considerations are always the proximity and the likelihood for blowback and fallout. With the far enemy, Russian brass is well aware of the retaliation and escalation that would lead to mutually assured destruction.

The story is different in the cyber domain, allowing the astute nation greater creativity and freedom. Russia has always been masterful at information operations with both external conflict and internal persuasion. Cyberspace merely facilitates an extension of this aptitude. And cyber operations harness a far wider array of options – both traditional and hybrid. This is Russia's gray area and it is becoming quite comfortable here.

B. On the Chinese Mindset

China is another major player in both the nuclear and cyber clubs. With quite a different modus operandi than Russia, it is imperative to deconstruct China's approach on each track. Does Chinese doctrine form any explicit links between nuclear and cyber capabilities? Or, are the two treated as separate and distinct? Educated inferences and operational patterns suggest that cyber is not a tool divorced from any other critical arena for China. Where Russia often lives in the gray area of hybrid operations, China conducts integrated and broad military operations. Cyber means are typically part and parcel with modern day joint operations and seldom separated tactically or strategically.

This assessment is further underscored by China's 2015 establishment of its Strategic Support Force. Experts have described the official mandate of this new military arm as covering space, cyber, and electronic or

electromagnetic warfare as well as strategic-level information support for joint operations. The goal is to get a head start by equipping a force with all the tools necessary to fight what China sees as the wars of the future: informatized wars. If that sounds slightly vague and intertwined, that is because it is for the moment. The new force has been cloaked in secrecy with few details forthcoming and little clarity surrounding its structure.

THE GOAL IS TO GET A HEAD START WITH ALL THE TOOLS NECESSARY TO FIGHT WHAT CHINA SEES AS THE WARS OF THE FUTURE: INFORMATIZED WARS. CHINA IS MORE INTERESTED IN OFFENSIVE CYBER OPERATIONS AS ONE OF THE MANY METHODS TO DEFENDING ITS OVERALL NATIONAL SECURITY, THUS APPLYING A MODEL OF NATIONAL DEFENSE VIA CYBER OFFENSE.

Along these same somewhat fuzzy lines, China seems more interested in offensive cyber operations as one of the many methods to defending its overall national security. China thus applies a model of national defense via cyber offense, and for China, the benefits of cyber tools resound far beyond the cyber domain itself. What is clear in examining Chinese doctrine, historically and at present, is that China frames information operations in a much broader context and does not restrict them to cyberspace alone.

Interestingly, the Chinese word for deterrence can be interpreted as 'deterrence' or 'dissuasion' as well as 'coercion,' or as the synthesis of these. This dramatically differentiates Chinese doctrine from Western thinking on such issues. For China, deterrence or dissuasion and coercion are not clearly demarcated or isolated tactics. They sit on the same continuum, often overlapping. This was inarguably important in shedding light on China's nuclear strategy, but it remains relevant in the cyber-nuclear purgatory era of today.

With that said, China's nuclear model is rather divergent from Russia's model of 'equal security.' China adheres to standards of 'minimal deterrence.' In nuclear strategy, this is the principle by which a state maintains just enough nuclear weapons to deter an adversary attack or first strike. It thus falls on the more defensive end of the nuclear spectrum.

It is worth recalling that China's motives in the cyber dimension have most frequently been fueled by a perceived imbalance when it compares itself to superpowers and competing nations. This has been especially true in terms of economic growth, which lends itself to cyber espionage – mainly in the corporate world. Yet this has not entirely precluded China from also pursuing space, civilian, or military targets – especially in seeking out information on adversary's policies, key personnel, and operational protocols. It all goes back to the integrated approach embedded in China's operational psyche.

A pivotal shift occurred in the Chinese strategic position after the global WannaCry attack in May 2017. China began to view itself as a victim, which led a noticeably greater open-mindedness in terms of cyber cooperation and participation across international lines – including with the United Nations Group of Governmental Experts. This may lend itself to hopes that China may yet become a key state to actively partake in creating and upholding international cyber norms going forward. There is already a leaning towards at least one key standard: refraining from attacks against civilian infrastructure during peacetime.

