MAY 7, 2018

STRATEGIC CULTURE AND CYBERWARFARE STRATEGIES: FOUR CASE STUDIES

SIPA CAPSTONE WORKSHOP

CLIENT ORGANIZATION: UNITED STATES CYBER COMMAND

FACULTY ADVISOR: PROF. GREGORY RATTRAY

ABDULRAHMAN YAAQOB AL-HAMADI; DANIEL NICHOLAS BOCCIO; ERIK KORN; RASHIDE ASSAD ATALA; SCOTT SCHER; AND STEVEN JUN SIC PARK

ACKNOWLEDGMENTS

The Strategic Cultures and Cyberwarfare Strategies team would like to express its deepest gratitude to Prof. Gregory Rattray, Dr. Emily O. Goldman and Dr. Michael Warner for their dedicated knowledge-based support for the project. We are also deeply thankful to Erica Borghard, Jenny Jun, Jack Snyder, JD Work, Jason Healey, Sean Kanuck, Adam Segal, and Nadiya Kostyuk for their time and invaluable insights.

ABSTRACT

This report presents the U.S. Cyber Command with a cross-case study based on the examination of China's, Russia's, Iran's, and the Democratic People's Republic of Korea's history, geography, politics, economy, religion, and philosophy in order to understand how each differing strategic culture guides the state's motivations and behaviors. This includes each country's employment of non-state actors and proxies, legal framework, and military-civilian relations. The strategic culture lens provides a deeper understanding of each state's cyberwarfare strategies. By examining how current factors are shaping the most likely future trajectory and what the most dangerous trajectory could look like, we provide lessons that the U.S. can draw upon for its own strategic formulations.

The team conducted literature and internet reviews to identify the influencing factors for each country's strategic cultures and current cyber capabilities. Additionally, the team conducted in-person and phone interviews with field experts to assist in the understanding of the issues, concepts, and processes to formulate the most relevant product for the client. Interviewees included Erica Borghard, Jenny Jun, Jack Snyder, JD Work, Jason Healey, Sean Kanuck, Adam Segal and Nadiya Kostyuk.

EXECUTIVE SUMMARY

This project examines how strategic culture influences the way Russia, China, Iran, and North Korea conceptualize, understand, and act within cyberspace to better inform future U.S. decision-making, policy creation, and national actions within cyberspace. This report is presented in the form of a cross-case study that attempts to answer two overarching research questions:

1. Strategic culture: How does strategic culture frame each state's understanding of the cyber domain and, therefore how does this understanding inform the capabilities they currently possess, intend to develop, and how they plan to use them?

2. Future trajectories: What does the most likely trajectory for each country look like? What does the most dangerous trajectory look like?

The strategic culture lens -understood as the embodiment of how history, geography, politics, economy, religion and philosophy shape a nation's identity and create a consistently structured national security response- is used to enable a broader and deeper understanding of each state's cyberwarfare strategy. Each case study provides a set of lessons that the U.S. can draw upon for its own cyber strategy as well as potential areas for future research.

CHINA

Chinese strategic culture is usually described by either the Confucian-Mencian paradigm or the Parabellum paradigm. However, it can be argued that cyberspace presents a new vehicle capable of supporting the employment of both. Consequently, an important analysis of Chinese strategic culture accounts for the use of cyberspace through a continued avoidance of violence in lieu of predominantly offensive operations. Espionage, intellectual property theft, and information dominance are all methods employed through cyber means to ensure the preservation of the state, protection of its national borders, and the prevention of perceived disruptive influences from potential adversaries seeking to prevent China's rise.

Although China's national strategy and objectives persist, a noticeable shift has been observed in the intensity and frequency of its cyberspace activities. However, China is likely to continue to use its interpretation of international law to legitimize both its domestic and international actions in the cyber domain. The establishment of the "Information Silk Road" as part of the OBOR initiative is likely to remain a major focus in growing China's economy and regional influence through cyberspace because it enables both information dominance domestically and deterrence of international interference associated with disputes in the South China Sea, Taiwan, and Tibet. Another economic consideration should also be taken into account is that China remains a large holder of U.S. debt, and this is likely to strongly influence Chinese decision-making when considering the impact of cyber operations that could negatively influence or potentially damage U.S. critical economic infrastructure.

On the other hand, misperception of signals from Beijing based on how China seeks to engage in cyberspace can lead to dangerous global impacts. A situation where the PLA views U.S. actions to be a violation of its cyber sovereignty maintains a propensity to be perceived as an offensive action and trigger a preemptive response from China. Consequently, this may lead to an escalatory crisis scenario that maintains the propensity of spreading to other domains. If escalation occurs through cyberspace, a U.S. response may not be able to achieve the desired magnitude of its intended effectiveness against specific digital targets as a result of tight controls across China's internet. Accordingly, these factors may compel the U.S. or other nations to consider kinetic avenues of approach toward their desired targets in some capacity.

Whether U.S. actions are deemed to be offensive or defense in nature, a violation of Chinese sovereignty (physical or asymmetric geographies), or as an active attempt to delegitimize the state government, will have profound impacts on China's deployment of its cyberspace capabilities. Consequently, the U.S. must seek to understand what China's 'nine-dash line' is in cyberspace, and how it can best formulate a strategy that will prevent an escalatory response as a result of misunderstood signals in all domains of warfare.

An important point of emphasis in the formulation of U.S. cyber strategy with China should also include a thorough analysis of how the Chinese government is likely to understand, interpret,

and implement future cyberspace agreements, as well as not just China's short-term strategic objectives, but also their long-term global ambitions twenty to thirty years from now.

Lastly, the consolidation efforts of President Xi Jinping this past year may be signaling a new development in how China seeks to use cyberspace to its advantage in the future. For example, the Confucian "mandate of heaven" can be conceptualized as a potential representation for how President Xi's legitimacy has been built upon his intent to restore China's world standing, and how a newly consolidated cyber force represents another means to achieve this national objective.

RUSSIA

The Russian approach to cyberspace is based on a Hobbesian zero-sum interpretation of the international arena in which a failure to vanquish spells defeat. Russia's conduct within the cyber domain has been informed by state affairs and political developments and makes a particular emphasis on offense. Deep operations theory has considerable visibility and applicability in Russia's approach to cyber warfare and appears most demonstrably in its offensive posture in the realms of Command and Control (C2), Psychological Operations (PsyOps), or Action on Objective. Deep operations theory is also evident in Russia's Information Security Doctrine of 2008, which marshals all sectors of Russian society to exercise efforts in furtherance of Russian national information security objectives. Another point of consideration is that progression to greater state control of the Internet appears to proceed in a piecemeal manner, where legislation has been passed addressing specific facets of information security instead of a nationwide firewall.

Conventional intelligence has shown greater Russian willingness to use force in the cyberspace domain. This includes using Ukraine as a testing ground for more of its advanced cyber weaponry and tactics. These have been employed in support of kinetic operations, as well as in pure cyber missions. Given past Russian success in cementing frozen conflicts, its need for cognizance in its actual capacity, and the risk of over stretch, further belligerence will likely occur in the Near Abroad. We can expect Russia will be active in group operations across domains, until they see their adversaries parried.

What appears to be the worst-case future trajectory is that Russia will exhibit even less reticence to engage in aggressive behavior. As a result of, minimal and shrinking economic and diplomatic common interest, and links with the West. This evaluation is seconded by the possibility that the DNC breach is a sign of Russian disregard for the consequences of its actions. If this were to be the case, then it would be more than reasonable to anticipate the most dangerous scenario to be a Russian doubling-down in the face of confrontation. In addition, with every capability that Russia has perpetrated on the West, there was a precedent in its near abroad. Whether through pure information operations in Estonia, hybrid operations in Georgia and Crimea, or infiltration of critical infrastructure systems in Eastern Ukraine. There are parallels in information operations to influence elections, the possibility of clash in flashpoints featuring the Russian Armed Forces, as well as the discovered presence of Russian malware in U.S. SCADA systems.

Russian action is trying to maximize its push for hegemony in what it deems its traditional spheres by any means necessary, just short of war. As for implications for the US, countering deception in the information space will require i) an understanding of the means and disguises through which Russians will obfuscate their actions in the domestic space; and ii) hardening soft targets, such as social media and defense against guerrilla cyber operations through proxy TOR servers.

Moreover, it will be necessary to adapt to the Russian understanding of deterrence, which is a reiteration of active measures. However, understanding and remembering Russia's desire for a strategic stability that aligns with great power balance, and one that reinforces the Russian perception of a multipolar world, is key. As the strategic stakes increase with symbolic and strategic importance, we see the lengths Russia will go to. Without communicated direct response or show to force from the West, Russia will feel emboldened to proceed with impunity.

In response to Russian influence operations during the 2016 election, notable steps were taken with respect to diplomatic and judicial retaliation. It is time that these are joined militarily. Atlantic Resolve is just one of many steps taken in the kinetic realm. A potent next step would be to join this with an OCO that imposes cost on Russia and makes them cognizant of not only the lengths to which the U.S. will proceed offensively, but what risk they pose to themselves.

IRAN

Today, significant features in the strategic culture of the Islamic Republic of Iran are: a strong national cultural identity, dominant leaders, and powerful military organizations as important players in strategic development as well as important receptors for strategic targeting. Both the strong national cultural identity, which is rooted in regional hegemonic ambitions, and the dominance of the theocratic ruling regime lead to a culture in which a powerful military arsenal is a must. Similarly, the powerful national identity and military culture lead to confrontation and rivalries with regional foes, which themselves become part of the strategic culture of Iran. These features are woven together such that they produce a comprehensive strategic culture that dictates Iran's foreign policy and military activities in general, and its cyber warfare activities in particular.

The history of Iran as a major civilization and hegemonic regional power has manifested in Iranian cyberattacks, many of which have targeted its regional adversaries, such as neighboring Arab Gulf countries and Israel. In addition, its presumed role as leader of the "Axis of Resistance" (to Israel) has channeled its aggressive cyber operations against U.S. and Western allies in the region. As a guardian of jurisprudence, and by extension a guardian of the state, the Supreme Leader and the Ayatollahs exert major control over guiding the use of cyber as a weapon. That is reflected in Iran's cyber warfare activities being geared not only to preserve and protect the regime from domestic and foreign threats but also to go on the offensive against these adversaries.

In all likelihood, Iran will continue to develop its cyber capabilities and expand the network of proxies to include Iraqi groups being supported by Iran. Domestically, the IRGC will continue espionage activities against its citizens to ensure a successful oppression of any popular protests. Regionally, Iran's cyberwarfare will continue to focus its sabotage efforts against its neighboring Arab countries, including targets crucial to U.S. interests in an effort to counter its adversaries and expand its interventionist policies. Globally, it will focus its efforts on espionage operations aiming to collect data in order to influence public opinion through propaganda. Further, in retaliation to the recent statements made by President Trump against Iran's

destabilizing activity in the region, the Iranian regime may target businesses belonging to the President's family and relatives.

The most dangerous scenario includes much more extensive and dangerous damage targeting U.S. domestic infrastructure and disruption of U.S. military operations. Although most of Iran's activities in the West have been for data mining or financial benefit, a cyber-attack on vital infrastructure facilities, such as nuclear facilities or electric power plants, in the U.S. cannot be completely ruled out. Furthermore, since Iran, its proxies, and allies are becoming the target of Westerns military operations, Iran may choose to escalate further and targeting U.S. bases in the region with a cyber-attack. The aim of the operation to disrupt the U.S. military operations in Syria, Afghanistan, and Iraq. Such operations are complicated and require expertise and vast technical resources. Therefore, Iran may rely mainly on its elite cyber force, the Passive Defense Organization.

Since it is expected that Iran would likely focus its cyber-attacks attention on the energy sector, it becomes necessary to realize the importance of allowing additional monitoring of facilities and internet-connected equipment to prevent any fall and failure. Coordination with the relevant government entities, is crucial. In addition, the focus of Iran's cyberspace activity is directed against the West, including the United States and, therefore, requires appropriate defensive arrangements, beginning with an up-to-date doctrine of cyberspace defense. Moreover, and since Iran's neighbors are a primary target of its cyber warfare, it would be advisable to encourage the Arab States to strengthen their cyber capability in order to face the Iranian threat.

DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA

Historically, the pursuit of aggressive military policies not only consolidated power, but also overwhelmed South Korea. However, because of the existence of the U.S. military base and the economic surpassing of South Korea, it is now a clear fact that North Korea has no rational hopes of achieving its grand mission to unite the Korean peninsula by military might. As so, efficacy of conventional use of force has been undermined to the maximum extent without risking engaging in full-fledged war.

The continued pursuit of an aggressive set of military policies placed the North Korean elites at a grid-lock situation against South Korea, the U.S., and the international community, which meant they could not take any more military action without escalating the situation. In addition, the Chinese declaration that they would not respect their past agreement to support North Korea in time of war against the U.S. has left Kim Jung-Un with little room to maneuver in addressing domestic power retention issues. Because exercising conventional capabilities would escalate the situation out of control for the North Korean leadership, it was necessary that the party and the military find a solution to enhance the efficacy of use of force in a method that does not escalate the current status quo. Such perception and need of the ruling class has resulted in unexpectedly sophisticated cyber capabilities to be developed, which surprised the western cyber security experts during the SWIFT and WannaCry hacking incidents.

Beyond the obvious continuation of current activities, one of the top three most likely future trajectories of Pyongyang elites would consider installing malware that can lay dormant in U.S. critical infrastructure systems, but that can effectively take down the system from its building-block level and up when invoked. Critical infrastructure, such as the three core U.S. electricity grids, are clear high value targets to cyber intrusion. However, because actual trigger of dormant malware would be a clear act of war, the DPRK would most likely only plant the malware as a fallback for the regime and, with high confidence, never pull the trigger unless Kim Jung-Un's life is directly threatened.

Second most likely is, with rise of the cloud computing industry, hijacking of computing infrastructure can become a lucrative exploit for North Korean hackers. Account credential theft can benefit the DPRK in multiple ways, including utilizing the computing resources to mine cryptocurrencies, leverage for botnet, and mask malicious deployment. It is highly probable that individual server operators across the world whose main expertise are not on the servers are all potential targets for North Korean hacker groups in this regard.

Last of the three most likely future trajectories is Kim Jung-Un and the RGB's investment toward long term (15~30 years) cyber-content capacity building. The RGB has a long history of experimenting their cyber capabilities on South Korea in terms of manipulating the public

sentiment. Currently, due to what deems to be intelligence failure, former directors of National Intelligence Service of South Korea were arrested on charges of operating a South Korean counter action team to counter what they claim is North Korean influence.

In this respect, the Russian interference in the American election would also have been a benchmark learning experience for RGB strategists. Considering the above along with the longevity nature of totalitarian regime policies, it is possible to hypothesize that North Korean strategists would seek to influence a democratic state's public opinion by indirectly affecting one of the five blocks in the digital media value chain. For example, the RGB can work to create original content designed around mockery of existing elected policymakers -it would not only significantly undermine the RGB's target individual, but it would also act to discourage policy makers to 'meddle' with North Korea.

The most dangerous future scenario would be North Korea wrongly being accused of a cyber offensive and being cornered into a kinetic act of war resolution. Such false accusation caused by the difficult nature of the cyber domain could systematically force the North Korean leadership into activating the first of the aforementioned scenarios –an execution of attack on critical infrastructure would directly lead to escalation of tension rapidly and uncontrollably for either states. North Korean elites have structured their society in a way that leaves them with limited response decision choices in exchange for continuation of power stability –such dynamics can be extended to the cyber domain and should be considered as the most dangerous trajectory possible.

Undermining Kim Jung-Un's leadership within North Korea would also be a personal red line for Kim Jung-Un. Although seemingly unassociated with cyber, impossible cases such as the U.S. pressuring Kim Jung-Un via enabling free flow of information for the mass population would be detrimental to sustainability and safety of the regime. The DPRK's intranet is believed to be fully compatible with the worldwide internet. Although Kim Jung-Un does not allow landlines to be connected, he could trigger the aforementioned malware in U.S. critical infrastructure as a retaliation for the improbable case that North Korea is enabled access to the current Western internet and its free flow of information

North Korea's key decision makers have anticipated and confirmed that cyber offers high utility in pursuing larger policy goals, and further even more aggressive cyber activities seem highly probable. More hackers having been assigned to money raising operations rather than intelligence collection, signals that North Korean policymakers are concentrating cyber capabilities to counter economic sanctions from the U.S., Japan, and South Korea.

For U.S. Cyber Command, drawing a clear online red line seems imperative as the nature of the DPRK's cyber operations render it nearly impractical to tackle via counter cyberattack. The DPRK will continue to be far less vulnerable to cyber-retaliation while their cyber offensive capabilities have been tailor-made under 'supreme teachings' of Kim Jung-Il and Kim Jung-Un. That, coupled with the reality that North Korean cyber operations are carried out clandestinely in third-party nations, makes the situation seem as if fighting against a 'ghost': the ghost can't be hunted or hurt but it can hurt you.

The U.S. must be as comprehensive in their approach to cyber defense as DPRK's cyber offensive is. Undermining, misinforming, and disadvantaging the U.S. involves targeting not only mass population and private companies, but also targeting specific individuals that may be advantageous to leverage against U.S. government entities such as Cyber Command. As well as high rank officials of private financial firms. Effectively countering such comprehensive and combined (kinetic and cyber) offensives by DPRK will require more private-public collaboration, as well as higher awareness from those in leadership positions.

Common Themes and General Implications for the U.S.

Imbedded within all four state's strategic culture is the dominating influence of an authoritative leader, animosity towards the West, and a strong patriotic/nationalistic response to perceived slights. Throughout the course of this project, the paramount element that manifested amongst each is the use of the cyber domain as an equalizer in four areas.

1. All four states analyzed desire prestige or relevance on the international stage, and have developed cyberwarfare strategies around achieving this objective;

2. For each of the cases, the understanding of the cyber domain is coupled with the state's understanding of Information Warfare (IW);

3. All four cases share the desire for sustaining their regimes; and

4. For each of the cases in this report, cyber capabilities have become an extension of their asymmetric warfare capability. Of particular importance is their use of proxies and the civil sector for achieving this means.

Within this mindset of equalization, the control over information is an integral part of all four state's cyberwarfare strategies, both domestically (defense) and internationally (offense). The cyber domain is being used to further drive animosity for the West amongst its citizens and has enhanced all four nation's ability to conduct military operations as a means to project power for coercion, while still remaining just short of the threshold for military response. These states see the cyber domain as a vail of deniability for actions that might evoke negative repercussions against them.

Based on these common themes we recommend three areas for which U.S. Cyber Command needs to be aware:

1. When predicting the future cyber behavior of these four states, accounting for their acute sensitivity to regime stability is paramount. Any activity conducted by the U.S. that might be perceived as disruptive to these regimes, has a high likelihood of being responded to via the cyber domain. As there are already questions around whether the 2015 cyber agreement between the U.S. and China has actually had any impact on Chinese economic cyberattacks, the current trade war could easily push China to resume these industrial espionage operations. Over the past ten years, Russia has ramped up its use of offensive cyberattacks and has become embolden in its targets, as seen in the recent Democratic National Convention (DNC) hack and election meddling. As relations between the U.S. and Russia continue to deteriorate and the effects of newly imposed sanctions are felt by Russia, the likelihood of them resorting to a cyber response is extremely high. If the recent comments around the Iran nuclear deal are perceived by the Iranian regime as legitimate threats that

will lead to newly imposed sanctions, Iran may retaliate with cyberattacks against economic targets associated with the U.S. North Korea has been able to offset some of the financial effects of economic sanctions imposed on them through cyber operations. Economic cyber activity will continue and potentially expand for North Korea especially as tensions with the U.S. rise.

2. Defending against operations conducted by these states will continue to be a challenge for U.S. Cyber Command because of their willingness to employ the civil sector and proxies. These non-state actors provide the adversaries with greater control and flexibility in the domain. Proxies also adhere to their own ideals and motivations, meaning they operate according to different rules. This should be the greatest area of concern for U.S. Cyber Command. China seems to have started shifting focus from intellectual property theft to a more highly precise offensive targeting of critical infrastructure. In addition to the threat posed by Russia and China, U.S. Cyber Command must be on the lookout for Iranian and North Korean threats to critical infrastructure as well. Since both states are relatively insulated from a U.S. cyber response due to their lack of ICT infrastructure, they perceive themselves as having a low level of vulnerability in this domain.

3. Preparation for continued contention over the cyber domain must take into account the potential second and third order effects of peripheral diplomatic and military incidents spilling over into the cyber domain. The recent kinetic action against the Assad regime by the United States and its allies has real potential to cause cyber actors sympathetic to the regime to retaliate against the United States, Israel, or Western interests. We cannot rule out the possibility that Russia or Iran would use their cyber capabilities to attack the United States in retaliation for the recent missile deployment in Syria. As spill over incidents continue to rise, the cyber repercussions to future operations will have to be considered before they are conducted.

TABLE OF CONTENTS

PROJECT OBJECTIVE

The complex characteristics of the cyber domain, coupled with the fast pace at which it continues to evolve, has led to multifaceted national security challenges.[1] U.S. Cyber Command has previously analyzed historical and conceptual cyberspace analogies in relation to how different variables influence U.S. understanding of this domain. Conversely, this project examines how strategic culture influences the way Russia, China, Iran, and North Korea conceptualize, understand, and act within cyberspace to better inform future U.S. decision-making, policy creation, and national actions for effective competition in cyberspace.

APPROACH AND METHODOLOGY

ANALYTICAL FRAMEWORK

This report is presented in the form of a cross-case study. The unit of observation for each case is the nation-state. Given the heterogeneous nature of the units under study, the cross-case research design is the best suited for i) the intensive study of each individual case and its underlying dimensions; but also, ii) the comparison between cases.[2]

This report attempts to answer two overarching research questions:

Strategic culture: How does strategic culture frame each state's understanding of the cyber domain and, therefore how does this understanding inform the capabilities they currently possess, intend to develop, and how they plan to use them?