C. On the North Korean Predicament

On numerous levels, analysts have been struggling to comprehend North Korea for years. Does it measure survival and existential needs the same way other nations do, or does it calculate its odds based on entirely different

variables unknown to us? North Korea's pursuit of a nuclear arsenal skews the picture further. Some area experts argue that despite conjecture to the contrary, the nation is actually quite rational and its nuclear aspirations exist precisely to ensure its survival. Regardless, the possession of such endangering weapons in the hands of a rogue state has been cause for concern from a U.S. standpoint – not to mention the risks of destabilization on the Korean peninsula and the fallout to the region, or the risks of proliferation to other rogue states and nonstate actors. This explains much about the fixation and persistence on denuclearization efforts. The carrot and the stick have been extended multiple times in recent history – talks, sanctions, talks, pressure, rinse, repeat.

Assume for a moment that North Korea is in fact a rational actor, and consider for an instant the example-setting in the current environment. Even if the North Koreans were contemplating a negotiated solution, the recent reneging of the Iran agreement would leave them with questions on trust and assuredness. We could categorically point back to more than a few times they have violated agreements, walked away from negotiations, or reversed the direction of cooperation and muted progress. But this sort of finger-pointing would only beget more of the same, and it will not engender any progress of its own. Nevertheless, this remains a likely cycle in the near-term. With this very real possibility that the U.S. and its partners will make little headway on the North Korean nuclear front for the time being, it is imperative to examine how North Korea is utilizing its nuclear and cyber capabilities as well as how the United States may be using cyber weapons against North Korea's nuclear program.

1. On North Korea's Use of Cyber Weapons

North Korea is an interesting point of discussion when studying cyber as a full-scope weapon. Kim Jong-un seems astutely aware of this. The 2014 Sony Pictures hack is a case in point. Operationally, there were at least a few alternative methods for achieving the end goal without a cyber attack. Conventional means – bombing Sony, for instance – may have indeed destroyed 70 percent of the computer systems just the same. The North Koreans calculated, however, that a brazen and pronounced attack like that would almost certainly guarantee retaliation. If for nothing else, no U.S. president would be able to avoid a heavy-handed response to the provocative images of Hollywood up in flames. Likely having gamed this out, Kim Jong-un went the cyber route and achieved fundamentally the same result sans blowback.

THIS IS THE FUNDAMENTAL 'WHAT IF' HYPOTHETICAL THAT WILL SHAPE DETERRENCE THINKING IN THE CYBER REALM GOING FORWARD. THE SILENT WORD IN DETERRENCE THEORY IS THE WORD 'CREDIBLE', AND IT SPEAKS VOLUMES. THE ELUSIVE QUESTION IS: WHAT WOULD IT TAKE TO CREATE CREDIBLE DETERRENCE IN THE CYBER ARENA – WHERE THERE IS NO VISIBLE COUNT OF WARHEADS AS IN THE NUCLEAR SPHERE; WHERE THERE IS NO MAGICAL MISSILE DETECTION OR CATCHALL MISSILE DEFENSE?

The lesson for the North Koreans was a reinforcement that cyber is in fact a great short-of-war weapon. The lesson for the U.S. was that we have not yet figured out the deterrence part of the cyber equation. Revisiting the issue of deterrence – which is very much tied to the North Korea discussion – an insightful thought exercise fits here: had President Obama chosen to retaliate to previous egregious cyber attacks, would that have altered the calculus for North Korea's 2014 Sony hack? Or, had the U.S. retaliated more seriously to any previous cyber attack, would Russia have thought twice before launching its string of hacks in recent years –

from the State Department in 2014 to the Joint Chiefs of Staff in 2015 and ultimately the election campaign hack in 2016? (For more background on Russia's 2016 hack, see "New Frontier in Defense: Cyberspace and U.S. Foreign Policy.")

This is the fundamental 'what if' hypothetical that will shape deterrence thinking in the cyber realm going forward. The silent word in deterrence theory is the word 'credible', and it speaks volumes. The elusive question is: what would it take to create credible deterrence in the cyber arena – where there is no visible count of warheads as in the nuclear sphere; where there is no magical missile detection or catchall missile defense? The U.S. military, policymakers, and experts are still grappling with this question and there is not yet a clear-cut answer. As the thinking continues to evolve and refine, it is worth highlighting the disparity between the growing number of offensive cyber incidents of this kind and the lack of substantial responses to them. It is, in fact, difficult to name a significant cyber incident in the post-Stuxnet era where the offender paid a serious price. North Korea (and Russia) know this.

2. On the Disruption of the North Korean Missile Program by Cyber Means

While we may not yet have solved the puzzle of deterring cyber attacks, we have made some headway on exercising cyber force as a deterrent in other domains. North Korea presents a valuable case study on the subject of applying cyber means to destabilize nuclear capabilities – from facilities to weapons to command and control. This has been an understudied area, partly because of the lack of real world instances and partly because it is very difficult to speculate on the methods and efficacy of such an approach from the outside.

In 2014, President Obama decided to employ cyber and electronic warfare to disrupt and obstruct North Korean missile tests, sending some of their Musudan intermediate range missiles plummeting into the sea. Though there is no public record of the success of the cyber measures authorized, one can make inferences based on the heightened failure rate of the Musudan following U.S. operations. This was not likely a coincidence. While it is very common for countries to see high failure rates early in their missile program, this was not an early stage for the North Koreans. In fact, they had past the phase of low success rates, identified and ironed out their wrinkles, and worked down the failure rate. Then, suddenly, the Musudan failure rate rose to 88 percent around the same time that the U.S. was exploiting its "left of launch" program – attacks designed to hit the target before the launch can happen.

We cannot hazard a perfect guess as to why the trend changed. It is possible that Kim Jong-un upgraded his systems or altered the operations once he realized what was happening. (We are dealing with a weapon with a fleeting nature, after all, where what works in cyber operations one day may not work the next day.) It is also possible that President Obama made an active decision to stand down. If the latter was the case, there are a number of potential reasons for such a move – not least of all that cyber capabilities are most valuable when concealed and this makes it more critical to factor in timing and be cautious of overuse. Sometimes it is worth waiting till the cyber operation really counts, instead of showing one's hand too early. The atmospheric tests Kim Jong-un has long promised would not be a regrettable moment to use strategic surprise with disruptive cyber operations, for example. Thus, the calculus remains extremely delicate and difficult.

IV. STRATEGIC LESSONS: LOOKING BACK AND THINKING AHEAD

"Ransomware, Cyber Crime, Security" by The Digital Artist is licensed under CC0.

Cyberspace stands as its own domain for conflict to manifest, but it simultaneously impacts traditional domains and strategic thinking in unprecedented ways. This is especially palpable in the nuclear realm. The coinciding existence of these two strategically impactful elements of national security creates an uncertain environment that is still being explored and analyzed. This new era cannot – must not – be left to the wayside. It can irreversibly impact interstate relations, balance of power, and global stability.

Nuclear weapons have for decades marked certain uncrossable lines and impassable boundaries among great powers. Their very existence made them at once the greatest existential threat and the guarantor of survival. In part, such stability stemmed from the exclusivity of the nuclear club. The time, resources, cost, and expertise required to develop and maintain sizeable arsenals precluded most states from pursuing nuclear weapons.

Times have changed alongside priorities. The five original nuclear states – the U.S., the U.K., France, Russia, and China – comprised the nuclear club consented to by 191 nations by the 1970 Treaty on the Non-Proliferation of Nuclear Weapons (NPT). Three states not party to the NPT have since developed nuclear arsenals – including Israel, India, and Pakistan – with Iran and North Korea recently attempting the same. For these states, the threshold seems to be perceived as demonstrably lowered – as their actions have emphatically evidenced. Their cost-benefit analysis and risk calculus have been strategically divergent from other states. We are witnessing a break in the patterns of history. The safeguards we took for granted may or may not be able to prevent nuclear

proliferation, and we may yet see more aspirants or copy-cats to come. The emphatic lesson here is that while the nuclear problem lives on, the principles deriving from nuclear security may in fact be dying. In other words, nuclear threats may continue to remain paramount – making this a global security challenge we have not yet left behind.

WE ARE WITNESSING A BREAK IN THE PATTERNS OF HISTORY. THE SAFEGUARDS WE TOOK FOR GRANTED MAY OR MAY NOT BE ABLE TO PREVENT NUCLEAR PROLIFERATION, AND WE MAY YET SEE MORE ASPIRANTS OR COPY-CATS TO COME. THE EMPHATIC LESSON HERE IS THAT WHILE THE NUCLEAR PROBLEM LIVES ON, THE PRINCIPLES DERIVING FROM NUCLEAR SECURITY MAY IN FACT BE DYING.