Future trajectories: What does the most likely strategic trajectory for each country look like? What does the most dangerous strategic trajectory look like?

The strategic culture lens enables a broader and deeper understanding of each state's cyberwarfare strategy. Each case study provides a set of lessons that the U.S. can draw upon for

[1] The development of cyber capabilities can enable opportunities for better communication, economic development, and security, amongst others, but it can also lead to more vulnerabilities and threats.
[2] John Gerring, "The Case Study: What It Is and What It Does," in Carles Boix and Susan C. Stokes, *The Oxford Handbook of Comparative Politics*, Oxford University Press (United Kingdom, 2009), pp. 90-122.

its own cyber strategy. In addition, the report also presents a set of general implications moving forward and highlights potential areas for future research.

Strategic Culture

Throughout this report, strategic culture is understood as the embodiment of how influencing factors shape a nation's identity and create a consistently structured national security response. When analyzing strategic culture, we examine the varying approaches to this concept, at what point the tone of the debate is set, what contributes to the development of strategic concepts, and how policymakers are influenced on strategic issues.

Strategic culture is widely referenced in writings on International Relations (IR) in an attempt to explain the distinctive behavior of states through an examination of their individual unique properties. Strategic culture is a limited and prioritized set of grand-strategic preferences that are consistent across the objects of analysis and strongly persistent across time.

For Jack Snyder,

> strategic culture can be defined as the sum total of ideas, conditioned emotional responses, and patterns of habitual behavior [cognitive behavior] that members of a national strategic community have acquired through instruction or imitation and share with each other with regard to military strategy. By identifying historical and organizational factors, strategic culture attempts to explain the origins and continuing vitality of certain attitudes and behavior.[3]

The strategic culture of a state has a multitude of sources. Ranging from the national to the organizational (in particular the military, which can be further divided into the separate branches, all with a unique subset of strategic cultures), with the former being the underlying influence in which the latter is formed. Strategic culture is codified in collective memory and identity through education, training, political narratives, popular culture, and renditions of

[3] Jack L. Snyder, "The Soviet Strategic Culture: Implications for Limited Nuclear Operations," Rand (United States, 1977), available at: https://www.rand.org/content/dam/rand/pubs/reports/2005/R2154.pdf (last consulted: January 2018).

historical events. Within organizational subculture, individuals are socialized into a specific mode of thinking, thereby viewing the world through a unique strategic culture lens; this lens subsequently creates a particular national security concept. The perseverance of these distinct beliefs, attitudes, institutional associations, and history over time constitutes an enduring set of factors that influence decisions in addition to policy objectives.

These preexisting strategic conceptions can strongly influence a state's adoption of, or resistance to, the implementation and use of new technologies. This aspect of strategic culture is of particular importance in the context of cybersecurity. Each nation's attitudes toward the development and deployment of cyber capabilities is likely to be directly influenced by the distinctive organizational subculture that controls it.

Analyzing both levels of strategic culture is imperative for understanding the motivations and manner in which states choose to act in the cyber domain. Without a clear understanding of the national actor, engaging in strategic assessments of other states could prove to be precarious: states can inadvertently act in a provocative manner or unwisely misinterpret intentions.

According to Alastair I. Johnston, strategic culture is an integrated

> system of symbols (argumentation structures, languages, analogies, metaphors) which acts to establish pervasive and long-lasting strategic preferences by formulating concepts of the role and efficacy of military force in interstate political affairs, and by clothing these conceptions with such an aura of factuality that the strategic preferences seem uniquely realistic and efficacious.[4]

Strategic culture provides an analytic lens through which the motivations and behaviors of a nation can be observed and evaluated. We utilize this framework by defining the independent variables that together are assessed to constitute a state's strategic culture. These variables include history, geography, politics, economics, philosophy, and religion, and the relationship

[4] Alastair I. Johnston, "Thinking About Strategic Culture," *International Security*, Vol. 19, No. 4 (Spring, 1995), pp. 32-64, available at: https://www.jstor.org/stable/2539119?seq=1#page_scan_tab_contents (last consulted: January 2018).

between them. While the effects of these variables are unique to each particular state, they subsequently permeate across the development of the nation's strategic culture.

Additionally, by studying strategic culture, it becomes evident that a nation's actions are not fully determined by policy and are deeply rooted within influential existential factors. By distinguishing the variables of strategic culture from other broader influences, we can better illuminate the underlying purpose of strategic culture: to provide decision-makers with a uniquely ordered set of strategic choices from which we can derive predictions about behavior.[5]

Preconceived notions over strategic decisions is where strategic culture begins to affect behavioral choices directly. "Historical or 'objective' variables such as technology, polarity, or relative material capabilities are all of secondary importance to strategic culture".[6] We believe that strategic culture can be a powerful and useful lens for the U.S. to understand its adversaries and inform its own strategic choices.

METHODOLOGY

According to Alexander George and Andrew Bennett, a case study is "a detailed examination of an aspect of a historical episode to develop or test explanations that may be generalizable to other events."[7] Case studies are valuable for testing hypotheses and developing theories[8] because of their:

1. Potential for achieving high conceptual validity;[9]
2. Strong procedures for fostering new hypotheses;
3. Value as a useful means to closely examine the hypothesized role of causal mechanisms;[10] and

[5] *Ibid.*
[6] *Ibid*.
[7] Alexander L. George and Andrew Bennett, *Case Studies and Theory Development in the Social Sciences*, MIT Press (United States, 2005), p. 5
[8] *Ibid*, p. 18
[9] Identify and measure the indicators that best represent the theoretical concepts the researcher intends to measure by searching for analytically equivalent phenomena across different contexts.
[10] Within a single case, we can look closely at different intervening variables and shed light on unexpected aspects of the operation of a particular causal mechanism or help identify what conditions trigger the causal mechanism.

4. Capacity for addressing causal complexity.[11]

Special attention must be payed to the trade-off between parsimony and richness, as well as to the tension between achieving high internal validity and good historical explanations versus making generalizations.[12] To address this, each case study will present its own set of lessons for the U.S., in addition to the report's general recommendations for policy and research.

To answer the question of how strategic culture influences the state's understanding of the cyber domain, each case study will characterize the state's strategic culture by explaining their understanding of the:

1. Role of force in state affairs;
2. Nature of the adversary and of the threat;
3. Efficacy of the use of force;[13]
4. Use of non-state actors and proxies
5. Legal framework; and
6. Military-civilian relations

To better understand where a state's strategic culture originates, each case study delves into the following independent variables: history, geography, politics, economy, religion, and philosophy,[14] and the relationship between them.

The second section of each case study focuses on current factors that are shaping the most likely future trajectory and describe what each state's most dangerous trajectory could look like. Each case study ends by providing a set of lessons that the U.S. can draw upon for its own strategic formulations.

[11] This advantage is relative rather than absolute. For example, case studies can allow for equifinality (the property of allowing or having the same effect or result from different events), but to do so they produce generalizations that are narrower or more contingent. Case studies also require substantial process-tracing evidence to document complex interactions.
[12] George and Bennett, *Op. Cit.*, p. 22.
[13] Johnston, *Op. Cit.*
[14] Snyder, Jack, *Op. Cit.*

This project is based on literature and internet reviews that help identify the independent variables of these states' strategic cultures. Additionally, each case study relies on in-person or phone interviews with field experts that include Jenny Jun, Jack Snyder, JD Work, Jason Healey, Sean Kanuck, Adam Segal, and Nadiya Kostyuk. These interviews helped inform a more comprehensive understanding of the issues, concepts, and processes concerning this project.

CASE STUDIES

CHINA

…. The war can only be fought battle by battle,
and the enemy can only be eliminated bit by bit….

-Mao Tse-Tung in a speech delivered
on November 18th, 1957[15]

INTRODUCTION

China's rise as a principal actor within cyberspace has transformed a once predominantly neutral domain into a medium conducive to "endless competition," one that has become intensely dominated by an escalatory struggle between the U.S. and China.[16] China's present-day posture and activities within cyberspace have generally been characterized through attempted acts of international espionage, industrial and military intellectual property theft, and control of information within its own borders.

These actions may seem overtly conclusive to other countries like the U.S. who view these activities through a specific lens, one that has been subsequently informed by their own strategic cultures. However, China's history, geography, politics, economics, religion, and philosophy have all actively informed and influenced the pursuit of state-defined strategic objectives. Consequently, these variables have influenced the lens China applies to cyberspace operations, a domain it utilizes as a vital component of its national security strategy.

Accordingly, this case study will explore how China understands cyberspace as an instrument of foreign policy, the formulation of its own strategic culture, comparisons based on these strategic culture variables, and an assessment of how China may conduct itself in the future. These factors

[15] "Some Background Notes on Mao Tse-Tung's Philosophy of Force," Office of Research and Analysis (United States Information Agency, October 28, 1960), 12, https://hv.proquest.com/pdfs/103376/103376_002_0925/103376_002_0925_From_1_to_19.pdf.
[16] Yoonyoung Cho and Jongpil Chung, "Bring the State Back In: Conflict and Cooperation Among States in Cybersecurity," *Pacific Focus* 32, no. 2 (August 1, 2017): 290–91, https://doi.org/10.1111/pafo.12096.

will help determine how China's concept of cyberspace influences its views on the role of force in state affairs, nature of the perceived threats, efficacy of the use of force, use of non-state actors and proxies, legal framework, and its military-civilian relationship. Concurrently, it is anticipated that an examination of these contributing factors will also help explain how China's approach informs its conduct and posture within cyberspace.

Defining China's Strategic Culture

Although varying views exist on the exact characteristics of Chinese strategic culture, Alastair Iain Johnston highlights the following predominant features from other literature: theoretical and practical preference for strategic defense,[17] preference for limited war,[18] and low estimation of the efficacy of violence,[19] in addition to an observation of low variation from the time of Sun Tzu through Mao Zedong. Johnston's findings also present a Chinese preference for offensive strategies that have also been suggested in additional historical literature.[20]

In his findings, Johnston consequently proposes the existence of two different paradigms for Chinese strategic culture. The first is identified as the Confucian-Mencian paradigm, which assumes conflict to be avoidable, and when force must be used, it should be defensively employed on a minimal scale.[21] The second paradigm is identified as the Parabellum Paradigm, which "assumes that conflict is a constant feature of human affairs, that it is due largely to the rapacious or threatening nature of the adversary, and that in this zero-sum context the application of violence is highly efficacious for dealing with the enemy;" the Chinese concept of "quan bian," or absolute flexibility, is also a feature of this paradigm that links the success of offensive violence to a strategy that facilitates the necessary environmental conditions for success.[22]

[17] Walls, garrisons, static positional defense, and alliance building as opposed to invasion.
[18] Restrained application of force.
[19] Sun Tzu's subduing the enemy without fighting.
[20] Alastair I. Johnston, *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History* (Princeton, N.J.: Princeton University Press, 1995), 25.
[21] Johnston, 249.
[22] Johnston, 249.

Nevertheless, it can be argued that cyberspace presents a new vehicle capable of supporting the employment of both paradigms. Strategic defense, limited war, and restrained application of force are valid characteristics, but the pursuit of offensive strategies and operations should not be excluded as alternatives that support this type of Chinese strategic posture.

This case study presents an adaptation of Johnston's description in an attempt to account for China's perception and subsequent actions within cyberspace. Consequently, an important analysis of Chinese strategic culture accounts for the use of cyberspace through a continued avoidance of violence in lieu of predominantly offensive operations. Espionage, intellectual property theft, and information dominance are all methods employed through cyber means to ensure the preservation of the state, protection of its national borders (both physical and abstract), and the prevention of perceived disruptive influences from potential adversaries seeking to prevent China's rise. China's unique history, geography, politics, economy, religion, and philosophy have shaped their strategic culture, as well as the comparisons they employ in their approach in cyberspace. Moreover, these variables of Chinese strategic culture are distinctive, have maintained stickiness or persistence over time, contribute to a common mindset and social practices, and are habits or ideas transmitted through socialization, as discussed with Jack Snyder during a recent interview.[23]

INDEPENDENT VARIABLES

HISTORY

Chinese nationalism, deeply rooted in history and born throughout the Century of Humiliation, is one of the strongest components of China's strategic culture. Simply put, Chinese nationalism not only entails the pride of being Chinese, but most importantly, the shared recollection of past humiliations and the desire to return to greatness.[24]

---

[23] Jack Snyder, Discussion on Strategic Culture, In Person Interview Conducted At: Columbia University School of International and Public Affairs (SIPA), March 5, 2018.

[24] Colonel Kenneth D. Johnson, *China's Strategic Culture: A Perspective for the United States* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2009), https://permanent.access.gpo.gov/websites/ssi.armywarcollege.edu/pubs/display.cfm-pubID=924.htm.

The Opium War between Great Britain and China, which ended with the Treaty of Nanjing, led to the disintegration of the Chinese Empire and the loss of sovereignty as Great Britain and France delineated zones of influence and privilege.[25] Half a century later, the First Sino-Japanese War demonstrated the shift in regional dominance in East Asia from China to Japan when China had to recognize the independence of Korea and then ceded territory to Japan as well.[26]

By 1900, the resentment took action in the form of the Boxer Uprising,[27] which in turn gave way to the Eight Nation Alliance[28] invasion of China, where troops looted cities, murdered and assaulted Chinese citizens. The Boxer Protocol of 1901[29] led to the Revolution of 1911[30] that finally ended the Qing Empire. With the Republic of China still in its infancy, China suffered another setback when the Allied Powers transferred Shandong from Germany to Japan in 1919.[31]

The Japanese invasion of Manchuria in 1931, and the Second Sino-Japanese War between 1937 and 1945 threatened the very survival of the Chinese nation. However, when the CCP declared victory and the People's Republic of China was established in 1949, the final and one of the most painful humiliations came with the Truman administration's failure to recognize the Chinese communist government.[32]

---

[25] Signed in 1842, the Nanjing Treaty ended the First Opium War and ceded Hong Kong to the United Kingdom in perpetuity, established five ports and granted most favored nation to the both the UK and France in addition to extraterritoriality.

[26] The First Sino-Japanese war was fought between the Qing Empire and the Empire of Japan between 1894 and 1895 over the Korean Peninsula as a tributary state. On the one hand, the war demonstrated the success of the Meiji restoration and of the influence of Western-style military in the Japanese army and navy; on the other, it revealed the high level of corruption and incompetence. It ended with the Treaty of Shimonoseki.

[27] A violent anti-foreign and anti-Christian movement in response to the imperialist expansion and the spread of western influences in China.

[28] The United States, the United Kingdom, Russia, Japan, Italy, Germany, France and Austria-Hungary.

[29] Signed by China, the Eight Nation Alliance, Belgium, Spain and the Netherlands, it is often regarded as one of the Unequal Treaties and forced China to pay more than what today would be $330 million USD in reparations, foreign troops were permitted to station in Beijing and China was forbidden to import arms.

[30] Also known as the Xinhai Revolution, it consisted of many revolts and uprisings that against the Qing state, which proved ineffective to modernize China and repel foreign aggression. A year after that, 1912 was declared the First Year of the Republic of China.

[31] The 1919 Treaty of Versailles transferred Shandong from Germany to Japan, instead of restoring it to China, prompting the May Fourth Movement and the spread of Marxism in China, which prepared the ideological foundation for the establishment of the Chinese Communist Party.

[32] Johnson, *China's Strategic Culture [Electronic Resource]*, 5.

The Chinese intervention in the Korean War reflected both the weight of the memory of these historical defeats, the humiliation at the hands of foreign powers that accompanied them, and the defensive to offensive nature of Chinese strategic culture. China only supported North Korea against the U.S. when the 38th parallel was crossed and the North Korean army was pushed back towards the Yalu River, which was viewed as a threat to Chinese reconstruction and security.[33]

More recently, the Chinese government's perception of the Color Revolutions in Central Europe and Asia have also influenced their national security approach.[34] This wariness of outside influence has solidified a call to control information domestically and on the periphery. China had already survived a similar scare in 1989 at Tiananmen Square, in which large scale protests advocated for more freedom of speech and press in the country.[35] As a result, China continues to be wary of Western influences, and looks on with suspicion towards any destabilizing or negative events that might be perceived as an attempt to reduce Chinese national security.

GEOGRAPHY

China's physical territory is comparable to that of the U.S., but its population of 1.2 billion people is approximately four times larger than the U.S. with sixty percent concentrated across just 600 miles

Figure 1: Map of China

[33] Johnson, 6.
[34] Titus C. Chen, "China's Reaction to the Color Revolutions: Adaptive Authoritarianism in Full Swing," *Asian Perspective* 34, no. 2 (2010): 6.
[35] Emilio Iasiello, "China's Cyber Initiatives Counter International Pressure," *Journal of Strategic Security* 10, no. 1 (2017): 15, https://doi.org/10.5038/1944-0472.10.1.1548.

of the country's coast.[36] The vast majority of the country's land is sparsely populated and maintains natural features that have made it historically difficult to defend.[37] A cartographic depiction of China can be found in Figure 1.[38]

China shares geographic borders with a large conglomeration of nation-state powers that may pose potential national security threats. Land borders with Russia, North Korea, Vietnam, India, and Pakistan, as well as contested sea claims with South Korea and Japan among others, continue to represent a source of conflict and dispute.[39] These geographical elements have prompted a constant fear of invasion that arguably persists even in the modern era.

Thus, a strong desire to protect its sovereign physical geography and national borders is indicative of the influence that geography and experience have had on Chinese actions across multiple domains. Stemming from predominately negative historical experiences with the West in 19th century, national sovereignty evolved into a defining feature of China's national geographic identity. Whether its political orientation was in the form of a Republic, Nationalist government, or Communist state, all forms have stressed a sovereign China.[40] Accordingly, China's perception of what constitutes its national geography,[41] remains an important feature of its strategic culture.

China has felt compelled to defend these features of its sovereignty. For example, China's "nine-dash line" claim made in 2009 to the United Nations (UN) alleged that specific land features of the South China Sea were a part of their national "marine entitlements under international

[36] Andrew J. Nathan, "China's Geography and Security Goals," Columbia University, Asia For Educators, 2009, http://afe.easia.columbia.edu/special/china_1950_china_geosec.htm#internal.
[37] A long southern coastline makes the nation susceptible to attack by sea, while its more mountainous northern border with colder conditions has historically proven to be difficult to guard against invaders; this northern border has been traditionally more sparsely populated with minority inhabitants retaining unpredictable loyalties, effectively introducing lack of an effective "buffer" zone of states to block potential invaders.
[38] *China*, 500 miles (United States: Google, ORION-ME, SK Telecom, ZENDRIN, 2018), https://www.google.com/maps/place/China/@27.8781788,87.199404,4z/data=!4m5!3m4!1s0x31508e64e5c642c1:0x951daa7c349f366f!8m2!3d35.86166!4d104.195397.
[39] Nathan, "China's Geography and Security Goals."
[40] Matthew Erie, "Sovereignty, Internationalism, and the Chinese In-Between," *East-West Center*, International Graduate Student Conference Series, February 19, 2004, 12.
[41] Including contested geographies like the South China Sea, Tibet and Taiwan.

law."[42] This nine-dash line reference illustrates how China has sought to pursue a specific type of approach to its geography that is supported by the adoption of domestic legislation, as well as the establishment of advantageous international laws and norms.

Another influencing element and present-day geographic association is the application of China's Great Wall methodology as an attempt to achieve similar strategic objectives.[43] Although the wall constituted a physical and material attempt to prevent invasions from adversaries, it also eventually became largely symbolic as well.[44] This psychological representation is still strongly represented today in its application to Chinese national security and the desire of the government to prevent outside influence through knowledge. State control has become an overtly stated strategic objective of the Chinese government in recent years. This concept of information dominance and mastery can link back to Sun Tzu's approach to warfare. Specifically, the value of "foreknowledge," and the employment of spies to gain knowledge of an enemy's disposition results in acquisition of the "highest intelligence," thereby further enabling "great results."[45]

POLITICS

[42] Joel P. Trachtman, "Integrating Lawfare and Warfare," *Boston College International and Comparative Law Review; Newton* 39, no. 2 (2016): 273.

[43] Initial construction of the great wall precedes Sun Tzu and dates back to third century B.C., with some sections of the wall being built during the "Warring States Period."

[44] The Great Wall came to represent both a physical "manifestation of Chinese strength" and psychological "representation of the barrier maintained by the Chinese state to repel foreign influences and exert control over its citizens."

[45] Bin Sun and Lionel Giles, *Sun Tzu on the Art of War: The Oldest Military Treatise in the World* (Champaign, Ill: Project Gutenberg, 2016), 89–93, https://ezproxy.cul.columbia.edu/login?qurl=https%3a%2f%2fsearch.ebscohost.com%2flogin.aspx%3fdirect%3dtrue%26db%3dnlebk%26AN%3d2011517%26site%3dehost-live%26scope%3dsite.

The Legalist[46] and Confucian[47] philosophies have historically maintained a profound impact on social and governing systems. Although not as popular in modern China, legalism has still had a profound effect on how the government conducts itself. When faced with the threat of losing control, the Chinese governments have been observed resorting to "some degree of legalism."[48] The effects of this approach continue to be personified through the modern day Chinese Communist government.