The relevance of nuclear security does not rest solely on non-nuclear states now experimenting with dreams of becoming nuclear powers – whether for leverage against existing powers or a seat at the table with them. This continues to be an increasingly grave concern – whether we are dealing with Iran, North Korea, or other states with the same dangerous ambitions. The momentum certainly exists for states to develop nuclear weapons, as we have already seen an expansion of the nuclear club by at least three – and that is only in recent history. We have to remember that we are dealing with 1930s physics and 1940s technology. Such aspirations may pose their own challenges – from the material acquisitions to the science and technology – but these are no longer insurmountable for the truly dedicated state with sufficient funding and resources. The perceived incentives also seem to abound for nuclear contenders. For some states in particular, regional security is a markedly swaying factor in the rationale – India and Pakistan prove the point. Nevertheless, the principal motivation is often of a higher order: to reserve a seat at the table of global powers and be taken seriously by the superpowers that determine the course of history.

Simultaneously, the problem is worsened as there has also been a reduction of certainty when it comes to superpowers and the original members of the nuclear club. For decades, the rules of the game have been understood and adhered to when it comes to the possession and use of nuclear weapons. This has been uniquely true due to the existential threat guaranteed by such use. However, these rules are being more loosely interpreted today and are at risk of erosion. The development of ballistic missile systems only further shakes up decades of nuclear stability. Moreover, the advancement of cyber capabilities will likely have major implications here – not least of all in impacting command and control systems.

The reduction of certainty has only been exacerbated by the tenuous nature of operating in the 'Wild West' of cyberspace, where no clear rules have ever existed. In fact, we seem to be living in an era where experimentation prevails and rules writ large are designed and adjusted casually for individual states' convenience, rather than formalized and cemented for mass observance. Thus, the absence of rules in the cyber domain has been a significant and complicating factor for both the nuclear and cyber spheres.

In the 1980s, President Ronald Reagan exclaimed that nuclear weapons are unthinkable and we must never let the world come to nuclear war. That simple statement launched a phase of unprecedented cooperation between Soviet and American scientists and military officers. Now, that era of cooperation has eroded, resulting in the reversal of years of progress.

On a broader level, the once-unthinkable issue of usability is in question today. Technological advancement on all fronts has led to new levels of exploration and new ranges of usability for nuclear and cyber weapons. One glaring

example is the potentially versatile employment of EMPs – as a means of creating a sub-strategic use of nuclear weapons themselves and as a way of answering the problem of nuclear weapons in the hands of rogue states.

THE REDUCTION OF CERTAINTY HAS ONLY BEEN EXACERBATED BY THE TENUOUS NATURE OF OPERATING IN THE 'WILD WEST' OF CYBERSPACE, WHERE NO CLEAR RULES HAVE EVER EXISTED. IN FACT, WE SEEM TO BE LIVING IN AN ERA WHERE EXPERIMENTATION PREVAILS AND RULES WRIT LARGE ARE DESIGNED AND ADJUSTED CASUALLY FOR INDIVIDUAL STATES' CONVENIENCE, RATHER THAN FORMALIZED AND CEMENTED FOR MASS OBSERVANCE. THUS, THE ABSENCE OF RULES IN THE CYBER DOMAIN HAS BEEN A SIGNIFICANT AND COMPLICATING FACTOR FOR BOTH THE NUCLEAR AND CYBER SPHERES.

As cyberspace has become a fundamental dimension of modern life, it has touched every other facet of the current world order. It has altered the operating environment as well as the strategic culture that for decades underpinned global stability and security – from the nuclear to the conventional domain.

While there may be no clear analogy between cyber and nuclear power, the two have become entangled in both subtle and obvious ways. It does not help that the community of policymakers, experts, and practitioners surrounding these two important areas have been siloed from each other. Going forward, it will be crucial to build bridges between thought leaders and specialists in these two pivotal areas.

Where the nuclear era was defined by a degree of transparency, cyberspace is inherently opaque and invisible. It is tricky business to navigate through this dark space without any radar on what our adversaries are doing, how fast they are traveling, which direction they are going, or what their destination is. Add to this the reality that nuclear systems – facilities, weapons, command and control – could all be targets on the cyber highway. What is needed is greater communication and clarity in order to steer clear of everything from accidents and exploitations to provocations and incitements.

This is where perception becomes one of the great intangibles. Unquestionably, perception is a determining factor in calculating actions and reactions in most aspects of international affairs overall – notably when dealing with adversary or rogue states as well as nonstate actors.

AS CYBERSPACE HAS BECOME A FUNDAMENTAL DIMENSION OF MODERN LIFE, IT HAS TOUCHED EVERY OTHER FACET OF THE CURRENT WORLD ORDER. IT HAS ALTERED THE OPERATING ENVIRONMENT AS WELL AS THE STRATEGIC CULTURE THAT FOR DECADES UNDERPINNED GLOBAL STABILITY AND SECURITY – FROM THE NUCLEAR TO THE CONVENTIONAL DOMAIN.

The perception factor is analogously of great consequence to those playing on the same side, for they are not always on the same page. Given the frequent isolation of experts in the nuclear domain from those in the cyber domain, there can be great variance in everything from the interpretation of imminent security challenges to threat assessments. These critical national security communities have much to gain from each other and much to contribute to national security. Their knowledge and concerns must be shared. Their solutions must be jointly explored. Their divide must be bridged. Their sound barrier must be broken.

NATIONAL COMMITTEE ON AMERICAN FOREIGN POLICY (NCAFP)

FALL 2017 CYBER CONFERENCE

MUTUALLY ASSURED DISRUPTION:
FRAMING CYBERSECURITY IN NUCLEAR TERMS

Thursday, October 12, 2017

PARTICIPANT LIST

PANELISTS

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

Dr. Ben BUCHANAN
Postdoctoral Fellow, Cyber Security Project
Belfer Center for Science & International Affairs at Harvard University

Dr. Andrew J. FUTTER
Associate Professor of International Politics
University of Leicester

Ms. Sheryl HINGORANI
Senior Manager, Systems Analysis & Engineering
Sandia National Laboratories

Dr. David MUSSINGTON
Director
Center for Public Policy and Private Enterprise at University of Maryland

Mr. Rafal ROHOZINSKI
Co-Founder & Principal
SecDev Group

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

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

Lieutenant Colonel Timothy L. THOMAS (Ret.)
Senior Analyst
Foreign Military Studies Office at Fort Leavenworth

Mr. Jeffrey A. TRICOLI
Cyber Section Chief
Federal Bureau of Investigation

Mr. Paul S. TRIOLO
Practice Head, Geo-Technology
Eurasia Group

PARTICIPANTS

Mr. John H. BELL
Consultant
Lagoda Investment Management

Mr. Vic CAMAYA
Special Agent, Cyber Squad, New York Field Office
Federal Bureau of Investigation

Dr. James COCKAYNE
Head of Office
United Nations University Office at the United Nations

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

Mr. Mike DVILYANSKI
Special Agent, Cyber Squad, New York Field Office
Federal Bureau of Investigation

Dr. Thomas GRAHAM
Managing Director
Kissinger Associates

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

Mr. David P. HUNT
Chairman
Charles Pratt & Co., LLC

Mr. Karim KEMAL
Program Assistant, Nuclear Security Program
Carnegie Corporation

Dr. Camino KAVANAGH
Visiting Fellow, Department of War Studies
King's College London

Ms. Simran R. MAKER
Associate Project Director, Cybersecurity Initiative & Middle East Initiative
National Committee on American Foreign Policy

Mr. John C. MALLERY
Research Scientist
MIT Computer Science & Artificial Intelligence Laboratory

Mr. Thomas MOORE
Senior Advisor
National Committee on U.S.-China Relations

Ms. Allison PYTLAK
Programme Manager, Disarmament
Women's International League for Peace & Freedom

Mr. Nicholas RHODES
Political Advisor
U.S. Mission to the United Nations

Mr. Josh RYDER
Senior Director, Network & Cybersecurity Engineering & Operations
AppNexus Inc.

Mr. Evgeny SCHERBAKOV
Program Assistant, International Peace and Security Program
Carnegie Corporation

Ms. Kerstin VIGNARD
Chief of Operations & Deputy to the Director
United Nations Institute for Disarmament Research

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

OBSERVERS

Ms. Juliet LEE
Associate Project Manager, Forum on Asia-Pacific Security
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