Instead of using "The Analects" from Confucius's most famous writings, the CCP has chosen to adopt the "imperial Confucius" methodology that stresses "obedience to the emperor, hierarchy, and loyalty instead.[49] Moreover, the Confucian concept of "harmony" has reemerged, and is understood by China's government as the individual fulfillment of responsibilities within society that results in prosperity for the state as a whole.[50]

Confucian values also contributed to a monism of political authority that radiates from the virtuous ruler, thus tending to promote bureaucratic centralism. This "addiction to the ideal of unification" comes since the Warring States Period, when the main question for rival states was not about how to live alongside one another, but rather about which state would rule the whole.[51]

---

[46] Yuri Pines, "Legalism in Chinese Philosophy," in *The Stanford Encyclopedia of Philosophy*, ed. Edward N. Zalta, Spring 2017 (Metaphysics Research Lab, Stanford University, 2017), https://plato.stanford.edu/archives/spr2017/entries/chinese-legalism/. Legalism is a philosophy that become widely popular during the Waring States period (453-221 BCE), advocating the establishment of a "rich state and powerful army" in order to ensure "domestic stability" during this period of inter-intra state conflicts; this school of philosophy encouraged individuals to pursue interests in ways that would only benefit the state. Additionally, legalism implies more than the terminology found in its naming convention. Accordingly, legalism (known as "fa") also refers to "methods, standards, impersonal regulations and the like," making it more broadly applied than the rule of law concept (known as "fa jia").

[47] Confucian philosophy is known to have been an opposing view of legalism, before predominately supplanting the predominant legalist viewpoint. However, the ancient Confucian philosophy has been adapted to meet the needs of China's communist political structure.

[48] Emily Mark, "Legalism," Encyclopedia, *Ancient History Encyclopedia* (blog), January 31, 2016, https://www.ancient.eu/Legalism/.

[49] Simon Worrall, "Why Is Confucius Still Relevant Today? His Sound Bites Hold Up," National Geographic, National Geographic News, March 25, 2015, https://news.nationalgeographic.com/2015/03/150325-confucius-china-asia-philosophy-communist-party-ngbooktalk/.

[50] Worrall.

[51] Christopher A. Ford, An Interview with Christopher A. Ford, interview by Mengjia Wan, November 1, 2016, 3, http://www.nbr.org/research/activity.aspx?id=718.

Consequently, the role of the Party today, as it relates to state control over the general population, is an important point of emphasis particularly in relation to Maoist doctrine. Accordingly, the Party remains actively involved with the general population, "engaging in propaganda, discussion, persuasion, and exhortation to gauge mass reactions to policy and to lead mass action."[52] The importance of the population in Chinese Communist doctrine is continually underscored as vital. Consequently, this importance constitutes the Maoist approach to mobilization known as "the mass line," which refers to the Party's dependence on the masses to achieve its desired goals; this reference is meant to highlight the importance of "mass participation in the execution, rather than in the formulation, of policy."[53] Furthermore, the Party's desire to thoroughly regulate the flow of information to its general populace remains an evident influence in Chinese domestic politics as the CCP remains committed to ensuring long-term survival of the regime.

ECONOMY

The historical defeats and painful humiliations at the hands of foreign powers discussed in section 3.1.1 became the seed for the three forms of Chinese nationalism: i) Nativism;[54] ii) Anti-traditionalism;[55] and iii) Pragmatism.[56] Most observers would agree that pragmatism is the dominant form of nationalism, at least since the late 1970s when the Chinese government started reforming and modernizing the economy.[57]

---

[52] Stanley Lubman, "Mao and Mediation: Politics and Dispute Resolution in Communist China," *California Law Review* 55, no. 5 (November 1967): 1303, https://doi.org/10.2307/3479330.

[53] Lubman, 1303.

[54] Nativist nationalism identifies the sources of China's weakness as foreign intervention and the consequent subversion of Chinese virtues. It the return to Confucian tradition and self-reliance as the best strategy to revitalize the nation.

[55] Contrary to nativist nationalism, anti-traditional nationalism believes that Chinese tradition and culture are the source of China's weakness and advocates for the adoption of certain foreign traits and models as the road to modernization.

[56] Pragmatic nationalism believes that the source of China's weakness is its economic backwardness. Therefore, it should use whatever it is necessary to modernize its economy, regardless of whether that is national or foreign, modern or traditional.

[57] In 1978, the Communist Party of China let by Deng Xiaoping started the "Socialism with Chinese characteristics" program of economic and market reforms. In the first stage, agriculture was decollectivized, entrepreneurs were allowed to start businesses and foreign investment was allowed in the country. During the second stage, privatization and outsourcing of state-owned industries were accompanied by the removal of price controls and some regulations.

Chinese nationalism is as much about the pride of being Chinese as it is about the shared recollection of past humiliations; it is the desire to return to greatness with sustained economic progress, which is viewed as the primary means to achieve this revival. The importance placed on economic advancement and modernization is reflected within China's efforts to improve its political and security standing around the world, guarantee its access to raw materials and technologies, as well as its placement within international markets for the export of its goods. As it seeks to rise again to great power, China knows that its development depends on a certain degree of world peace, which might help explain the change in China's approach to multilateralism since 1971.[58] In this sense, China's public commitment to its 'peaceful rise' can be explained as a strategy to let the U.S. bear the burden of maintaining the status quo around the world for a couple of decades, thereby allowing China to retool its economy and "then the world's balance of power [will be] forever altered."[59]

As China continues to orient itself towards preemption, it remains focused on growing its economy through industrial advancements as opposed to physical confrontation. The cultural variable of "guanxi" governs interactions within business and introduces "moral obligations that stem from personal relationships above all other considerations;" if relationships require gifts in exchange for certain "favors," guanxi likely supports this exchange.[60] This relationship can be constituted through different types of business exchanges. Transactions within guanxi can be monetarily based, but also might be "'hidden' and not made obvious to the casual observer;" this could include hosting dinners or providing invitations for potential clients.[61]

RELIGION

The religious variable within Chinese culture also accounts for important contributions to its strategic culture. A closer look at the influences of Sun Tzu's approach to warfare reveals

[58] China entered the United Nations in 1971 and has joined all the major intergovernmental organizations within its system, in addition to Asian regional economic, security and political organizations.
[59] Lisa Margonelli, *Oil on the Brain: Adventures from the Pump to the Pipeline* (New York: Nan A. Talese/ Doubleday, 2007), 268.
[60] Scott Stewart, "Guanxi: How Business Is Done in China," Stratfor: Worldview, April 27, 2017, https://worldview.stratfor.com/article/guanxi-how-business-done-china.
[61] "What Is Guanxi?," World Learner Chinese, accessed March 20, 2018, http://www.worldlearnerchinese.com/content/what-guanxi.

significant impacts from Taoism. In fact, 'Tao' is considered to be the "core of the overall framework" for "The Art of War."[62] Further within Tao itself, a balance between the two variables of "Yin" and "Yang" is revealed to constitute the two essential ideas within Sun Tzu's general perspective that have permeated into China's current national strategy.[63] Additionally, this balance in 'Tao' is distilled through two distinctive ideas. First, Sun Tzu's general perspective towards warfare includes prudence and victory without battle; and second, Sun Tzu's strategies and tactics on balancing are grounded on the notion of "Shi" or "situational momentum."[64] Accordingly, the concept of 'Shi' is very much still present in the way China formulates its strategic approach to national security. Mainly, 'Shi' is considered to be a Chinese strategy used to "exploit the 'strategic configuration of power' to its advantage and maximize its ability to preserve its national independence and develop its comprehensive national power."[65] This cultural element linked to 'Tao' is not only evident within Sun Tzu's strategic philosophy, but also appears to remain a vibrant influence in how China views the achievement of its national security objectives.

Other important aspects of Chinese culture influence this religious variable as well. The concept of Guanxi (mentioned earlier in relation to China's economy variable) is also related to religious influences on Chinese strategic culture as well. "Guanxi" is meant to embody "sharing favors between individuals, connections, relationships, and the ability to exert influence, while the concept of "mianzi" loosely translates to "face" or "saving face, losing face, and giving face."[66] With both concepts indicating a concern with national image, this "non-kinetic, non-violent, but still offensive" strategy provides an operational concept directly aligned with Sun Tzu's deeply rooted 'Tao' approach to warfare.[67] Additional contributing elements within the mianzi concept

[62] Peter Ping Li and Monsol Young, "How to Approach the Ancient Chinese Wisdom? A Commentary Concerning Sun Tzu's The Art of War," *Management and Organizational Review*, Dialogue, Debate, and Discussion, 13, no. 4 (December 2017): 913, https://doi.org/10.1017/mor.2017.60.
[63] Ping Li and Young, 914.
[64] Ping Li and Young, 914.
[65] David Lai, *Learning from the Stones [Electronic Resource]: A GO Approach to Mastering China's Strategic Concept, Shi* (Carlisle, PA: Army War College, Strategic Studies Institute, 2004), 1, https://permanent.access.gpo.gov/lps51974/LPS51974.pdf.
[66] Emilio Iasiello, "China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities," *Journal of Strategic Security* 9, no. 2 (Summer 2016): 50.
[67] Iasiello, 50–51.

are also important to mention as well. The Chinese are often thought of as "relational beings" connected through specific obligations identified as "qing" (affection), "yi" (righteousness), "bie" (distinction), "xu" (order), and "cheng" (society); this emphasis provides insight into the importance of mianzi by explaining the attention paid "to the kind of respect that is given to or given by others."[68] This view of respect is an important element within the religious variable, as a perceived lack thereof from perceived adversaries can provide an impetus for certain types of behavior or actions.

PHILOSOPHY

Modern Chinese philosophy has been influenced through various internal and external sources of information. In addition to early Chinese philosophers being heavily influenced by European and American political thought, science, and philosophy, Confucian influence (referenced within the politics variable as well) also continues to endure as its classical education is applied to new concepts that have been introduced within the twentieth century.[69] Other influential texts include "The Book of Great Unity" (Datongshu) developed from Buddhist views on "the inevitability of suffering," and Confucian teachings on "perfectibility of humanity;" the "Tianyanlun" text that discusses the tenets of social Darwinism provided some influence on this variable as well.[70]

Additionally, another prevalent philosophical approach is embodied through the Chinese conceptualization of deterrence, and the idea of compelling certain actions from a perceived adversary. The Chinese philosophy on deterrence is typically referred to as "weishe,"[71] a strategic concept employed to prevent the enemy from making certain movements, and to also

[68] Rodney Chu Wai-chi, "The Dynamics of Cyber China: The Characteristics of Chinese ICT Use," *Knowledge, Technology, & Policy* 21, no. 1 (March 2008): 31, https://doi.org/10.1007/s12130-008-9043-y.
[69] Evan Lampe, "Cultural History of Reading," in *Modern China*, ed. Gabrielle Watling, vol. 1 (Westport, CT: Greenwood Press, 2008), 317, http://go.galegroup.com.ezproxy.cul.columbia.edu/ps/i.do?p=GVRL&u=columbiau&id=GALE%7CCX2441100023&v=2.1&it=r&sid=summon&authCount=1.
[70] Lampe, 317.
[71] Kevin Pollpeter, "Part II Military Strategy and Institutions, Chapter 6: Chinese Writings on Cyberwarfare and Coercion," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (Oxford University Press, 2015), 13, http://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780190201265.001.0001/acprof-9780190201265-chapter-6.

force an enemy to take actions that are advantageous to China.[72] Accordingly, weishe can be viewed as another embodiment of Sun Tzu's philosophical approach to conflict, focusing on the avoidance of prolonged conflicts with capable adversaries.

Within Chinese philosophy on coercion lies three separate and distinct elements: "capability, will, and signaling," with capability and will constituting the "two 'wings' of coercion."[73] Concurrently, signaling[74] is a vitally important element within coercion. Although will and capability remain essential, the effective communication of these elements is vital in an effort to make targets aware of the full costs associated with a conflict.[75] If these warnings and signals continue to go unnoticed, then China may be compelled to deploy more offensive capabilities.[76]

China's Cyberwarfare Strategies and Capabilities

The influence of the aforementioned independent variables for Chinese strategic culture has resulted in the emergence of a distinct cyberspace strategy. That is, a formulation for how China views the use of cyberspace in achieving its national strategic objectives. Accordingly, China's global advancements in Information and Communications Technology (ICT) reflect its strategy of "informatization" of all national civilian and military infrastructure, which is meant to ensure sustained economic growth, an ability to compete internationally regarding ICT, and an effective means to safeguard its national security.[77] China's subsequent strategy can therefore

---

[72] Pollpeter, 13.

[73] Pollpeter, 14.

[74] Paul H.B. Godwin and Alice L. Miller, "China's Forbearance Has Limits: Chinese Threat and Retaliation Signaling and Its Implications for a Sino-American Military Confrontation," ed. Phillip C. Saunders, *Institute for National Strategic Studies: National Defense University Press*, China Strategic Perspectives, April 2013, 29. The concept of signaling and early warning has been prevalent in a number of conventional Chinese actions. In China's response to international crisis or disputes, it often begins with public warnings and statements which is then followed by escalatory statements with explicit warnings of military force.

[75] Pollpeter, "Part II Military Strategy and Institutions, Chapter 6: Chinese Writings on Cyberwarfare and Coercion," 14.

[76] Axelrod, "A Repertory of Cyber Analogies," 110. One reference that personifies this element of coercion was China's decision to take a military stand in defense of North Korea during the Korean War. Although China provided warning according to this methodology, the continued U.S. route of North Korean land forces prompted China to cross the Yalu River to repel their advance; contact with U.S. forces was minimal at first to present another level of warning but was subsequently followed by a much larger response once this warning was perceived to be ignored.

[77] Mark A. Stokes, Jenny Lin, and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure" (Project 2049, November 11, 2011), 2, https://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf.

be illustrated according to six dependent variables that demonstrate China's cyber capabilities, methods, and motivations. Consequently, how China understands the role of force in state affairs, nature of the threat, efficacy in the use of force, use of non-state actors and proxies, legal frameworks, and the military-civilian relationship constitute the variables that effectively illustrate its capabilities, methods, and motivations by, with, and through cyberspace. This approach is distinct to China and has been shaped through the construct of its own strategic culture variables (history, geography, politics, economy, religion, and philosophy).

DEPENDENT VARIABLES

ROLE OF FORCE IN STATE AFFAIRS

Although China has not been known to make a habit out of engaging in large-scale violent military conflicts following the Korean War, its expenditure on the instruments of war has exponentially grown over the past 25 years to nearly $225 billion (illustrated in Figure 2 from the Stockholm International Peace Research Institute).[78] This begs the question of how China sees the role of force in its state affairs since it has shown itself to be relatively innocuous when it comes to traditional forms of conflict and confrontation. Accordingly, the role of asymmetric warfare within cyberspace that China has sought to exploit cannot be ignored. Moreover, how China views the role of this asymmetric confrontation during the modern era stems from the lessons it learned observing U.S. engagement during Operation Desert Storm; it was at this point that Chinese military leaders observed what they perceived to be an important role of "computer viruses to disrupt Iraqi information systems."[79]

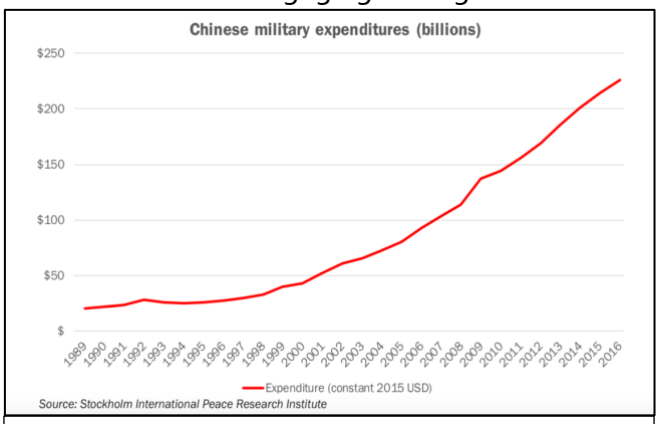


Figure 2: Stockholm International Peace Research

The PLA specifically began to shift focus in this regard: PLA strategists started to concentrate planning considerations on the role of Information Technology (IT) in connecting forces on the battlefield, the exploitation of vulnerabilities within IT systems, and the drafting of new doctrine for fighting in "high-tech" conflicts.[80] Observing U.S. operations during Operation Desert Storm

---

[78] Bruce Jones, "Containment, Competition, and Cooperation in US-China Relations," ed. Ryan Hass, Tarun Chhabra, and Bruce Jones (Brookings Institution, November 21, 2017), 3, https://www.brookings.edu/wp-content/uploads/2017/11/fp_20171121_china_interview.pdf.

[79] Arun Warikoo, "Cyber Warfare: China's Role and Challenge to the United States," *Himalayan and Central Asian Studies; New Delhi* 17, no. 3/4 (December 2014): 62.

[80] Samuel Klein, "Beyond Capabilities: Investigating China's Military Strategy and Objectives in Cyberspace," *The Cyber Defense Review*, December 3, 2016. Available at Samuel Klein, "Beyond Capabilities: Investigating China's Military Strategy and Objectives in Cyberspace," The Cyber Defense Review, December 3, 2016, http://cyberdefensereview.army.mil/The-Journal/Article-Display/Article/1136045/beyond-capabilities-investigating-chinas-military-strategy-and-objectives-in-cy/.

provided Chinese military leaders with an illustration of how precise and effective interconnected joint operations could be. The leveraging of IT and information systems better enabled communications between soldiers, sailors, marines, and airmen. This observation served as a "major wake-up call" for both the CCP and the PLA.[81] The consequent result was an abrupt change in course for Chinese military strategy. PLA leadership witnessed the potential of "enhanced Information Warfare (IW), networked systems, and 'digitalized' combat forces," which resulted in their strategic focus on "informatization."[82]

For China, the role of cyber has evolved into a means of advancing state affairs in multiple realms to include economic, political, and military.[83] It can be argued that China's military cyber strategy exists not only as a primary instrument to advance political goals, but also as an effective mechanism to achieve both economic and military objectives it views as essential for national security. Accordingly, the Chinese military holds the role of cyber warfare in high regard as "the best way to neutralize an enemy that is technologically superior;" the People's Liberation Army (PLA) doctrinally views these tactics as extremely effective in the achievement of both political and military goals.[84] Cyber remains a primary component of the PLA's overall IW strategy. As a result, Chinese military doctrine considers IW[85] a primary means to achieve information dominance in order to counter larger and more capable adversaries.[86]

Within this IW doctrine, the components of the "Three Warfare" strategy are relevant in discussing the role of force in China's state affairs. Consequently, China's IW approach is described as a "three-prong information warfare approach" that includes media, legal, and psychological components.[87] Although "legal warfare" will be subsequently discussed within the legal framework variable, the concept of "lawfare" has been characterized by some as a "strategy of using-or misusing-law as a substitute for traditional military means to achieve a

[81] *Ibid.*
[82] *Ibid.*
[83] Thomas Waldman, "Politics and War: Clausewitz's Paradoxical Equation," *Parameters; Carlisle Barracks* 40, no. 3 (Autumn 2010): 2.
[84] Warikoo, "Cyber Warfare: China's Role and Challenge to the United States," 62–63.
[85] Known as "xinxi zhanzheng."
[86] Warikoo, "Cyber Warfare: China's Role and Challenge to the United States," 63.
[87] Iasiello, "China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities," 45.

warfighting objective."[88] Therefore, just as law has been specifically used by China to legally enable cyber operations, lawfare acts as an integrated component of the modern warfare approach the state takes to both domestic and international confrontations.

The psychological element of warfare is aimed at destabilizing the ability of perceived enemies to conduct combat operations.[89] Psychological warfare is in many ways considered to be "the most far-reaching," with a stated goal that focuses on the ability to "influence, constrain, and/or alter an opponent's thoughts, emotions, and habits while at the same time strengthening friendly psychology."[90] China views the role of psychology in warfare to be an integral doctrinal concept for the PLA. Accordingly, PLA writings stipulate a need to conduct this type of warfare within the political, economic, technical, and military realms during peacetime operations in order to effectively construct operational plans, successfully conduct gain-loss analysis, and to ultimately gain an advantage that allows the PLA to dictate levels of attack.[91] In addition to a seemingly offensive employment of psychological warfare, China also utilizes a defensive variation oriented towards strengthening indoctrination as well.[92]

China seeks to use the public opinion and media element of the "Three Warfare" strategy to influence both domestic and international public opinion in support of Chinese military actions and interests.[93] Its purpose is to "shift the overall balance of strength between a nation and that nation's components."[94] Accordingly, Chinese writing on public opinion is constituted through

---

[88] Trachtman, "Integrating Lawfare and Warfare," 268.

[89] Iasiello, "China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities," 51. This objective can be achieved by "deterring, shocking, and demoralizing the enemy military personnel and supporting civilian populations."

[90] Dean Cheng, "Winning Without Fighting: The Chinese Psychological Warfare Challenge," Backgrounder (Washington, DC: The Heritage Foundation, April 11, 2013), 2, /global-politics/report/winning-without-fighting-the-chinese-psychological-warfare-challenge.

[91] Cheng, 2.

[92] To combat perceived enemy counter-messages, preempting counter-psychological warfare efforts to preserve uniformity of one's own domestic population, forces, and leaders, controlling public opinion through media and strategic communications, and focusing on creating strong national solidarity through politically unifying efforts. A defensive approach is characterized through strong counter-operations to combat the influences of enemy-messaging efforts.

[93] Iasiello, "China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities," 51.

[94] Dean Cheng, "Winning Without Fighting: Chinese Public Opinion Warfare and the Need for a Robust American Response," Backgrounder (Washington, DC: The Heritage Foundation, November 26, 2012), 4, /global-politics/report/winning-without-fighting-the-chinese-psychological-warfare-challenge. With expressed goals of

the following pillars in framing military operations: following top-down guidance, emphasis on preemption, exploitation of all available resources, and flexible response.[95] As with the other elements of warfare applied to Chinese state affairs, both offensive [96] and defensive [97] applications can be employed.[98] These capabilities are expressly manifested within China's Great Firewall and Great Cannon references, which provide the state distinct mechanisms to assume both offensive and defensive postures. The Great Firewall acts to prevent information from sources perceived to be detrimental to the national message, while the Great Cannon provides an offensive platform to launch cyber-attack operations against anti-government targets as a show of force.

NATURE OF THE THREAT

According to Alastair I. Johnston, Chinese strategic culture does not necessarily demonize the enemy, but considers that it can be enculturated and pacified.[99] Security is multidimensional: it is in part a function of the behavior of the adversary and in part a function of one's own internal cohesion and socioeconomic well-being. Some scholars trace the roots of the minimal-violence doctrine to Sun Tzu's notion of "not fighting and subduing the enemy" and others to Lao Zi's "softness to overcome hardness."[100] However, Johnston points to the Confucian "emphasis on the ruler's cultivation of virtue and good government as the basis for the security and prosperity of the state."[101] External security rests on creating conditions such that people will be content with their place in the socioeconomic and political order, causing the adversary to submit willingly to the ruler's authority.[102]

---

preserving friendly morale, generating public support at home and abroad, weakening the will of a perceived enemy to fight, and to introduce information that acts to alter an enemies sense of China's intentions, capabilities, or military objectives.

[95] Cheng, 3–4.

[96] The offensive approach is typically geared towards weakening an opponent's will and support.

[97] A defensive approach is characterized through strong counter-operations to combat the influences of enemy-messaging efforts.

[98] Cheng, "Winning Without Fighting," November 26, 2012, 4–5.

[99] Johnston, *Cultural Realism*, 62–64.

[100] Johnston, 63.

[101] Johnston, 62–64.

[102] Alastair Iain Johnston, *Cultural Realism. Strategic Culture and Grand Strategy in Chinese History*, Princeton University Press (United States, 1995), pp. 64-66

Chinese leadership views a majority of critical threats as emanating from outside. Of particular importance to the cyber domain is the U.S. relationship with Taiwan,[103] since it has emerged as a global supplier of information technology and components.[104] China's weariness to outside threats is rooted in the Century of Humiliation, its perception of the Color Revolutions, and Tiananmen Square experience. Viewed through a Confucian lens, China's desire for economic progress and modernization is an attempt to restore previous humiliations by confronting perceived adversaries through its conception of socioeconomic betterment.

Multiple landmark events have also demonstrated how this Chinese threat perception has continued to be reinforced. The 1999 Chinese embassy bombing in Belgrade during the Kosovo War and 2001 aircraft collision with an American pilot were both influential events that reinforced Western suspicions. In contrast to what the U.S. considered an accidental bombing, China viewed the destruction of its Belgrade embassy as both a "barbaric attack" and "gross violation of Chinese sovereignty" that reinforced a general feeling of mistrust about U.S. nature and intentions.[105] This prompted some of the first observed Chinese deployments of cyber capabilities in support of specified political objectives. Following this event, Chinese citizens mobilized to deface several U.S. government websites that included the Department of the Interior, the U.S. Embassy in Beijing, and the Department of Energy; these types of defacement operations subsequently continued as a tactic against regional adversaries like Taiwan as well.[106] China also employed similar tactics following the collision of a U.S. surveillance plane and Chinese fighter in 2001, an event that coincided with the second anniversary of the Belgrade

[103] China perceives an independent Taiwan as a threat to Chinese legitimacy.
[104] Frank W. Simcox, "Flexible Options for Cyber Deterrence," Research Paper (Maxwell AFB Montgomery AL: Air War College Center For Strategy and Technology, February 11, 2009), 117, http://www.dtic.mil/docs/citations/ADA539892.
[105] James Griffiths, "How China Used the US Bombing of Its Belgrade Embassy to Win a PR Victory," Public Radio International, May 5, 2014, https://www.pri.org/stories/2014-05-05/how-china-used-us-bombing-its-belgrade-embassy-win-pr-victory.
[106] Dorothy Denning, "Cyberwarriors," HIR: Harvard International Review, May 6, 2006, http://hir.harvard.edu/article/?a=905.

embassy bombing.[107] These tactics have continued in recent years as well regarding Chinese regional disputes.

This past September, Hong Kong's pro-Democracy party "Demosisto" had its website defaced with patriotic pro-Chinese messages in response to the pro-Hong Kong independence movement. This attack was in addition to a 2016 intrusion targeting two Hong Kong government departments prior to their legislative elections.[108] These response actions continue to demonstrate an evolution in how China has sought to combat perceived threats from outside actions and influences.

The advantageous nature of cyber operations provides China with numerous motivations, such as deterrence of other states by infiltration of their critical infrastructure, acquisition of knowledge through cyberspace espionage in order to quickly facilitate military advancements, and most importantly, the attainment of economic gains through industrial espionage to advance their technologies. Use of these actions in cyberspace can partially be attributed to prolonged inequities experienced by China at the hands of Western powers, thereby providing a perceived justification for these cyber actions that are meant to help close the gap created by these historical humiliations.[109] Consequently, even though China's recent initiation of efforts like the "Information Silk Road" (encompassed by the OBOR initiative) have been viewed as a way to gain control of more information, it is primarily thought to be a part of the Chinese broader strategy to enhance its economic standing, operation, and growth through "e-commerce, digital economy, smart cities, science and technology."[110]

EFFICACY OF THE USE OF FORCE

[107] Pamela Hess, "China Prevented Repeat Cyber Attack on US," UPI, October 29, 2002, https://www.upi.com/China-prevented-repeat-cyber-attack-on-US/51011035913195/.

[108] Raquel Carvalho, "Cyberattackers Hack Website of Hong Kong Pro-Democracy Party Demosisto," *South China Morning Post* (September 9th, 2017). Available at: http://www.scmp.com/news/hong-kong/law-crime/article/2110477/cyberattackers-hack-website-hong-kong-pro-democracy-party (last consulted: May 2018)

[109] Jason Healey, "Dynamics of Cyber Conflict Class 7" (Dynamics of Cyber Conflict Course, Columbia University School of International and Public Affairs, March 5, 2018).

[110] Rachel Brown, *Beijing's Silk Road Goes Digital*, Council on Foreign Relations (June 6, 2017), available at: *https://www.cfr.org/blog/beijings-silk-road-goes-digital* (last consulted: March 2018).

China's interpretation of the efficacy of force is predominately non-kinetic but still maintains a propensity to be offensively oriented. Sun Tzu's concept of achieving victory without the use of force has been linked to China's use of cyberspace as a medium to gain advantages against larger countries with superior military capabilities like the United States. More specifically, Sun Tzu's [111] advocacy for "the implementation of non-kinetic, non-violent, but still offensive operations" to influence the "cognitive processes of a country's leadership and population" draws applicable linkages to China's utilization of cyberspace in support of its peacetime strategy. [112] China is assessed to lead the world in the number of attributed hostile cyber incidents and is considered to maintain one of the best overall offensive cyber capabilities in the world.[113] These non-violent actions in cyberspace have been predominately expressed through attempts to achieve information dominance in both critical sectors of industry, as well as foreign government intelligence institutions.[114]

China approaches the efficacy of force through predominately asymmetric means, as it understands that it does not match well conventionally with perceived Western adversaries. Accordingly, China possesses a strategic interest in deterring other states by infiltrating their critical infrastructure, acquiring knowledge through cyberspace espionage, and attaining economic gains through industrial intellectual property theft; these actions are taken in an

[111] A closer look at the influences of Sun Tzu's approach to warfare reveal significant impacts from Taoism, considered to be the "core of the overall framework" for "The Art of War." Further within Tao itself, a balance between the two variables of "Yin" and "Yang" is revealed to constitute the two essential ideas within Sun Tzu's general perspective that have permeated into China's current cyber strategy. This balance in 'Tao' is distilled through two distinctive ideas. First, Sun Tzu's general perspective towards warfare includes prudence and victory without battle; and second, Sun Tzu's strategies and tactics on balancing are grounded on the notion of "Shi" or "situational momentum."

[112] Iasiello, "China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities," 51.

[113] Marc R. DeVore and Lee Sangho, "APT(Advanced Persistent Threat)s and Influence: Cyber Weapons and the Changing Calculus of Conflict," *The Journal of East Asian Affairs; Seoul* 31, no. 1 (Spring/Summer 2017): 48.

[114] The U.S. Office of Personnel Management (OPM) intrusion that resulted in the exfiltration of biometric data for 5.6 million Federal employees, acquisition of sensitive F-35 fighter aircraft information from Lockheed Martin, and the targeted spear-phishing campaign to obtain network manager information from EMC Corporation's Security Division are all examples of China's non-violent offensive actions through cyberspace. This operational employment has been integrated into the doctrinal approach utilized by the PLA. The Anti-Access Area Denial (A2AD) doctrine emphasizes the use of cyber capabilities against perceived adversaries like the U.S. in order to prevent intervention in East Asian conflicts; employment of these capabilities would likely be oriented to prevent American intervention in conventional conflicts over contested geography like the Taiwan Strait. As previously discussed in the philosophy and religion sections, opportunities that can provide a political or military advantage for China are often the focus of exploitation.

attempt to avoid political and military pressure, accelerate its ability to rapidly develop conventional military capabilities, and to gain technological insights that hasten its economic advancement.[115] Although the "death by 1,000 cuts" reference has been used to illustrate this point in the past, stronger linkages and interdependencies between U.S. and Chinese financial markets have cast some doubt on this comparison.[116] However, this strategy still aligns with what Chinese military planners refer to as "a powerful asymmetric opportunity in a deterrence strategy;" this strategy is viewed as a means to make the costs of conventional engagements too high for other nations to interfere in China's sphere of influence.[117] Subsequently, nations considering interference measures in Chinese affairs would also need to account for second and third order effects that might negatively influence their own domestic economy, infrastructure security, and military system defenses.

Consequently, the "old wine into new bottles" parallel can be referenced when attempting to explain China's deterrent actions in cyberspace.[118] The predominant connection for this comparison initially related to similarities in nuclear deterrence strategies: nuclear deterrence represents the old wine, while cyberspace constitutes the new bottle.[119] This reference suggests a "modus operandi" comprised of punishment through coercion in the China-U.S. cyber relationship.[120] Consequently, China conducts information operations through cyberspace in an attempt to not only strengthen its own economy,[121] but to also maintain domestic stability and national security.[122]

---

[115] Magnus Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," *Journal of Strategic Security* 4, no. 2 (Summer 2011): 3.
[116] James A. Lewis and Simon Hansen, "China's Cyberpower: International and Domestic Priorities," Special Report: ASPI (Australia: Australian Strategic Policy Institute, November 2014), 2, https://www.files.ethz.ch/isn/185655/China%27s%20cyberpower_%20international%20and%20domestic%20priorities.pdf.
[117] Hjortdal, "China's Use of Cyber Warfare," 5–6.
[118] Meaning "treating the contents of a preexisting concept as if they were new."
[119] Lora Saalman, "Pouring 'New' Wine into New Bottles: China-U.S. Deterrence Relations in Cyberspace," *Seton Hall Journal of Diplomacy and International Relations* 17, no. 1/2 (2016 2015): 23.
[120] Saalman, 23.
[121] Private sector intellectual property targets, weaken both regime and international opponents, targeting of U.S. intelligence sources and military capabilities collection.
[122] Information dominance.

Accordingly, China's desire in creating a strong security environment and conducting malware-based intelligence, reconnaissance, attacks, and interruption capabilities is "to achieve military, economic, or political aims without having to send soldiers into the fight."[123] China's use of cyberspace also appears oriented towards preemption through cyber mechanisms that are focused on intellectual property and intelligence collection, as opposed to physical confrontation.

[123] Saalman, "Pouring 'New' Wine into New Bottles," 25.

NON-STATE ACTORS AND PROXIES

China's cyber strategy has evolved to account for the presence of non-state proxies as well. China's "mass line" doctrine helps to depict this relationship, which constitutes a vital component of Maoist ideology. Mao's doctrine indicates that the mass line "blurs and sometimes obscures the distinction between government and nongovernmental organizations and activity."[124] This relationship has further manifested itself in several different forms as China's strategic lens for the use of cyber capabilities has progressed. For example, the initial patriot hacker activity related to the Belgrade embassy bombing and subsequent aircraft collision events can be categorized differently than modern employment methods and motivations for these same types of capabilities. Accordingly, Jason Healey's "Spectrum of State Responsibility" (shown in Figure 3) can help to characterize this relationship; initial Chinese cyber activities can potentially be categorized as "state-encouraged" or at the very least "state-ignored," with the government tacitly supportive of this non-state activity or at a minimum overlooking it.[125] However, modern-day integration of these non-state proxies has evolved under President Xi Jinping with a focus on more consolidation and control. Classification of this modern utilization can potentially better align with the "state-integrated" spectrum category, as the national government has worked to closely integrate important third-parties with state

[124] Lubman, "Mao and Mediation," 1303.
[125] Jason Healey, "Beyond Attribution: Seeking National Responsibility in Cyberspace" (Cyber Statecraft Initiative: Atlantic Council, February 22, 2012), 2, http://www.atlanticcouncil.org/publications/issue-briefs/beyond-attribution-seeking-national-responsibility-in-cyberspace.

forces that allow for more control of national capabilities.[126] China's gradual movement up the spectrum of state responsibility is an assessment that was reiterated in an interview with Jason Healey.[127]

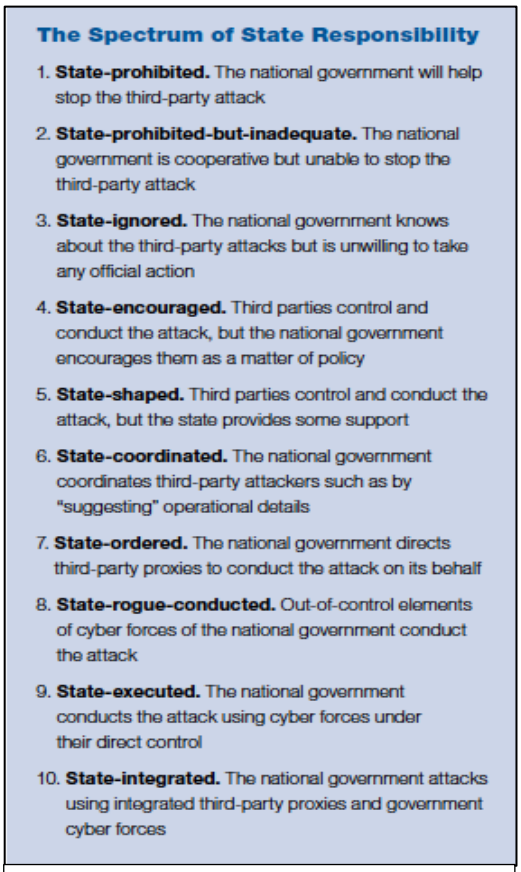


Figure 3: Spectrum of State Responsibility

Consequently, the existence of the Red Hacker Alliance[128] and China's Voluntary Fifty-Cent Army[129] demonstrate an increasingly reliance on the use of non-state actors for cyber-attacks and operations in this capacity. The Chinese continue to base their military strategy on the mobilization of the entire population in a struggle for their nation.[130] Taking this vision into the cyber domain represents a cooperative relationship between the PLA and Chinese hacker organizations like the Red Hacker Alliance; although the government denies any relationship with the Red Hacker Alliance (claiming that Chinese law forbids attacks using the Internet), it is likely the Party at a minimum tolerates its activities, which provides China with plausible deniability.[131]

The Voluntary Fifty-Cent Army can be seen as the materialization of China's use of the public opinion and media element within the "Three Warfare" strategy to influence both domestic and international public opinion in support of Chinese interests. The CCP has neither the capacity

[126] Healey, 2.
[127] Jason Healey, Discussion on Cyberspace Analogies and Strategic Culture, In Person Interview Conducted At: Columbia University School of International and Public Affairs (SIPA), March 26, 2018.
[128] Mara Hvistendahl, "Hackers: The China Syndrome," Popular Science, April 23, 2009, https://www.popsci.com/scitech/article/2009-04/hackers-china-syndrome.
[129] The colloquial term for Internet commentators, allegedly hired by Chinese authorities in an attempt to manipulate public opinion in favor of the Chinese Communist Party. The name derives from the allegation that commentators were paid fifty cents for every post.
[130] Mao Tse-tung's People's War.
[131] Simcox, "Flexible Options for Cyber Deterrence," 11–12.

nor the intention to censor all public expression;[132] in fact, "beyond a number of well-patrolled 'forbidden zones' the Chinese state speaks with many voices."[133] Although the Voluntary Fifty-Cent Army's was spontaneously born, President Xi Jinping's government has undoubtedly tried to co-opt them.[134] Moreover, compensation for this support is not necessarily directly dispersed from the Ministry of Defense, and in some cases it may be constituted through a more indirect payment in the form of state favors; this concept is further expanded upon within the subsequent military-civilian relationship output variable.[135]

China's integration of both unconventional and conventional cyber forces has also been illustrated through its employment of numerous Advanced Persistent Threats (APTs). One of the first comprehensive exposures of a Chinese-linked APT was the 2013 Mandiant report, which provided a detailed account of APT1 cyber operations (linked to PLA Unit 61398), to include infrastructure, command and control, and "modus operandi" in cyberspace.[136] The CAMERASHY report[137] was another thorough attribution assessment that followed in 2015, linking the "Naikon" APT group to the PLA Chengu Military Region Second Technical Reconnaissance Bureau (PLA Unit 78020); this unit has been associated with malicious spear phishing campaigns targeting Southeast Asian military, diplomatic, and economic targets in order to "establish beachheads into target organizations" for follow on cyber operations.[138] These threat actors are considered to be "the most sophisticated form of cyber weapon that

[132] Rongbin Han, "The 'Voluntary Fifty-Cent Army' in Chinese Cyberspace," *China Policy Institute: Analysis* (blog), February 29, 2016, https://cpianalysis.org/2016/02/29/the-voluntary-fifty-cent-army-in-chinese-cyberspace/.
[133] Rongbin Han, "Manufacturing Consent in Cyberspace: China's 'Fifty-Cent Army,'" *Journal of Current Chinese Affairs* 44, no. 2 (June 29, 2015): 105–34.
[134] Han, "The 'Voluntary Fifty-Cent Army' in Chinese Cyberspace."
[135] JD Work, Discussion on Chinese, North Korean, and Russian Conduct in Cyberspace, In Person Interview Conducted At: Columbia University School of International and Public Affairs (SIPA), March 19, 2018.
[136] "APT 1: Exposing One of China's Cyber Espionage Units" (MANDIANT, 2013), https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.
[137] "PROJECT CAMERASHY: Closing the Aperture on China's Unit 78020" (Vienna, VA: Threat Connect and Defense Group Inc (DGI), 2015), 5, https://cdn2.hubspot.net/hubfs/454298/Project_CAMERASHY_ThreatConnect_Copyright_2015.pdf. The CAMERASHY Report was a joint report issued by ThreatConnect Inc. and Defense Group Inc. that provided intelligence on the Advanced Persistent Threat (APT) group known as "Naikon;" this report provides technical analysis that constructs a case against this Chinese entity that has been targeting government and commercial interests in South Asia, Southeast Asia, and the South China Sea.
[138] "PROJECT CAMERASHY: Closing the Aperture on China's Unit 78020," 7.

exists."[139] Additionally, it has also been alleged that members of the PLA conduct cyber operations outside of their conventional military capacity. Specifically, some PLA units have been accused of conducting "moonlighting" operations for nefarious motivations and entities outside the scope of their government-sanctioned activities.[140]

Consequently, APTs are thought to be constituted through both state military units and non-state proxies as well. Specifically, the cybersecurity firm FireEye has assessed Chinese attribution for APT's 1, 3, 10, 12, 16, 17, 18, 19, and 30.[141] Significant Chinese employment of the APT construct has been observed through APT1 (linked to PLA Unit 61398 within 3PLA), APT3 (the UPS Team), and APT12 (the Calc Team); these APT's have been accused of targeting the industrial Information Technology (IT), aerospace, satellites, and telecommunication sectors, as well as journalists, governments, and the Defense Industrial Base (DIB).[142] Accordingly, these APTs have been assessed to be involved in numerous significant cyber intrusions that include Titan Rain[143], Operation Aurora,[144] and the Office of Personnel Management (OPM) breach.[145] China's integration of APT's into its military structure is indicative of its how it seeks to harness the full array of its capabilities in order to achieve national strategic objectives.

---

[139] DeVore and Sangho, "APT(Advanced Persistent Threat)s and Influence: Cyber Weapons and the Changing Calculus of Conflict," 40.

[140] Elsa Kania, "Careful What You Wish For -Change and Continuity in China's Cyber Threats," *Real Clear Defense* (April 5th, 2018). Available at: https://www.realcleardefense.com/articles/2018/04/05/careful_what_you_wish_forchange_and_continuity_in_chinas_cyber_threats_113284.html (last consulted: May 2018)

[141] "Advanced Persistent Threat Groups," FireEye, 2018, https://www.fireeye.com/current-threats/apt-groups.html.

[142] "Advanced Persistent Threat Groups."

[143] Nathan Thornburgh, "The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)," Time Archive: 1923 to the Present, September 5, 2005, http://www.cs.washington.edu/education/courses/csep590/05au/readings/titan.rain.htm.
High level targets of this attack included NASA, Redstone Arsenal, and Lockheed Martin's F-35 fighter jet plans.

[144] Kim Zetter, "Google Hack Attack Was Ultra Sophisticated, New Details Show," WIRED, January 14, 2010, https://www.wired.com/2010/01/operation-aurora/. Advanced encryption and stealth programming that exploited an Internet Explorer Zero-Day to extract source code from 34 companies in the technology, financial, and defense sectors.

[145] Brendan Koerner, "Inside the OPM Hack, the Cyberattack That Shocked the US Government," *WIRED* (blog), October 23, 2016, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/. Breach involved the compromise of sensitive U.S. government employee information, including 18 million SF 86's, 5.6 million digital fingerprint images, and 4.2 million complete personnel files; specific IP addresses, email accounts, and a domain server registered to a Marvel Comic superhero indicated involvement from known Chinese APT's

LEGAL FRAMEWORK

China's "Three Warfare" approach again provides an important context for how China views the use of legislative means to achieve its strategic objectives. In addition to psychological and public opinion/media means, "legal warfare" is highlighted as an important mechanism that allows China to gain political advantages in altering public and international opinions.[146] The scope of legal warfare focuses on building legal authorizations for government sanctioned actions. This strategic mechanism essentially refers to an attempt to achieve superiority through mobilization of both domestic and international laws to gain political initiative and military victory; tactics within this mechanism include "legal deterrence, legal attack, legal counterattack, legal binding, and legal protection."[147] This approach allows China to "claim the legal high ground or assert Chinese interests," while also providing flexibility to shape cyberspace in an advantageous way that builds international support and blunts political repercussions.[148]

Furthermore, the aforementioned concept of "lawfare" has been characteriszed by some as a "strategy of using -or misusing- law as a substitute for traditional military means to achieve a warfighting objective."[149] These legal maneuvers are further enabled through the previously examined influence of Confucian and Legalist elements previously discussed.[150]

China's legal framework is unique in how it views what constitutes cyberspace and the elements therein. In contrast to how the U.S. views this domain,[151] China takes a more holistic approach that includes both the technology aspect and the actual data traversing or stored within it as

[146] Ford, An Interview with Christopher A. Ford, 3.
[147] Sangkuk Lee, "China's 'Three Warfares': Origins, Applications, and Organizations," *Journal of Strategic Studies* 37, no. 2 (February 23, 2014): 203, https://doi.org/10.1080/01402390.2013.870071.
[148] Iasiello, "China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities," 51.
[149] Trachtman, "Integrating Lawfare and Warfare," 268.
[150] Specifically, the influence of advocated for the instrument of law to be used in an ideological mechanism that supports government. Moreover, China seeks to utilize the legal mechanisms of international institutions like the United Nations to further bolster its legal standing in cyberspace. In doing so, China can bolster its legal legitimacy for actions in cyberspace, mitigate negative attacks against those actions since it remains in compliance with international institutions, and also allows the government to further employ non-kinetic asymmetric tactics without the use of military force.
[151] Through a narrower technological lens.

well.[152] Additionally, the role of government has informed the Chinese national legal framework that was created to govern cybersecurity and actions within cyberspace. With a tremendous emphasis placed on the relationship between cybersecurity and national security, the Chinese government views itself as "a holistic enabler supporting the protection and development of economic and social initiatives;" economic initiatives are implied to include the technological elements and data within its perceived national cyberspace that drives prosperity and social harmony.[153] Consequently, President Xi Jinping's government has pursued a legal strategy that in their view fully enables the fulfillment of this perceived role. This legislation has helped provide the Chinese government with a legal mechanism that supports mitigation actions against activity it deems to be unacceptable.[154] Accordingly, a number of key cyber legislative actions have been passed and implemented over the last few years in order to advance this agenda: the "National Security Law" of 2015;[155] the "Anti-Terror Law" of 2015;[156] and the "Cyber Security Law" of 2016.[157]

China has also approached legal frameworks and norms for cyberspace from an international avenue as well. The Shanghai Cooperation Organization (SCO) is one mechanism that China has sought to utilize for initiating the establishment of global cyberspace norms. Specifically, a

[152] Iasiello, "China's Cyber Initiatives Counter International Pressure," 2.
[153] Iasiello, 2–3.
[154] Iasiello, 4.
[155] The passage of this legislation effectively outlines Chinese guiding principles for national security, definition of national security across various sectors, functions and responsibilities of the National People's Congress, important variables of the "national security regime," allocation of resources, as well as the responsibilities of citizens and corporations to ensure national security. Application of this legislative framework is meant to span across multiple domains of what China views as within its national boundaries, including the "polar beds, outer space, and cyberspace" as appropriate realms of sovereignty.
[156] This legislation seeks to "compel technology companies" to decrypt information for use by the government authorities, thereby further implementing additional monitoring, compliance, and collaboration guidelines in the interest of "national security." The vague vernacular that constitutes the Anti-Terror Law, as with other security focused legislation, continues to provide the government with maximum flexibility in taking actions that it deems necessary for protection of the state.
[157] This law addresses "key Internet and information systems and data, as well as increasing the government's power to record and impede the dissemination of information it deemed illegal." This law focuses on private industry sectors that operate within China's national borders that have been identified as critical for state security. Consequently, the legal scope predominately includes new network security guidelines for telecoms, energy, transport, finance, national defense, and government administration. This legal instrument provides the Chinese government with an enhanced capability to monitor and control information, as well as a legal mechanism to enforce foreign enterprise compliance.

2009 agreement between SCO members[158] regarding cooperation in the Field of Ensuring International Information Security concluded with the submission of an initial draft International Code of Conduct for Information Security to the UN General Assembly in 2011; an updated draft was submitted for consideration in 2015 as well despite Western reservations.[159] China continues to pursue this international initiative in an attempt to solidify its concept of sovereignty.

These legislative frameworks and agreements have emerged as an important vehicle that better enables the protection of Chinese national sovereignty. This concept is manifested through an idea of "Internet sovereignty" that encompasses all individual and organizational entities operating within Chinese territory, as well as the legislation that binds their compliance to these mandated regulations.[160] This type of legal mechanism lacks kinetic military maneuvers, is absent of violence, and appears to align with what other countries also view as nationally important.

MILITARY-CIVILIAN RELATIONSHIP

The Chinese military-civilian relationship is intricately linked, as the relationship between the PLA and CCP remains a top-down architecture. Historically, the PLA possessed a continued allegiance to political leaders, influence in selection of the Chinese civilian leadership hierarchy, and an ability to shape the domestic political environment.[161] This characterization of the civil-military relationship evolved from Mao's 'People's War' doctrine, which emphasized utilization and mobilization of the Chinese population as critical to its ability in gaining a military advantage.[162] Although this relationship has somewhat evolved over the past 20 years, the PLA

[158] SCO Member States include: China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan.
[159] "Shanghai Cooperation Organization," Resources, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), July 29, 2014, https://www.ccdcoe.org/sco.
[160] Shannon Tiezzi, "China's 'Sovereign Internet,'" The Diplomat, June 24, 2014, https://thediplomat.com/2014/06/chinas-sovereign-internet/.
[161] Michael Kiselycznyk, "Civil-Military Relations in China: Assessing the PLA's Role in Elite Politics," ed. Phillip C. Saunders (Institute for National Strategic Studies: National Defense University Press, 2010), 1, https://permanent.access.gpo.gov/gpo16358/ChinaPerspectives-2.pdf.
[162] Nicholas Lyall, "China's Cyber Militias: China's Cyber Power Is in the Grip of Dual Trends - Pluralism and Centralization," The Diplomat, March 1, 2018, https://thediplomat.com/2018/03/chinas-cyber-militias/.

and CCP still maintain close ties and continue to focus on the achievement of China's national security objectives.

President Xi Jinping has taken action in recent years to further solidify this relationship. Accordingly, President Xi has "made the military central to his presidency and a main pillar of his personal authority." This includes taking the title of "Commander-in-Chief" for joint operations, a title that has not been used since Zhu De under Mao Zedong.[163] This relationship is evident in the previously discussed concepts of "lawfare" and "legal warfare," which further demonstrate the development of legislation as a direct mechanism to achieve both military and political objectives in cyberspace.

The interwoven connections between the government, the PLA, and some civilian industries also helps to characterize this relationship as it relates to cyberspace. Technology companies like Huawei, which operates in hundreds of countries and is the second largest supplier of telecommunications equipment in the world, maintain suspected links to the Chinese military and government.[164] This relationship aligns with how China's digital military strategy is thought to be constructed. Consisting of three separate sections, this interwoven construct includes: one unit known as the "specialized military network warfare forces" that is responsible for carrying out cyber-attacks and defense, a second unit comprised of civilian teams that are authorized by the military to conduct "network warfare operations," and a third unit acting outside of government departments that focuses on "external entities."[165] Additionally, this alignment has likely contributed to the effectiveness of China's "Golden Cyber-Shield."[166] This reference has

[163] Charles Clover, "Xi's China: Command and Control," *Financial Times* (blog), July 26, 2016, https://www.ft.com/content/ddeoaf68-4db2-11e6-88c5-db83e98a590a.
[164] Justin Hienz, "Chinese Cyber Attacks Are Looting U.S. Private Sector," *Defense Media Network* (blog), June 26, 2012, https://www.defensemedianetwork.com/stories/chinese-cyber-attacks-are-looting-u-s-private-sector/.
[165] Charlie Osborne, "China Reveals Existence of Cyber Warfare Hacking Teams," *ZDNet* (blog), March 20, 2015, http://www.zdnet.com/article/china-reveals-existence-of-cyber-warfare-hacking-teams/.
[166] The "great firewall of China" is synonymous with its "Golden Shield" project, in which it focuses on state control of information through cyberspace where it believes "whoever controls the Internet will control the world."

become largely associated with the government's tight Internet controls, and regulation of web traffic within its borders.[167]

This relationship has been further fostered through the creation of additional mutually supporting organizations such as the Strategic Support Force (SSF) and Cyberspace Administration of China (CAC). The CAC stresses this relationship as "imperative for the military to serve the people, and the people to prepare the military;" this emphasis is further constituted through the Long-Term Program for Science and Technology Development effort that highlights the importance of "integrating civilian and military scientific and technical efforts."[168] Accordingly, the close relationship between the PLA and various Chinese cyber militias (also highlighted in the previous discussion on APTs) has become apparent. Specifically, the PLA has historically endorsed the use of cyber militia's in order to support the achievement of national Chinese objectives.[169] Additionally, the recent creation of China's SSF constitutes another mechanism that further fosters this military-civilian relationship. Mainly, the SSF has been assessed to help mitigate "the risk of erratic cyber militias whilst still harnessing the power and capabilities of civil society."[170] Consequently, this relationship is one of mutual cooperation towards the application of Chinese grand strategy for the achievement of Party goals. Accordingly, this characterization subsequently aligns with the "mandate of heaven" conceptualization that represents a "social contract" between China's political and military leaders who together seek to restore "the country's standing in the world."[171]

Lastly, the Chinese concept of "guanxi" is again relevant in this regard, as it helps characterize the military-civilian relationship concerning integration of private industry. In a recent interview, JD Work emphasized this relational attribute as a means for how the military and government

[167] Andy Greenberg, "China's Golden Cyber-Shield," Forbes, July 31, 2007, https://www.forbes.com/2007/07/30/china-cybercrime-war-tech-cx_ag_0730internet.html#64b45e3f483c.
[168] Lyall, "China's Cyber Militias: China's Cyber Power Is in the Grip of Dual Trends - Pluralism and Centralization."
[169] Lyall.
[170] Lyall.
[171] Zhang WeiWei, "For China's One-Party Rulers, Legitimacy Flows From Prosperity and Competence," Philosophy + Culture Center, Berggruen Institute, March 1, 2017, http://philosophyandculture.berggruen.org/ideas/for-china-s-one-party-rulers-legitimacy-flows-from-prosperity-and-competence.

employ civilian private sector capabilities in cyberspace; individuals or companies who possess certain skills provide services to the state in exchange for favor in future government business.[172] This relational concept again highlights the potential for "moonlighting" and "for-hire-hackers" that practice their professional capacities for monetary or nefarious purposes.[173] Therefore, even though these civilian entities may not necessarily compensated monetarily for their services, they can still be reimbursed through non-monetary transactions in the future.

ASSESSMENT OF CHINA'S POTENTIAL FUTURE DISPOSITION

Through the study of these individual variables and their applicable links to cyberspace, a better understanding can be realized for how China may react to certain U.S. actions in various domains of conflict. Accordingly, the subsequent assessment intends to characterize the most likely and most dangerous trajectories for Chinese actions in an attempt to inform future U.S. cyber policy, strategy, and military campaign planning.

MOST LIKELY FUTURE TRAJECTORY

Although China's national strategy and objectives persist, a noticeable shift has been observed in the intensity and frequency of its cyberspace activities. In 2015 the U.S. confronted China on its intellectual property theft cyber activity, which prompted a threat of economic sanctions against them. This resulted in a commitment by China to refrain from conducting or supporting cyber-enabled theft that could provide an advantage to its companies.[174] However, proof of Chinese cyber-intrusions continues (although less) after this agreement, with cybersecurity firms like CrowdStrike tracing attacks back to China and National Security Agency (NSA) Director Admiral Michael Rogers testifying to Congress on continued activity against U.S. companies.[175]

---

[172] Work, Discussion on Chinese, North Korean, and Russian Conduct in Cyberspace.
[173] Levi Maxey, "China Pivots Its Hackers from Industrial Spies to Cyber Warriors," The Cipher Brief (blog), April 2, 2017, https://www.thecipherbrief.com/china-pivots-its-hackers-from-industrial-spies-to-cyber-warriors.
[174] Adam Segal, "How China Is Preparing for Cyberwar," *Christian Science Monitor*, March 20, 2017, https://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0320/How-China-is-preparing-for-cyberwar.
[175] Robert Knake and Adam Segal, "How the Next U.S. President Can Contain China in Cyberspace," *Journal of International Affairs; New York* 70, no. 1 (Winter 2016): 25.

The U.S. and China also agreed to further discuss the establishment of international cyberspace norms, which aligns with the previously discussed concepts of lawfare and legal warfare that China continues to engage in as a mechanism to legitimize its cyber activities and actions related to key territorial disputes. Consequently, despite these international agreements with other countries, China is likely to continue to use its interpretation of international law to legitimize both its domestic and international actions. Furthermore, despite these types of agreements, China's strategic goal of garnering "pre-conflict justification and post-conflict legal resolution" remains intact.[176] The domestic legislation and international norms discussed as part of China's legal framework will still enable the protection of its interests through cyberspace. Mainly, if the U.S. or another perceived rival takes action against China for activities such as espionage, the Chinese government now has the domestic legal legitimacy to "impose fines or expel" foreign businesses in retaliation.[177]

The OBOR initiative that includes the establishment of the "Information Silk Road" is also likely to remain a major focus in growing China's economy through cyberspace; this greater connectivity can provide the government with more oversight and control of information domestically, while also opening new markets for e-commerce efforts within the country.[178] The interconnected nature of the public and private sectors within China lend further credence to this assertion. Large Chinese telecommunications companies including Huawei and ZTE have been assessed to be "instruments of the state, as well as possible mediums that can be leveraged by the Chinese government for intelligence collection."[179] Accordingly, a combination of state-influenced industry and larger e-commerce markets could likely make it easier for the Chinese government to legally circumvent existing international agreements.

Another economic consideration should also be taken into account when examining China's most likely trajectory and its U.S. financial relationship. A recent interview with Sean Kanuck highlighted that China remains a large holder of U.S. debt, and maintains a vested interest in

[176] Iasiello, "China's Cyber Initiatives Counter International Pressure," 13.
[177] Iasiello, 13–14.
[178] Elizabeth C. Economy, "Beijing's Silk Road Goes Digital," *Council on Foreign Relations* (blog), June 6, 2017, https://www.cfr.org/blog/beijings-silk-road-goes-digital.
[179] Iasiello, "China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities," 53.

the continued capacity of America to pay those debts; this factor is likely to maintain a strong influence on Chinese decision-making when considering the impact of cyber operations that could negatively influence or potentially damage U.S. critical economic infrastructure or functionality.[180] Therefore, China is more likely to continue cyber operations that will better enable its placement and access within these critical systems, while also attempting to circumvent current international agreements that can further close the economic gap with Western countries through industrial and intellectual property theft.

This includes further intrusions into U.S. companies, and the extraction of critical information related to bid prices and contracts, as well as mergers and acquisitions.[181] This observed shift in activity provides China with the same economic advantages, while also allowing it to claim compliance with the 2015 intellectual property theft agreement. Accordingly, China has pursued this industrial information through its own corporate acquisitions, which now account for an average of 51% of all imports for the seven largest commercial IT manufacturers that supply the U.S. government. Microsoft constitutes one of the highest dependencies in this regard, with 73% of its components coming from China.[182]

China will also continue to take actions it deems necessary within a more regional sphere of influence in order to ensure the state and its political regime can maintain its geopolitical position power. Accordingly, China is more likely to undertake "soft power" initiatives through cyberspace that will enable both information dominance domestically and deterrence of international interference regarding regional confrontations associated with land disputes in the South China Sea, Taiwan, or Tibet. Consequently, as reiterated by Sean Kanuck, confrontation is likely to be an attempt to degrade regionally based actions. [183] Adam Segal also agreed that

[180] Sean Kanuck, Discussion on Strategic Goals of China, North Korea, Russian, and Iran in Cyberspace, Phone Interview Conducted At: Columbia University School of International and Public Affairs (SIPA), March 26, 2018.
[181] Sam Kim, "China Hacks U.S. Firms for Financial Information, FireEye Says," *Bloomberg.Com*, April 4, 2018, sec. Politics, https://www.bloomberg.com/news/articles/2018-04-04/china-hacks-u-s-firms-for-financial-information-fireeye-says.
[182] Robert Delaney, "US Urged to Act Immediately to Save Its Systems from the 'Growing Threat of Chinese Cyber Theft,'" South China Morning Post, April 20, 2018, http://www.scmp.com/news/china/article/2142513/us-urged-act-immediately-save-its-systems-growing-threat-chinese-cyber.
[183] Kanuck.

Chinese cyber actions in response to specific Western actions would likely be directed at regional Command and Control (C2) targets, U.S. allies, or other Western interests, and would likely unfold in a controlled escalation of small scale events.[184] Consequently, the U.S. must remain politically, militarily, and economically cognizant of these strategically important geographic disputes within China's regional sphere of influence where certain actions might cause China to react through cyber means.

All of these factors continue to support China's use and application of its warfare strategies to cyberspace as a means to achieve its strategic objectives. Chinese national strategy continues to indicate a desire to achieve a 'peaceful rise' through economic, political, diplomatic, or military struggles, which can potentially be achieved through cyber means.[185] This reference is likely to indicate a regional and global rise in both influence and power. China is likely to remain focused on establishing itself as a regional leader, and as a world power with a more predominant status.[186] Subsequently, espionage, intelligence collection, and enabling activities are likely to continue in the current environment as China continues to avoid serious penalties for these types of activity.

MOST DANGEROUS FUTURE TRAJECTORY

Misperception of signals from Beijing based on how China seeks to engage in cyberspace can lead to inherently dangerous global impacts. China's understanding of its sovereignty in cyberspace can lead to an escalatory situation even if this was not the intention of other nations. The PLA maintains a large repository of cyber tools that can be employed with the diverse placement and access gained through its espionage and intellectual property activities throughout the years. Therefore, a situation where the PLA views U.S. actions to be a violation of its cyber sovereignty or national geography in other domains maintains a propensity to be perceived as an offensive action. This being the case, inaccurate signaling may trigger a

[184] Adam Segal, Discussion on Chinese Strategic Culture and Cyberspace, Phone Interview Conducted, March 28, 2018.
[185] Lee, "China's 'Three Warfares,'" 216.
[186] Iasiello, "China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities," 69.

preemptive response from China's PLA.[187] This view arguably can also maintain some linkages to the philosophical influences of Sun Tzu who stressed that success of an attack could be assured "if you only attack places which are undefended."[188] Consequently, this may lead to an escalatory crisis scenario that maintains the propensity of spreading to other domains.[189]

The nine-dash line reference can also apply to this most dangerous future trajectory. Chinese claims to certain geographic markers within the South China Sea can pertain to similarly viewed markers within cyberspace considered to be sovereign Chinese territory. Specifically, this reference can illustrate how China views its own cyber sovereignty through what it deems a part of its own Internet geography. President Xi emphasized this concept in a 2015 speech to the World Internet Conference, stressing that Internet sovereignty must be respected as the "right of individual countries to independently choose their own path of cyber development."[190] If escalation occurs through cyberspace, a U.S. response may not be able to achieve the desired magnitude of its intended effectiveness against specific digital targets as a result of tight controls across China's internet. Accordingly, these factors may compel the U.S. or other nations to consider kinetic avenues of approach toward their desired targets in some capacity.

The assessed persistent presence of Chinese cyber actors on U.S. critical infrastructure provides China with advantageous targets of opportunity for this first strike preemptive mentality. With China considered to be one of just a few countries capable of shutting down critical infrastructure like the U.S. power grid, this type of action might be considered as either a coordinated military action, crisis signaling mechanism, or punitive response measure.[191] During

---

[187] Elsa B. Kania, "Cyber Deterrence in Times of Cyber Anarchy - Evaluating the Divergences in U.S. and Chinese Strategic Thinking," in *2016 International Conference on Cyber Conflict (CyCon U.S.)* (2016 International Conference on Cyber Conflict (CyCon U.S.), Washington D.C.: IEEE, 2016), 13, https://doi.org/10.1109/CYCONUS.2016.7836619.

[188] Sun Tzu, *Sun Tzu On the Art of War,the Oldest Military Treatise in the World,* trans. Lionel Giles (London: Luzac & Co., 1910), 44, http://hdl.handle.net/2027/uva.x030339883.

[189] This situation is indicative of the Yalu River reference cited earlier, when signals from China were either ignored, missed, or misunderstood to the point where they were compelled to repel the U.S. advance by force during the Korean War.

[190] Jinghan Zeng, Tim Stevens, and Yaru Chen, "China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty,'" *Politics & Policy* 45, no. 3 (June 1, 2017): 433–34, https://doi.org/10.1111/polp.12202.

[191] Robert K. Knake, "A Cyberattack on the U.S. Power Grid," Council on Foreign Relations, April 3, 2017, https://www.cfr.org/report/cyberattack-us-power-grid.

an interview with Adam Segal, he emphasized the point that even though China is not likely to undertake such extreme targeting measures in cyberspace, that does not mean they would not take such actions if the perceived repercussions of U.S. actions were deemed to be unacceptable; this situation might be categorized as the threat of regime collapse or an attempted overthrow of the Party, and could also stem from Western actions in China's sphere of influence that are viewed as a direct threat to Chinese national security.[192] Furthermore, as previously mentioned, the PLA's doctrinal approach maintains philosophical influences that advocate advantageous preemptive strikes, and the display of capability, will, and signaling. As such, this most dangerous type of scenario is certainly not out of the realm of possible for Chinese actions in cyberspace and can potentially be activated in alignment with the PLA's doctrinal approach to preemption. Therefore, if U.S. policies, kinetic and conventional maneuvers, or asymmetric actions are interpreted as overly offensive or as a violation of sovereignty, China has the capacity, competency, depth, and most importantly the will, to undertake such dangerous actions.

Informing U.S. Cyber Strategy

It is imperative to understand which levers the U.S. should consider using in order to best achieve its various policy, kinetic, and asymmetric objectives. As such, we must understand that U.S. actions within cyberspace will be viewed through a unique lens specific to China. This lens has been distinctly influenced by each of the aforementioned variables, and subsequently impacts China's strategic approach to cyberspace. Whether U.S. actions are deemed to be offensive or defense in nature, a violation of Chinese sovereignty (physical or asymmetric geographies), or as an active attempt to delegitimize the state government will have profound impacts on China's deployment of its cyberspace capabilities.

Accordingly, contested physical geography such as Taiwan and the South China Sea (among others) can provide more insight into how China views cyberspace. In the case of Taiwan, China has deployed missiles along the Taiwan Strait in an attempt to deter the potential for Western Interference, while the U.S. has countered these actions through the sale of arms to Taiwan and

[192] Segal, Discussion on Chinese Strategic Culture and Cyberspace.

provided additional security support as stipulated under the 1979 Taiwan Relations Act (TRA).[193] As such, certain actions (such as political recognition of Taiwan, for example) could be viewed by China as a violation of its national sovereignty. Furthermore, sovereignty violations of this nature regarding contested geography may also act as a catalyst for malicious asymmetric responses through cyberspace. Consequently, the U.S. must seek to understand what China's 'nine-dash line' is in cyberspace, and how it can best formulate a strategy that will prevent an escalatory response as a result of misunderstood signals in all domains of warfare.

An important point of emphasis in the formulation of U.S. cyber strategy with China should also include a thorough analysis of how the Chinese government is likely to understand, interpret, and implement future cyberspace agreements. The 2015 China-U.S. agreement to cease cyber-enabled intellectual property theft offers an applicable case; although activity significantly dropped after this agreement initially, a shift in strategy now indicates that Chinese operators are targeting dual-use technologies and civil society groups that are not covered under the current agreement.[194] Therefore the U.S. must seek to understand through China's strategic culture how these types of agreements on cyberspace policies will be adhered to in the future. Mainly, will these agreements be interpreted exactly as their specific lettering indicates, or will they be implemented as to the "spirit of the agreement" as well.[195] In a recent interview with Jason Healey, he emphasized the point that China perceives the U.S. to be extremely capable in determining attribution for cyber intrusions, a capability the Chinese do not feel as confident in; as a result, this perception makes China hesitant to enter into these types of agreements.[196] Accordingly, understanding distinctions such as these remain crucial, as they can help the U.S. strategically shape its policy, targeting, and operational characterization in regards to China.

---

[193] Eleanor Albert, "China-Taiwan Relations," *Council on Foreign Relations* (blog), December 7, 2016, https://www.cfr.org/backgrounder/china-taiwan-relations. The TRA was passed in 1979 and affirms unofficial U.S. ties with Taiwan that are constituted through a commitment to its security, as well as the supply of necessary "defense articles and services" for the island.

[194] Adam Segal, "An Update on U.S.-China Cybersecurity Relations," *Council on Foreign Relations* (blog), November 17, 2017, https://www.cfr.org/blog/update-us-china-cybersecurity-relations.

[195] Segal.

[196] Healey, Discussion on Cyberspace Analogies and Strategic Culture.

It is also important to highlight the timeline and planning cycle that China utilizes in preparing necessary movements for the achievement of its strategic objectives. This past October, President Xi Jinping outlined his plan to make China into a superpower within the next thirty years; in this speech he refers to the start of a "new era" in which China will move closer to "center stage," and emphasized that "to achieve great dreams there must be a great struggle."[197] Accordingly, it must be understood that even though China appears to be more regionally focused at this point in the short term, its long-term planning objectives may be indicating aspirations that are more global in nature. Therefore, the U.S. must strive to account not just for China's short-term strategic objectives, but also their long-term global ambitions twenty to thirty years from now. With this consideration accounted for, the U.S. can better formulate its own strategic planning cycle that can more directly and accurately inform Cyber Command's planning considerations for full spectrum cyberspace operations.

Lastly, the previously discussed consolidation efforts of President Xi Jinping this past year may be signaling a new development in how China seeks to use cyberspace to its advantage in the future. With plans to add President Xi's full doctrine on "Thought on Socialism with Chinese Characteristics for the New Era" into the national constitution, new parallels are beginning to be drawn between President Xi and Mao in terms of their political power.[198] Mao's view on political power is that it grew out of the "Barrel of a Gun," and that those intending to maintain this power must control the armed forces.[199] With the recent restructuring and consolidation of Chinese cyber capabilities under the newly established SSF, it appears President Xi is moving closer to Mao's methodology. These recent developments might therefore necessitate a different characterization of China's strategic approach to cyberspace, one that more closely aligns with Chinese views on legitimacy. Specifically, the Confucian "mandate of heaven"[200] can be

[197] Debra Killalea, "China's 30-Year Deadline to Rule the World," news.com.au, October 20, 1017, http://www.news.com.au/finance/work/leaders/chinas-30year-deadline-to-rule-the-world/news-story/70f62a5bc0e4580b83d5ca89a2479e94.
[198] "Xi Expected to Be Written Into Chinese Constitution," *Bloomberg News*, January 19, 2018, https://www.bloomberg.com/news/articles/2018-01-19/xi-jinping-thought-to-be-written-into-chinese-constitution.
[199] "Some Background Notes on Mao Tse-Tung's Philosophy of Force," 14.
[200] WeiWei, "For China's One-Party Rulers, Legitimacy Flows From Prosperity and Competence."

conceptualized as a potential representation for how President Xi's legitimacy has been built upon his intent to restore China's world standing, and how a newly consolidated cyber force represents another means to achieve this national objective.

Recommended Areas for Future Research

In order to reduce the potential for more dangerous outcomes, the U.S. can consider additional research or studies on potential influencing topics that may shape China's trajectory. The use of law as an instrument to legitimize China's domestic and international cyber activities may prove to be a rewarding area for deeper study. Understanding how these legal frameworks can be used to circumvent international agreements in cyberspace can better inform which policy levers to pull in future security situations. An additional recommended area for future study is how China might use its "Information Silk Road" to continue its international espionage activities as a result of the access it may gain from state-influenced Internet Security Providers (ISPs). A more in-depth study of how this topic may affect U.S. companies who choose to conduct business operations within China can help inform cybersecurity protocols and information protection procedures. This effort can also include a comprehensive study of the substantial increase in Chinese acquisitions of U.S. businesses following implementation of the intellectual property theft agreement in 2015. Chinese mergers and acquisitions involving U.S. companies have risen steadily from less than one-hundred in 2013 to just under three-hundred in 2017.[201]

Another potential area for future research might also include how China may seek to respond in cyberspace as a result of currently planned U.S. tariffs for certain Chinese imports. In response to new tariffs on steel and aluminum, China has already decided to move forward with retaliatory tariffs for 128 specific American products.[202] However, an important area for future observation can include if, when, and how China decides to go beyond conventional actions by, with, and through cyberspace. China's cybersecurity legal framework already provides a mechanism for potential retaliation through the use of "a number of informal tools to hurt U.S. firms" if the government eventually determines these actions to be hostile; some of these tools could include: "black box cybersecurity reviews," "hardline interpretation of ambiguous rules in China's cybersecurity law," and future implementation of "encryption requirements" that would

[201] Kim, "China Hacks U.S. Firms for Financial Information, FireEye Says."
[202] Megan Cassella, "China to Slap Tariffs on 128 U.S. Goods," *POLITICO* (blog), April 1, 2018, https://politi.co/2pVQj9L.

require pre-approval of domestic encryption products.[203] Additionally, the CCP's newly approved constitutional amendment to remove Presidential term limits will allow President Xi Jinping to continue his tenure.[204] President Xi Jinping has already moved to consolidate his power and silence domestic criticism through the use of Internet censorship; this censorship has focused on blocking searches related to criticism of President Xi Jinping's recent rise in power, as well as his actions to suppress free speech through cyber means.[205] Accordingly, President Xi Jinping has also taken actions to somewhat consolidate Chinese national cyber capabilities. Therefore, in contrast, the lack of a significant cyber response to these economic actions could also prove to be a significant finding for the evolution of China's strategic employment of cyber capabilities.

Lastly, China's deployment of the newly established SSF in support of the Party's objectives in cyberspace can prove to be a prolific area for future research. The consolidation of China's cyber capabilities appears to be another consequence of President Xi Jinping's desire for more state control. In a recent interview with Adam Segal, he reiterated that China's SSF construct is an area where the state is seeking to consolidate more but not completely decentralize; he believes some APT groups are likely remain outside the SSF and within the Ministry of State Security to support espionage objectives.[206] Therefore, how this force will be employed and for what purposes is still not completely clear. Adam Segal further elaborated that this current consolidation and how China decides to use the SSF is likely to be driven by what happens with U.S. and China trade relations in the next six months to a year.[207] Accordingly, a concerted effort to observe how these new cyber forces are constituted, employed, and controlled can provide a better understanding for how this potential evolution in China's cyber strategy may manifest itself in future international security situations.

---

[203] Samm Sacks, "How Will China Retaliate beyond Tariffs?," Center for Strategic & International Studies, *Commentary* (blog), March 29, 2018, https://www.csis.org/analysis/how-will-china-retaliate-beyond-tariffs.
[204] Jon Russell, "China's Web Censors Go into Overdrive as President Xi Jinping Consolidates Power," *TechCrunch* (blog), February 27, 2018, http://social.techcrunch.com/2018/02/26/chinas-web-censors-go-into-overdrive-as-president-xi-jinping-consolidates-power/.
[205] Russell.
[206] Segal, Discussion on Chinese Strategic Culture and Cyberspace.
[207] Segal.

RUSSIA

*A series of successive operations **is** a modern operation. Without depth, an operation is deprived of its essence and becomes historically conservative, failing to correspond with the new conditions that define it.*

-Georgii Samoilovich Isserson, on offense-in depth
in *The Foundation of Deep Strategy*[208]

INTRODUCTION

In line with the Clausewitzian dictum, the practice of international politics as war by other means is characteristic of relations between the United States (U.S.) and the Russian Federation (Russia). Russia's activity to date has manifested as an extension of its national interests, whether symbolic or strategic. These are i) disruption of the status quo abroad; and ii) exercising what it terms "information security" for the preservation of order, and the Russian state as we know it.[209]

Given events of the past 15 years, it is easy to fall into the trap of examination of Russian machinations through our own paradigms and contexts. Russia is a unique actor in the international arena, and its behavior is a product of many factors which have reverberated into Russia's development of a strategic culture in cyberspace. Russia has an Information Security Doctrine to complement its National Security Doctrine.[210] Consequently, this case study examines the Russian understanding of cyberspace as a domain and vector for the propagation of its national interests. Such elements include the employment of non-state actors and proxies in pursuit of national objectives; the legal lens through which the Russian government interprets domestic law and international commitments; the civilian-military relationship; and the development of the domain from Relcom to Kaspersky.[211] The analysis of the factors outlined

[208] Georgi Samoilovich Isserson. *The Evolution of Operational Art*. Translated by Bruce W. Meaning. 1930 ed. Fort Leavenworth, KS: Combat Studies Institute Press, 2013. Accessed March 13, 2018. http://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/OperationalArt.pdf p. 48
[209] L. V. Astakhova,"The concept of the information-security culture." Scientific and Technical Information Processing 41.1 (2014): 22-28. p. 26
[210] Ibid, p. 26
[211] M. Holt Ruffin, The Post-Soviet Handbook: A Guide to Grassroots Organizations and Internet Resources. University of Washington Press, 2018. p. 308

above will provide greater insight into the elements that inform Russia's conduct and posture within cyberspace.

DEFINING RUSSIA'S STRATEGIC CULTURE

The following section provides insight into the distinctive body of beliefs, attitudes, and practices regarding the use of force, which are specific to the Russian nation-state. By characterizing Russian behavior in cyberspace as a product of its long existence and unique factors in its development of nationhood and national cyberspace, we begin to understand how they inform Russia's external defense posture.

Russia's conduct within the cyber domain has been informed through a variety of independent variables. Beginning with its history, the composition of Russian strategy maintains a connection with a key Russian military theorist: Mikhail Vasilyevich Frunze.[212] Frunze's Unified Military Doctrine[213] takes an approach informed by state affairs and political developments, adapting the German Reichwehr's aggressive model to the Worker-Peasant-Soldier model of the Red Army, with particular emphasis on offense. [214] Frunze served as an inspiration to several early Soviet military theorists, including Georgii Samoilovich Isserson, [215] Vladimir Triandafillov,[216] and practiced most notably by Marshal Georgy Zhukov.[217]

Fig. 1, Diagram of C2 for Russian SORM II surveillance system, courtesy of securityaffairs.co

[212] An early Bolshevik revolutionary and notable Red Army commander during the Russian Civil War.
[213] The first indigenously Russian military treatise, written upon the consolidation of the Red Army.
[214] Thomas M. Lafleur, Mikhail Frunze and the unified military doctrine. ARMY COMMAND AND GENERAL STAFF COLL FORT LEAVENWORTH KS, 2004. < http://www.dtic.mil/get-tr-doc/pdf?AD=ADA429032>, pp. 1-114, p. 11
[215] Author of *Foundations of Deep Strategy*
[216] Author of *The Nature of the Operations of Modern Armies*
[217] Geoffrey Roberts, Stalin's general: the life of Georgy Zhukov. Random House Incorporated, 2012. p. 31

The more contemporary iteration of Frunze's theory, deep operations, has considerable visibility and applicability in Russia's approach to cyber warfare. Frunze's influence appears most demonstrably in Russia's offensive posture in cyberspace, especially in the earliest days of interstate cyber warfare, such as the 2007 Estonia attacks in response to the proposed removal of the Russian "Bronze Soldier" monument, and as a combined element of political and kinetic means and objectives during the 2008 Georgian war. Both of these instances, within the greater diplomatic aggressive posturing, also exhibit the offensive maneuvers in the realms of Command and Control (C2), Psychological Operations (PsyOps), or Action on Objective.

A connection to Frunze's influence is evident in Russia's Information Security Doctrine of 2008, sponsored by the Medvedev administration. This doctrine incorporates the defensive nature of "information security" as part of an integrated treatise that marshals all sectors of Russian society to exercise efforts in furtherance of Russian national information security objectives. [218] However, according to the UNRISD, there is a touch of irony in this orientation, as it was the role of the Relcom/Demos network that maintained open lines of communication during the USSR's August 1991 coup attempt against Gorbachev that kept the public informed and allowed for a mobilization against the coup. [219]

Another point of consideration in this defensive point of view is how Russia approaches practical information security beyond doctrine. While China and Iran are considered models in web filtering, Russia is not up to this par. [220] While Russia has not met first generation filtering standards, it does serve as a model in the political information security mold, wherein SORM II regulations dictate that ISPs must provide the FSB with access to "any and all content", and that anything objectionable by the FSB is grounds for shutdown. [221] Furthermore, progression to

[218] Ministry of Defense, Russian Federation, "Doctrine of Information Security of the Russian Federation." Accessed March 13, 2018. http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.
[219] Rafal Rohozinski, "Mapping Russian cyberspace: Perspectives on democracy and the net.", United Nations Research Institute for Social Development, Discussion Paper No. 115, (1999). p. iv
[220] opennet.net, "Internet Censorship Listed: How Does Each Country Compare?" the Guardian, April 16, 2012. http://www.theguardian.com/technology/datablog/2012/apr/16/internet-censorship-country-list.
[221] Bruce Etling, Karina Alexanyan, John Kelly, Robert Faris, John G. Palfrey, and Urs Gasser. "Public discourse in the Russian blogosphere: Mapping RuNet politics and mobilization." (2010). p. 6

greater state control of the Internet appears to proceed in a piecemeal manner, where in lieu of a nationwide firewall, legislation has been passed addressing specific facets of information security, such as VPN prohibition, data localization, or mandated operation through local telecoms, among others.[222]

It is in these series of prohibitions that we find a source in Dostoevsky, who throughout *The Brothers Karamazov*, illustrates the dichotomy between Slavic and Western influence in Alexei and Ivan, respectively.[223] In the eyes of Dostoevsky, it is of utmost importance for Russia to embrace its inner Alexei when facing Ivan, the permanent threat to the integrity of the Karamazov family, and therefore of the Russian Orthodox spiritual community in the face of real threats.[224]

In order to understand the Russian approach to the cyberspace domain, it is essential to recognize the role that the Internet and information play *vis-à-vis* the state. For Putin, according to the Center for Naval Analyses, Russia is engaged in a persistent struggle for state security, in which there are internal and external actors in the information sphere.[225] To the brainchild of a former KGB Colonel, such arguments bear considerable similarity to the Bolshevist idea of *kto kovo*, or Who Against Whom. The idea is a Hobbesian zero-sum interpretation of the anarchy of the international arena, in which a failure to vanquish spells defeat.[226] This would later be tempered in Soviet practice, which would indicate willingness to cut losses, as exemplified in the Yom Kippur War.[227] Nevertheless, the modern iteration remains consistent with the Western

[222] Catherine Shu, "Putin passes law that will ban VPNs in Russia." TechCrunch. July 30, 2017. Accessed March 13, 2018. https://techcrunch.com/2017/07/30/putin-passes-law-that-will-ban-vpns-in-russia/.
[223] Peter Savodnik, "The Secret Source of Putin's Evil." The Hive. January 09, 2017. Accessed March 12, 2018. https://www.vanityfair.com/news/2017/01/the-secret-source-of-putins-evil.
[224] Ewa Thompson, "Reflections on Errors in Some Western Interpretations of Fyodor Dostoevsky's The Brothers Karamazov" Rice University, <http://www.owlnet.rice.edu/~ethomp/Dostoevsky%20&%20Philosophy.pdf> p. 411
[225] Michael Connell and Sarah Vogler. Russia's Approach to Cyber Warfare. Center for Naval Analyses Arlington United States, 2017. p. i
[226] Interview with Jack Snyder, Ph.D., March 5th, 2018, 6:10-8:00 PM, Room 501A, International Affairs Building, Columbia University School of International and Public Affairs.
[227] Ibid

and self-described "anti-hegemonic" group of powers, to forgo the interpretation of cybersecurity as network security, for their definition as information security.[228]

The religious and philosophical variables of Russian culture have considerably contributed to strategic culture and the Russian approach to cyberspace. Some of the cornerstones of Russian literature have been emphasized as part of post-Information Security Doctrine policy musings by the Russian General Staff. One example of this is the Gerasimov doctrine, which reiterates the Russian fear of external influences affecting a state to such a great extent that even with the strongest consolidation, military might, and power projection can succumb to anarchy, citing the Arab Spring as a "lesson".[229] Gerasimov points out the covert nature of the machinations leading to such an eventuality.

Other important aspects of Russian strategic culture which influence its approach to the cyber domain include favoring first-order sources in lieu of documentation for collection and analysis for intelligence purposes. Ultimately, our analysis will have to understand how Russian cyber strategy revolves around how the dichotomy between Tolstoy and Dostoevsky, War & Peace and Crime & Punishment, governs Russia's propensity to use force and hold itself to a standard of behavior.

INDEPENDENT VARIABLES

HISTORY

Russian history has long possessed conditions non-catalytic to positive external relations. Since Kievan Rus, we can trace this archetype to two founding external forces: the Mongol Hordes and the Polish-Lithuanian Commonwealth. Ever since the start of Russia as we know it with the nascent Kievan Rus to the Duchy of Muscovy, the Mongol invasions of the 14th century,[230] and

[228] Thomas Ambrosio, Challenging America's global preeminence: Russia's quest for multipolarity. Taylor & Francis, 2017. Ch. 5

[229] Mark Galeotti. "The 'Gerasimov Doctrine' and Russian Non-Linear War." In Moscow's Shadows. September 17, 2017. Accessed April 03, 2018. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

[230] Charles J. Halperin, Russia and the Golden Horde: the Mongol impact on medieval Russian history. Vol. 445. Indiana University Press, 1987. p. vii

the Time of Troubles, have bred an early suspicion of external pressures against the Russian state,[231] whether forceful or political.

For the case of historical comparison, we must also determine what the proper early warning paradigm is, and whether this has offensive or defensive implications. In the US, this is, as former Secretary of Defense Panetta has described as "Pearl Harbor" or by the Atlantic Council's Jason Healey as "9/11". [232] [233] The Russia instance would have a few of note: politically, the Time of Troubles, with a defensive implication as a reaction to the perception of an adverse state of political affairs being the machination of external powers. For a preliminary examination, we must consider the majority defensive instances in Russian history. This may be considered as a byproduct of early Muscovy and the Tsardom, yet we consider the following. For a surprise attack in the mold of a Russian Pearl Harbor, the closest parallel we have is the casus belli of the Russo-Japanese War of 1904-05, where the Japanese shelling of the Russian city of Port Arthur, now Lyunshunkuo District in historical Manchuria, China, started the war. [234] While resolved peacefully with

Fig.2: Russian language propaganda in Donetsk, saying ""The fate of the Russian people- repeat the feat of their fathers, defending their native land. Enroll in the people's army of the Donetsk republic," calling upon themes of the Russian Civil War and WWII, courtesy of medium.com

[231] Chester SL. Dunning, Russia's First Civil War: The Time of Troubles and the Founding of the Romanov Dynasty. Penn State Press, 2010. p. 412

[232] Jason Bumiller and Thom Shanker. "Panetta Warns of Dire Threat of Cyberattack on U.S." The New York Times, October 11, 2012, sec. World. https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

[233] Jason Healey, "Preparing for Cyber 9/12." Atlantic Council. Accessed March 14, 2018. http://www.atlanticcouncil.org/publications/issue-briefs/preparing-for-cyber-9-12.

[234] Clifford F. Butcher. "Port Arthur was "the Pearl Harbor of 1904"." The Milwaukee Journal, January 19, 1942. Accessed March 14, 2018. https://news.google.com/newspapers?nid=1499&dat=19420119&id=-e4ZAAAAIBAJ&sjid=8SIEAAAAIBAJ&pg=4412,1516787.

mediation by President Theodore Roosevelt, the conditions of and territorial changes accepted and outlined in the Treaty of Portsmouth, are widely accepted as a Japanese victory. [235] While Russian strategic thinking had not evolved at this juncture to consider this Japanese result as a *kto kovo* moment for Russia, the war nonetheless contributed to a deteriorating political situation, the period during which included the 1905 revolution. [236] After this metaphor, the second greatest defensive paradigms, more familiar to the majority of readers, are Napoleon's invasion of Moscow during the first Russian Patriotic War, and the Battle of Stalingrad, within the greater context of the Great Patriotic War (WWII).

Up to the early 20th century, Russian did not have a wealth of military philosophy, theory, or scholarship to call its own. Compared with Clausewitzian developments contributing to Prussian military theory up to German unification, Russia from the time of the Tsardom and Empire lacked such development. Starting with Peter the Great, the first Tsar to be titled Emperor, Russia's strategic goal was to develop in line with the great powers of Western Europe. [237] This all changed with the Bolshevik revolution of 1917, in which Russia started to develop in its own mode in line with Marxist-Leninist teaching. This brought us Frunze, and his many iterations of the Unified Military Doctrine. This gave us the most contemporary Soviet iteration, which was its utilization under Marshal Zhukov.[238] After the demise of the Soviet Union, Russia's strategic orientation lacked a main adversary, and wound up in a geographic tailspin.[239]

After the loss of the Eastern Bloc and the Soviet Socialist Republics, the Federation itself was under risk as Chechen rebels managed to trounce the Russian Armed Forces during the First Chechen War, gaining de facto independence. [240] Upon repeat of their actions, increases in jihadist activity, and the Chechen invasion of Dagestan, this final death knell for the Yeltsin

[235] Editors of the Encyclopedia Britannica, "Russo-Japanese War | Causes, Summary, Map, & Significance." Encyclopedia Britannica. Accessed March 14, 2018. https://www.britannica.com/event/Russo-Japanese-War.
[236] Ibid
[237] L. R. Lewitter,"Peter the Great, Poland, and the Westernization of Russia." Journal of the History of Ideas 19, no. 4 (1958): 493-506. doi:10.2307/2707919. p. 493
[238] Roberts,. Stalin's general: the life of Georgy Zhukov, p. 31
[239] Department Of State. The Office of Electronic Information, Bureau of Public Affairs. "United States Relations with Russia: After the Cold War," June 4, 2007. https://2001-2009.state.gov/r/pa/ho/pubs/fs/85962.htm
[240] BBC News, "Timeline: Chechnya," BBC News, January 19, 2011. http://news.bbc.co.uk/2/hi/asia-pacific/country_profiles/2357267.stm.

administration gave way to former KGB Colonel, FSB head, and Prime Minister Vladimir Putin.[241]

Fig. 3: Map of the Russian Federation, courtesy of CIA

While the conventional phase of the Second Chechen War lasted about a year, a long and protracted guerrilla phase shook Russia up to 2008, with the consolidation of federation control as well as that of Ramzan Kadyrov.[242] In summation, the importance of this period was that the deteriorated security situation in the Federation, as well as the ever-present threat of external interference from the west, provided Putin with the ideal pretext to draft his Information Security Doctrine of 2008. The premise of the doctrine is best surmised as protection of the Russian information space from threats to state stability and sovereignty, regardless of origin. This is a precept that has extended not only to the Federation, but as enforceable in Russia's near abroad, as evidenced in 2007 and beyond.

GEOGRAPHY

The embrace of Eurasianism is evident in the delegation of responsibility for Russian intelligence. For many years after the fall of the USSR, GRU had the primary responsibility for the near abroad, while the FSB would have responsibility for everything but. [243] Moreover, this has been evident in Russia's geopolitical orientation to Eurasianism as well. According to Penn State, a key manifestation of Russia's Information Security Doctrine was a UN General Assembly resolution, along with other post-Soviet states, for international information security

[241] Ibid
[242] Ibid
[243] Mark Galeotti, "Putin's Secret Weapon." Foreign Policy. Accessed March 14, 2018. https://foreignpolicy.com/2014/07/07/putins-secret-weapon/.

tightening.[244] Such behavior appears to be consistent, as Putin and Xi Jinping of China have mutually pledged a policy of non-interference.[245]

Moreover, there is consideration of geographic weaknesses informing Russian defense weakness, and therefore suspicion. In an interview with Columbia SIPA's Senior Research Scholar Jason Healey, a considerable portion of Russian geographic weakness is the existence of steppes and poorly defensible terrain in a large portion of Russia's western territory up to the Urals.[246] Also, the terrain of Siberia is nonconductive to effective defense in the East. As these have proved to be independent of the Time of Troubles and the Mongol Horde, they have proven to be invitations to adversaries from Napoleon and Hitler in the West, to Japanese and Chinese saber rattling in the East. [247] Finally, it would be a combined experience of set-back in Chechnya as well as the humiliation faced in Afghanistan that would form an immutable orientation of zero-tolerance towards any insurgencies in Russia proper and the near abroad, a fundamental tenant of Russian national security policy. [248]

POLITICS

According to Critical Threats, linguistically it is also important not to underestimate the role of language in intelligence activities. Aside from Cyrillic and transliterated or Romanized domains among forensic clues, suspect domains can also be written in the closest equivalent Roman character to the Cyrillic original.[249] One example of which is the community of Russian hackery hosted on xakep[.]ru, whose URL best approximates the original Cyrillic spelling.[250]

---

[244] Dr. Michael L. Thomas and Dr. Dennis J. Bellafiore. "Geospatial Intelligence and Cyberspace." Cyber-Geography in Geospatial Intelligence. 2017. Accessed March 14, 2018. https://www.e-education.psu.edu/geog479/node/557.

[245] Elizabeth Wishnick, "In search of the 'Other'in Asia: Russia–China relations revisited." The Pacific Review 30, no. 1 (2017): 114-132. p. 119

[246] Interview with Jason Healy on March 26th, 2018. Columbia University, New York City

[247] Interview with Jason Healey, March 26th, 2018, 3:00-3:40 PM, Room 1337, International Affairs Building, Columbia University School of International and Public Affairs.

[248] United States. Defense Intelligence Agency. Military Power Publications. Military Power Publications. Compiled by Lt. Gen. Vincent Stewart, USMC. 2017. Accessed March 14, 2018. http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf. p. 18-19

[249] Kara Flook, "Russia and the Cyber Threat." Critical Threats. Accessed March 14, 2018. https://www.criticalthreats.org/analysis/russia-and-the-cyber-threat.

[250] *Ibid.*

To understand the Russian political trajectory today, we must understand Putin. Those familiar with the immediate post-Soviet period recognized the turmoil and lower standards of living than many were accustomed to in Soviet times. This gave rise to Putin in the aftermath of a combined moribund economy, jihadist threats from the North Caucasus, and ever decreasing public confidence in Boris Yeltsin. A unique feature of Putinism from the start was its ability to transcend political philosophy, gaining the support of the major Russian schools of political thought.[251]

Moreover, within these schools of thought, the ever-present authoritarian streak in Russian politics merits recognition. Present since Tsardom and Empire, as well as the Soviet Union through Lenin's "dictatorship of the proletariat", even in iterations of democratic facade the post-Soviet period demonstrated the political ambient that fostered authoritarianism. Some theorize its roots in Mongol times, a period that officially separated Russia from the conventional West.[252] The 1993 constitutional crisis,[253] Putin's return under Medvedev,[254] and Alexei Navalny's expulsion from the 2018 election[255] all predicate Russia's return to personal rule, as was present during Tsarist times, in order to rule over a vast and ungovernable space. Furthermore, given the status quo and the Russian penchant to view relations as a zero sum *kto kovo*, if one is not with Russia or its leader, the default is to view it as an enemy, and as such, given Russian theories of total war and skepticism towards the west, makes for a belligerent mobilization in support of the *vodzh*, or leader.[256]

ECONOMY

[251] Marcin A. Piotrowski, 'Russia's Security Policy', in Janusz Bugajski (ed.), Toward an Understanding of Russia: New European Perspectives (New York: Council on Foreign Relations, 2002). p. 60

[252] Peter N. Stearns, Michael Adas, Stuart B. Schwartz, and Marc Jason Gilbert. World civilizations: The global experience. Pearson, 2014. p. 460

[253] RFE/RL, "Twenty Years After: Key Players In Russia's October 1993 Crisis." RadioFreeEurope/RadioLiberty. Accessed March 14, 2018. https://www.rferl.org/a/russia-players-1993-crisis/25125000.html.

[254] The Economist, "On Putin's Terms." The Economist, November 14, 2008. https://www.economist.com/node/12622987.

[255] John Bacon, "Russia Bars Navalny Presidential Bid." Accessed March 14, 2018. https://uw-media.usatoday.com/video/embed/108918976?sitelabel=reimagine&continuousplay=true&placement=uw-smallarticleattophtml5&pagetype=story.

[256] Mikhail Khodorkovsky, "Opinion | A Problem Much Bigger Than Putin." The New York Times, September 12, 2017, sec. Opinion. https://www.nytimes.com/2017/09/12/opinion/putin-russia-mikhail-khodorkovsky.html.

The economic factors contributing to the current Russian posture are attributable to the shock therapy during the collapse of the Soviet Union. Massive privatizations and acquisitions by oligarchs in the wake of the fall of the Soviet Union, which coming on the heels of ample educational investment in the sciences in the heyday of the USSR, led to a glut of computer scientists with a dearth of employment opportunity.[257] This later created a cost-effective workforce/contracting situation for GRU, which presently bears the brunt of external intelligence and information operations.[258] According to Critical Threats, the role of programmer also holds considerable prestige as the title of economist did in Soviet times, but a glut of programmers with few jobs to match challenged this perception.[259]

As such, Russian nationals would be sought after by firms abroad such as Microsoft and IBM.[260] This, combined with a lack of an economic environment that fosters innovation, per Thomas Friedman, results in a market where "more patents are registered by Microsoft alone than all of Russia." [261] Furthermore, criminal actions perpetrated by Russian nationals do not receive the universal opprobrium that they would in other countries due to the perception that because of Russia's current economic situation, as long as foreign entities and not Russians are the victims, such acts are acceptable.[262] Moreover, Critical Threats states that a popular Russian perception is that if Westerners neglect to protect themselves from criminal activities, then their suffering is merited.[263]

An additional factor is the organized crime factor, which not only perpetuates a widespread system of pervasive corruption in Russia proper, but can also serve as an autonomously funded vehicle for extortion abroad. Aside from the mafia, Critical Threats cites the Russian Business Network (RBN), a crime syndicate rife with petty criminals as well as the *siloviki,* or collective

[257] Connell and Vogler, Russia's Approach to Cyber Warfare., p. 8
[258] Roland Heickerö, Emerging cyber threats and Russian views on Information warfare and Information operations. Defence Analysis, Swedish Defence Research Agency (FOI), 2010. p. 31
[259] Flook, "Russia and the Cyber Threat.", 2009.
[260] Heickerö, Emerging cyber threats and Russian views on Information warfare and Information operations. p. 35
[261] Thomas Friedman, "Opinion | Is Putin a C.I.A. Agent?" The New York Times, sec. Opinion. Accessed April 3, 2018. https://www.nytimes.com/2018/04/03/opinion/putin-cia-weakening-russia.html.
[262] Heickerö, Emerging cyber threats and Russian views on Information warfare and Information operations, p. 36
[263] Flook, "Russia and the Cyber Threat.", 2009

Russian security services. While the RBN has been absent for some time now, and many have contemplated its extinction, it gained a reputation for its criminal activity of the most notorious nature.[264] Finally, as far as Putin is concerned, while the trials and tribulations of the Yeltsin era provided no reprieve from the opprobrium that he received, the payoff of shock therapy, an economic recovery joined by a rise in commodity prices, oil included, in the early 2000s provided a boost to the Russian GDP per capita, as well as Putin's popularity.[265] This employ of the criminal underworld combined with technical prowess represents a departure from past Soviet tactics of using fellow travelers as agents, in that it uses private Russian citizens in a vast effort to act on the state's behalf while obfuscating as much as possible.

RELIGION

According to the DIA, the Eurasianist and traditionalist paradigm are often iterated in themes of Russian propaganda, if not on their own merit, then in denunciation of the West and the values of the liberal world order that it has embraced.[266] The dual role that the Orthodox Church played during Soviet times, whether as active opposition via the ROCOR,[267] or collaborator with the KGB for synods in communion with Moscow, is important to recall as an element of counterintelligence.[268] While this wouldn't be a dismissal of the potency of the Church in Russian state affairs, consideration of this history leads us into a political-religious-philosophical axis from which Russians orient their views on international relations.

A notable aspect of religion as it relates to this assessment is twofold: given the integration by writers such as Tolstoy and Dostoevsky, there is considerable intersection between contemporary Russian philosophy and the Orthodox Church. And Russian re-emergence of religiosity given the fall of the Soviet Union and the end of state atheism, with considerable

[264] Ibid
[265] Gerd Ludwig, "Why Many Young Russians See a Hero in Putin." Magazine, November 8, 2016. https://www.nationalgeographic.com/magazine/2016/12/putin-generation-russia-soviet-union/.
[266] Stewart, "Russia Military Power: Building a Military to Support Great Power Aspirations", p. 39
[267] Elliott Robert Barkan, ed. Immigrants in American history: Arrival, adaptation, and integration. Vol. 1. ABC-CLIO, 2013. p. 1242
[268] Ksenia Luchenko, "Why Do the Russians Trust the Church Set up by the KGB? | Opinion." Newsweek, February 10, 2018. http://www.newsweek.com/why-do-russians-trust-church-set-kgb-802635.

attention given to predominant Russian Orthodoxy.[269] According to RAND, as a trend the state has shown a gradually increasing embrace of the Church as legitimator and guarantor of popular legitimacy.[270] Furthermore, with Russian state embrace of the Church as one of the four traditional religions of Russia, including Judaism, Islam, and Buddhism, allowed for a greater dimension of state control in the face of potential subversion from external religious elements.[271] The overall guise for legitimacy in this instance was traditionalism, where even those outside of the big four were granted the courtesies of state as long as they conformed to traditional Russian values. The same could not be said for anything outside of this traditional veneer.[272]

Moreover, starting under the Medvedev administration, there has been greater emphasis of placing the Church at the forefront of patriotic education, or *dukhovno nravstvennoe vospitanie*.[273] Moreover, the Church provides a guise of legitimation of the protonationalist idea of Rus. Coterminous with the original patriarchy and Russia's adoption of Orthodox, to include a see and territory coterminous with present day Russia, Belarus, and the Ukraine. Any threat to this, in Putin's eyes, would undermine the security of the state as well, or the *dukhovnaya bezopasnost*.[274] This role therefore allows not only the Church, but traditional religious elements within Russia to set the tone for the information security standard, up to the point of Patriarch Kirill blessing Ministry of Internal Affairs hardware to protect against cyber attacks.[275] This news is novel, and we have yet to see Russian Orthodoxy or the other traditional faiths manifest as a decisive influence on doctrine or operations, its presence merits our attention.

PHILOSOPHY

[269] Catherine Evtuhov,. The cross & the sickle: Sergei Bulgakov and the fate of Russian religious philosophy. Cornell University Press, 1997. p. 54
[270] Katya Migacheva and Bryan Frederick, eds., Religion, Conflict, and Stability in the Former Soviet Union. Santa Monica, CA: RAND Corporation, 2018. https://www.rand.org/pubs/research_reports/RR2195.html. p. 8
[271] Ibid, p. 161
[272] Ibid, p .10
[273] Ibid, p. 170
[274] Ibid, p. 174
[275] Henry Joseph-Grant, "Russia's Top Religious Official Sprays Holy Water on Computers to Prevent Cyber Attacks – Irish Tech News." Accessed May 2, 2018. https://irishtechnews.ie/russias-top-religious-official-sprays-holy-water-on-computers-to-prevent-cyber-attacks/.

"The Karamazovs are not scoundrels but philosophers, because all real Russian people are philosophers…" -Dimitry Karamazov in *Fyodor Dostoevsky, The Brothers Karamazov*[276]

In Russia's strategic position in Eurasia, it has had ample opportunity to adopt philosophical teachings from both East and West to create its own national *raison d'être*. From the East, we see elements of the Sun Tzu Bing Fa in military strategy.[277] However, from the West, we see a more profound influence. The pursuit of philosophy, per Dostoevsky in *The Brothers Karamazov*, has become a Russian pastime. For the pursuit of meaning with derivatives in Plato's pursuit of virtue, wisdom, power, and ideals.[278] Furthermore, philosophy served as a dual edge sword throughout Russian history, as a consolidating model for which the state could call upon in governance, as well as a means to subvert the state.

Additionally, we see historical development. The 19th century saw debate on how Russians relate to the rest of the world and to God, and in the 20th century with how to create the ideal society. Whether through material means which brought Marxism-Leninism, or in one's self, in the debate between existentialism and personalism, to the debate between structure and personality. Such debates share relevance to the core principle of theories of information and communication. Of the most potent influences, as far as military power goes, one may look no further than Dostoevsky. It was he who pioneered existentialism before its popularity via Sartre.[279]

In summation, Russian philosophy can be reduced to two ever-competing dichotomies. One is the totalitarian tendency, in which we see themes such as *sobornost* (spiritual community), national unity, resurrection of the fathers, among other tendencies attributable to the Tsarist era, communism, or Dugin's Eurasianism. On the opposite side, we see the anti-totalitarian

[276] Mikhail Epstein, "The phoenix of philosophy. On the meaning and significance of contemporary Russian thought." Symposion: A Journal of Russian Thought 1 (1996): 35-74. <http://www.emory.edu/INTELNET/rus_thought_overview.html>
[277] Heickerö, Emerging cyber threats and Russian views on Information warfare and Information operations. p. 24
[278] Epstein, 1996
[279] Steven Crowell, "Existentialism", The Stanford Encyclopedia of Philosophy (Winter 2017 Edition), Edward N. Zalta (ed.), URL = <https://plato.stanford.edu/archives/win2017/entries/existentialism/>.

tendency, featuring themes such as existentialism, polyphony, personalism, critique of ideology, and post-utopian thinking.

Eurasianism, while not new, also had to compete with Western oriented and Greater Russia theory. Western orientation, common since Peter the Great but given new life in the Yeltsin era, proposed alignment with the West in order to prevent recalcitrant elements in Russian society from engineering a "Weimar Russia".[280] In contrast, Greater Russia theory, promoted by those such as Alexandr Solzhenitsyn and Vladimir Zhirinovsky, is a classical revanchist theory on the reassumption of Russian hegemony not only over the former Soviet Union, but over the Eastern Orthodox world.[281]

Additionally, we have the notable Bolshevik contribution to Russian philosophy, in the game theorist's zero-sum interpretation of *kto kovo.* Translated into "Who, whom", this was elaborated by Lenin to signify "Who will overtake whom?". This is a very zero-sum approach to the Russian view of international affairs, as it assumes that one is either a conqueror or is conquered. [282] This also aligns well with the summation of Russian nature as "messianic, totalitarian, ascetic, nihilistic, and cynical."[283]While Russia is no longer Bolshevist, it can be effectively argued that this at the very least aligns well with Russian perceptions of encirclement, as well as with Putin's exploitation of poor relations with the West to maintain an offensive position. From these themes, we can assert and determine that Eurasianism and its *sobornost* are the deepest philosophical contributors to Russia's orientation in the domain, whereas Solzhenitsyn and Bolshevism are corollaries and tactical informers, respectively.

Russia's Cyberwarfare Strategies and Capabilities

With an understanding of Russia's development as a nation-state and how factors in this development have affected its perception of the international environment and its national defense, we will examine how this posturing is manifest in cyberspace. Given Russia's long

[280] Piotrowski, 'Russia's Security Policy'. p. 60
[281] Ibid, p. 60
[282] Josef Joffe, "The First Totalitarian." The New York Times, October 19, 2017, sec. Book Review. https://www.nytimes.com/2017/10/19/books/review/victor-sebestyen-lenin-biography.html.
[283] Alexander Pantsov. The Bolsheviks and the Chinese Revolution 1919-1927. Routledge, 2013. p. 16

existence, we will see how entrenched practices that have become part of its national *raison d'être* have become part of critical applications of this culture. In the role of war in state affairs, we will see internal and external applications of cyber power. This is based on what Russia's perception of the enemy is, the prowess it has, and its ability to respond. From there, this will determine Russian propensity to use force, and the actors it employs to do so. Whether they are regular Armed Forces and official intelligence officers, or anything but. This topic will be further parsed in understanding how Russia understands the rules of war, how this relates to civilian and military pursuits to cyber war, and what this implies for restraint. These dependent variables will provide us with the best commencement for understanding the Russian way of cyberwarfare, and its implications for the national defense.

DEPENDENT VARIABLES

ROLE OF FORCE IN STATE AFFAIRS

According to the Center for Naval Analyses, Russia's adoption of *informatsionnaya voyna,* or information war, is an important distinction from the direct translation and practice of what we would term *kibervoyna,* or cyber war.[284]This allows for Russia to exact offensive and purportedly nonlethal operations against its adversaries without the risk of sparking the kinetic action that its adversaries perceive as cyber war, thus not risking a response. A consideration brought to light with the conduct of pure cyber in Estonia and combination with kinetic means in Georgia. The same source states, according to Col. Chekinov and Lt. Gen. Bogdanov, that the key to this is plausible deniability.[285]

Moreover, Russia commonly views information warfare as one component of total war, in which the entire resources of the state are mobilized.[286] However, according to the Swedish Defense Research Agency, Russia views information warfare as a traditional prelude to kinetic, evident in its implementation in the pre-C2 obfuscation phase of the 2008 Georgia war. The same source, citing Russia's willingness for negotiation and treaty definition of acceptable behavior in

[284] Connell and Vogler, "Russia's Approach to Cyber Warfare", p. 3
[285] Ibid, p. 4-5
[286] Aelkus. "The Risks of Underpromising Cyberpower." Essays. Accessed March 15, 2018. http://aelkus.github.io/essays/cyberpower.html.

a discussion of war and peace, but not law and order, is demonstrative of the acceptability with which they place both behaviors. It is a trend that has been described as a fusion of traditional Leninist obfuscation enhanced with the potencies that information and network operations afford.[287] Overall, what we witness is a greater willingness to exercise force in cyberspace when the core or peripheral are deemed compromised.[288]

NATURE OF THE THREAT

"Russia is built on what it's afraid of." -Jason Healy[289]

From our understanding, Russia has adopted a total war strategy based on its efficacy in past operations and based on perception of the threat facing it. From roots in medieval to post-Cold War history, it is evident that Russia is deriving its strategic orientation from its perception of nation-states motives towards it and its exercise of power. According to DIA, Russia's articulation of international vision includes "multipolarity predicated on state sovereignty and non-interference in internal affairs".[290] Per Galeotti, while not a blockade, which is the correct definition of an economic application of war, Russia interprets economic sanctions as an act of war.[291] Even more revealing is the absence of "phase zero" as we understand it, which combined with the siege mentality present in many non-democratic regimes, perpetuates the mindset of permanent fusion of war and peace, albeit with less emphasis on peace.[292]

Runet is a component of Russian distinctness and how they view the web. Several entities speak of Runet as an amalgamation of the Russian internet. Coined by Azerbaijani-Israeli Raffi Aslanbekov, Runet remains distinct as the community of Russian-language websites designed for the Russian domestic market. A component of which was also embraced by foreign IT

[287] George Perkovich and Ariel E. Levite, eds. Understanding Cyber Conflict: Fourteen Analogies. Georgetown University Press, 2017. p. 82
[288] Ibid, p. 81
[289] Jason Healey, 2018
[290] Stewart, "Russia Military Power: Building a Military to Support Great Power Aspirations", p. 14
[291] Galeotti, "I'm Sorry for Creating the Gerasimov Doctrine", 2018
[292] Perkovich and Levite, p. 83-4

companies in Russia as a way to cater to the non-English speaking market.[293] However, this approach has historically faced setbacks when implemented by foreign IT providers such as Google, where Russians tend to prefer domestic and locally tailored IT services.[294] While not used to describe a Russian territorial intranet, the term has come into favor by the Russian government as a descriptive term for Russian cyberspace territorial delineation.[295]

In addition, according to the Swedish Defense Research Agency, Russia holds its immediate operational goal as gaining and holding an information advantage over its adversaries.[296] Moreover, since Russia's interpretation of the information warfare doctrine is inclusive of internal and external information security, victory for them is predicated on the indisputable defeat of their adversaries in the information domain.[297] Finally, we see an influence of Eurasianism in current perceptions of the West. While mistrust of foreigners is nothing new for Russians, a core tenant of Eurasianism is the perception of American encirclement.[298] While fear of state disintegration by external force was a motivating factor for Chechnya and supporting Operation Enduring Freedom, NATO enlargement and the prospect of a Chechnya-like situation in Syria motivated Russia to act.[299] [300]

Finally, beyond the American consideration, according to CFR's Adam Segal, it appears that due to the overwhelming consolidation of power by Putin via United Russia and the All-Russian People's Front, Putin's worst fear is any mass public manifestation that threatens his rule.[301] Mr. Segal stated that this started to pick up steam during the Color Revolutions as well as the

[293] Alexander Malukov. "Raffi Aslanbekov." Physiognomy of the Russian Internet. 2013. Accessed March 15, 2018. https://translate.google.com/translate?sl=auto&tl=en&js=y&prev=_t&hl=en&ie=UTF-8&u=http://ezhe.ru/fri/30/&edit-text=&act=url.
[294] Etling et Al, "Public discourse in the Russian blogosphere: Mapping RuNet politics and mobilization.", p. 9-12
[295] Lyombe S. Eko, New media, old regimes: case studies in comparative communication law and policy. Lexington Books, 2012. p. 260
[296] Heickerö, Emerging cyber threats and Russian views on Information warfare and Information operations. p. 17
[297] Ibid, p. 17-18
[298] Piotrowski, 'Russia's Security Policy', p. 60
[299] Graeme P. Herd, "The Russo-Chechen Information Warfare and 9/11: Al- Qaeda through the South Caucasus Looking Glass?" European Security 11, no. 4 (Winter, 2002).
[300] Fiona Hill, "The Real Reason Putin Supports Assad," Foreign Affairs, March 25, 2013
[301] Interview with Adam Segal, Ph.D, March 28th, 2018, 3:00-3:30 PM, Room 1336, International Affairs Building, Columbia University School of International and Public Affairs.

Arab Spring, and Columbia SIPA's Adjunct Professor for Cyber Threat Intelligence Analysis, JD. Work, stated that Euromaidan was a further escalator.[302]

Efficacy of the Use of Force

According to the BBC, a considerable portion of Russia's efficacy of use of force is based on its practice of military deception, or *maskirovka*. This was first harnessed in the Battle of Kulikovo Field, ousting the first major strategic enemy of the Russians, the Mongols. In terms of efficacy, *maskirovka* is designed to be the utmost expression of fury in battle as part of an ambush designed to vanquish an enemy or force it to retreat. Not only has this been a staple of conventional warfare, but it is also crucial to unconventional warfare, such as its employ by the covert military actors of the Crimea takeover. Tactics such as *kamufliazh*, *demonstrativnye manevry*, *skrytie*, *imitatsia,* and *desinformatsia* have all shown to be Russian information and cyber operation staples, from the 2016 DNC breach to Olympic Destroyer. It also manifests in cyber and information operations in a notable display of cynicism. [303] For the DNC Breach, which was intended to discredit through exposition, the immediate effect for the Russians was to demonstrate a practical application of whataboutism or implying equivalence between any actions between Russia and its adversaries, no matter the veracity of such a claim.

Fig. 4: WWII-era Soviet propaganda depicting Hitler's invasion of the USSR in a similar vein as Napoleon's invasion of Russia, courtesy of histmag.org

[302] Interview with Joshua D. Work, March 19th, 2018, 8:00-9:00 AM, Lehman 1, Lehman Social Science Library, International Affairs Building, Columbia University School of International and Public Affairs.
[303] Ash, "How Russia outfoxes its enemies.", 2015

According to Small Wars Journal, an additional notable Russian tactic that has allowed them great breadth and control on the battlefield, whether kinetic or cyber, was harnessed during Napoleon's invasion. In this instance, the Russian army relied on the depth of the Russian territorial terrain, using it as a lure to draw in Napoleon's army. Where in a case study worthy of Clausewitz, once the French logistic chain was overstretched, the Russian army would attack. This, combined with the famed winter that weakened Napoleon's troops and later forced his retreat, is a cornerstone of Russian strategy. Aside from its obvious advantages between Russia turning the tide against Germany in WWII and the conclusion of Stalingrad, it also has implications for the cyber domain.[304]

Organizationally, we can classify active measures as our domain-agnostic grand operational framework for influencing the events in a target country to compel will. Deception, in turn, is a tactic designed to obfuscate the origins and future plans that the operation's initiator is performing. As for the information operation and warfare domain, this fluid and hard to govern venue offers a ripe environment for Russians to exploit political differences, while employing as many masks and fronts as possible so that a Russian connection is near invisible to the untrained eye.

In the information domain, active measures gained its popularity in this era as well, as not only a contribution to the partisan effort behind German lines in the USSR, but also in support of resistance and partisan movements in Western Europe, which would form the groundwork for communist electioneering after the war.[305] Seeing any opportunity to exploit a lack of consensus would be the crux of Soviet information operations became an cornerstone of operations against the United States since the 1960s, aping in the 1980s.[306] For the lures, social engineering and spear phishing have proven to be key components of the reconnaissance phase of Russian cyber operations. Moreover, the extent to which a cyber force is enveloped in the depths of the

[304] Maj. Ronald W. Sprang, USA. "The Evolution of Russian Operational Art." Small Wars Journal. Accessed March 13, 2018. http://smallwarsjournal.com/jrnl/art/evolution-russian-operational-art.
[305] Disinformation: A Primer in Russian Active Measures and Influence Campaigns, 115th Cong., 1-15 (2017) (testimony of Eugene Rumer, Roy Godson, Clint Watts, and Kevin Mandia).
https://www.hsdl.org/?view&did=802222, p. 3
[306] Ibid, p. 3-6

Deep and/or Dark Web is a testament to the risks of being drawn in and, without proper precautions in place, expose themselves to operational security breach. This is also a testament to the risk that Russian forces run themselves of over-extension in territory not their own, as Afghanistan has proven.

According to the CNA review, we can interpret the Russian efficacy of the use of force as follows: tolerance for setbacks in the mold of the later Soviet tolerance to pull back in exchange for greater strategic success. It is a modus operandi that was practiced in Estonia, where the tactical objective was not achieved, as damage to Estonia was minimal and the plan to relocate the Bronze Soldier proceeded. However, it was a strategic coup in that it paved the way for Georgia.[307]

According to Galeotti, use of force, even in deft navigation of the legal gray zone with the employ of semi legal actors, it is measurably and cyclically inefficient.[308] Most succinctly, it is capable of overstretch. This is often a reflection of Russia's own limited resources. This also comes on the heels of its incumbent military modernization efforts, which while producing notable hardware for itself and its partners, also conjures up images of the Brezhnev-Andropov-Chernenko military buildups.

NON-STATE ACTORS AND PROXIES

According to Newsweek, the employ of non-state actors is additionally worrying as they are not only script-kiddies, but developers as well. The creator of BlackEnergy was notable in his distribution of an intended bank fraud malware and use it against governments. There is a distinction in activity, however, that can distinguish between actions for materialistic financial gain and those intended to benefit the Russian state: in recent analysis of APT28, researchers noticed a decrease in intellectual property theft, and an increase in reconnaissance of defense ministries and departments.[309] Moreover, the recent restrictions on federal acquisition of

[307] Connell and Vogler, "Russia's Approach to Cyber Warfare", p. 5
[308] Galeotti, "I'm Sorry for Creating the Gerasimov Doctrine", 2018
[309] Owen Matthews, "From Russia With Malware." Newsweek. March 28, 2016. Accessed March 13, 2018. http://www.newsweek.com/2015/05/15/russias-greatest-weapon-may-be-its-hackers-328864.html.

Kaspersky products due to Yevgeny's affiliation with a KGB Technical School,[310] while not indicative of collusion, is a testament to the extent that non-governmental actors can show roots in Russian intelligence. This offers considerable depth and capacity for non-official action, as evidenced by the recent employ of GameoverZeuS.[311]

The CNA review attests to the difficulty in attribution of non-state actors to the Russian government. That being said, as is typical with like-minded peers, Russia has enlisted the services of non-state actors, ranging from underemployed hackers to thieves-in law. In addition to cost efficacy of employ of these actors, there is a potent legal rationale for employ: in current practice, handlers provide the proxies with actionable intelligence, in which the officers involved can claim plausible deniability. Furthermore, based on ideological alignment, Russia may be able to enlist the assistance of hackers free of charge.[312]

According to Critical Threats, we can also see similarity in the origins of the domain in Russia, albeit with different public-sector applications. Like in the early days of our hacking, Russian hackers would be arrested and offered the options of prison or service for the FSB. [313] It is believed that this initial cadre provided the manpower for the Moonlight Maze breach as well as initial information operations against Chechen rebels during the 2002 Moscow theatre crisis, using similar TTP that would be employed in Estonia.

According to the DIA, there are two ways that the GRU and FSB can influence the management of non-state actors and proxies. Often, if the groups in question such as Wikileaks have ideological aims that parallel Russian interests, then Russian intelligence services will act in tandem so that there is sufficient distance for reasons of plausible deniability in the case of belligerency or attribution. In another instance, Russian intelligence will often sponsor its own third-party actors, such as with the breach of the USCENTCOM feed by the "Cyber Caliphate".[314]

---

[310] Daniel Seiden, "Kaspersky Could Allow Russian Spying, U.S. Tells Court." Bloomberg Big Law Business, 6 February 2018, Accessed March 15, 2018. https://biglawbusiness.com/kaspersky-could-allow-russian-spying-u-s-tells-court/.
[311] Jack Detsch, "How Russia and Others Use Cybercriminals as Proxies." Christian Science Monitor, June 28, 2017. https://www.csmonitor.com/USA/2017/0628/How-Russia-and-others-use-cybercriminals-as-proxies.
[312] Connell and Vogler, "Russia's Approach to Cyber Warfare", p. 23
[313] Flook, "Russia and the Cyber Threat.", 2009
[314] Stewart, "Russia Military Power: Building a Military to Support Great Power Aspirations", p. 39

Moreover, an oft-used method void of middlemen, or greater difficulty in attribution, in the employ of professional trolls and bots, such as those under the aegis of the Internet Research Agency.[315]

LEGAL FRAMEWORK

In the practice of plausible deniability as part of *maskirovka*, Russian diplomatic and justice establishments can claim adherence to the letter of the law. Thus delegitimizing any attempt by an adversary to pursue punitive measures.[316]

According to DIA, we gain further insight into the practical view of legalism by Russia from Putin's speech of March 18th, 2014. Wherein he criticizes the US for purported manifestation of state power in the international arena by exercise of force as opposed to international law, providing fortification for adoption of the literalist school.[317] This combines with Russian perception that the US seeks to impose international norms.

There is an interesting take, however, on the termination of adherence to legal norms and practical adherence to realist paradigms exhibited in Mark Galeotti's *Russian New Way of War*. He cites Tolstoy's *War & Peace*, wherein the First Patriotic War is described as a fencing duel between Napoleon and Tsar Alexander, where Napoleon's goal was to compel the Tsar to do his will. Tolstoy then describes the next phase, or the Russian repel, as Alexander donning a club, to which Napoleon protests based on the rules of war, which the Tsar had assumed did not exist.[318] This further joins philosophically with a nihilistic approach to law, wherein citizens question the need to obey the law when, in their estimation, the state does not.[319] This also provides insight into the Russian approach to war from a legal standpoint. According to RAND's Bruce McClintock, Russian's are experts, when the letter of the law is or is not articulated ad nauseam, at operating in the grey areas of the law, evading questions of illegality, and refuting claims of

[315] Ibid, p. 40
[316] Connell and Vogler, "Russia's Approach to Cyber Warfare", p. 23
[317] Stewart, "Russia Military Power: Building a Military to Support Great Power Aspirations", p. v
[318] Mark Galeotti, "Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'?." Small Wars & Insurgencies 27, no. 2 (2016): 282-301. p. 282
[319] Kathryn Hendley, "Who are the legal nihilists in Russia?" Post-Soviet Affairs 28, no. 2 (2012): 149-186. p. 154

with the assertion of countermeasures.[320] Moreover, Galeotti states that the assertion of the Gerasimov doctrine is as a corollary to the Clausewitzian dictum on politics and war, albeit reversed. [321]

Additionally, Russia has proven, not only through proxies, but also through the employ of *russkiye* (ethnic Russians) abroad, to place as many degrees of separation between act and the Russian Federation itself. As to obscure liability and attribution. However, most notable according to the Swedish Defense Research Agency is that Russia has not made public any cyber policy document comparable to our JP 3-13.[322] From what we do know, outside of the spectrum of information warfare, Russia does make mention of the components of what we know as cyber warfare, inclusive of electronic warfare and implementation of the kill chain, albeit with one glaring replacement: in lieu of computer network operations, they refer to mathematical programming impact, a decidedly root view of OCO and DCO.[323]

MILITARY-CIVILIAN RELATIONSHIP

According to the Swedish Defense Research Agency, the employ of the GRU in handling non-state actors ranging from Russians abroad to patriotic hackers, risks muddying the civil-military divide. Yet this is in accordance with Russian interpretations of total war when they believe their national integrity or existence is threatened.[324]

Additionally, it is important to consider the possibility of division between expectations, willingness to embrace risk, and acceptance of consequences. This is a debate that not only pervades the divide between civilians and the military, but also within the military. It most notably arose when Defense Minister Igor Sergeyev and Chief of General Staff Gen. Anatoly Kvashnin endured a three-year disagreement about apportionment of resources, whether to rebuild the nuclear arsenal or conventional forces.[325] Brian Taylor reiterates this, where he notes

[320] Bruce McClintock, "Russian Information Warfare: A Reality That Needs a Response," RAND Corporation, July 21, 2017. https://www.rand.org/blog/2017/07/russian-information-warfare-a-reality-that-needs-a.html.
[321] Galeotti, "I'm Sorry for Creating the Gerasimov Doctrine", 2018
[322] Heickerö, Emerging cyber threats and Russian views on Information warfare and Information operations. p. 12
[323] Ibid, p. 4
[324] Heickerö, Emerging cyber threats and Russian views on Information warfare and Information operations. p. 48
[325] Piotrowski, 'Russia's Security Policy', p. 64

that dependent on the years in service that a Russian officer has, there can be gaps in understanding with respect to implementation of policy.[326]

Moreover, as Russian society grows more and more autocratic, there is another force at work coaxing a divide. Like a popular perception of the Foreign Service, the Russian foreign policy establishment has been perceived as effete and cosmopolitan. They saw good relations with the West as key to consolidation of power at home.[327] The intelligence corps, however, who saw their priorities as protection of the Russian state at home and abroad, challenged this. Clashes involving this divide include the attempts during the 1980s by the Ministry of Foreign Affairs to preserve detente while the KGB triggered direct action from Africa to Afghanistan. As such, especially given present Russian official discourse of American-led "globalist" attempts to isolate Russia, this is indication of the heavy predominance of the spies in Russian government. This would be indicative of a greater propensity for offensive engagement in the domain. If the Russian foreign policy establishment cannot be an effective check on the belligerent propensities of the intelligence community, then a greater divide would indicate a greater willingness to use force.

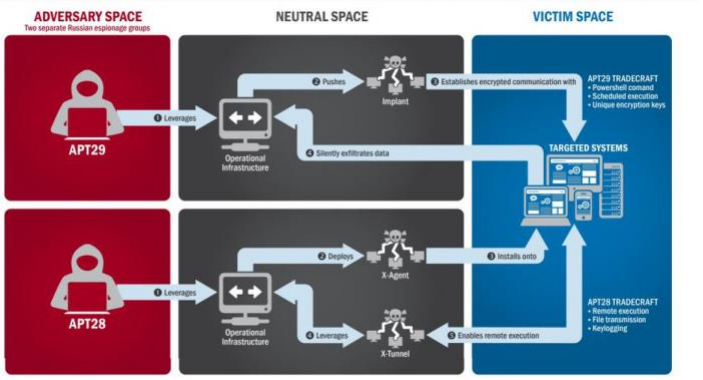


Fig. 5: Depiction of combined operational methods by APT 28 (a.k.a. Fancy Bear/GRU) and APT 29 (a.k.a. Cozy Bear/FSB), courtesy of us-cert.gov

Moreover, there is a perceived divide between the FSB and GRU. While the GRU has been at the forefront of cyber operations, most notably through APT28, it had to re-earn this favor as a result of its substandard performance during the 2008 Georgia War, a conflict that it should have

[326] Brian D. Taylor, Politics and the Russian army: civil-military relations, 1689-2000. Cambridge University Press, 2003. p. 34

[327] Alex Hazanov and Yakov Feygin. "Analysis | Russia Hacked Our Election Because the Spies Took Over." Washington Post, August 2, 2017, sec. Made by History Analysis Analysis Interpretation of the news based on evidence, including data, as well as anticipating how events might unfold based on past events. https://www.washingtonpost.com/news/made-by-history/wp/2017/08/02/russia-hacked-our-election-because-the-spies-took-over/.

mastered given its responsibility for Russia's near abroad.[328] Therefore they are seen as in a popularity contest with the FSB, whose former Director Putin has described as his favored Chekists, hearkening back to the legacy of the pre-WWII Soviet Cheka.[329]

Assessment of Russia's Potential Future Disposition

Cognizant of the factors that constitute Russian cyber capability today, the implications for the future are to be examined on the basis of likelihood and danger. The Russian arsenal and propensity for use as a component of Russian expeditionary offensive activity, as well as in the exercise of cyber warfare in its own right, is demonstrative of intent. Therefore, while not perfectly analogous to the most dangerous scenario, it is our evaluation that the most dangerous scenario will consist of tactics, techniques, and procedures that Russian actors have employed in the past, as well as some that have yet to be tested.

Most Likely Future Trajectory

Cognizance of Russian information and cyber capability has grown multifold in the aftermath of the 2008 Georgia war, and exponentially after the deterioration in relations between Russia and the West. Starting with Russian operations in Ukraine around 2014, and even more so in the aftermath of the 2016 election. In that time, conventional intelligence has shown greater Russian acceptance of willingness to use force in the cyberspace domain.[330] This has included using Ukraine as a testing ground for more of its advanced cyber weaponry and tactics, which have been employed in support of kinetic operations. Or in pure cyber missions, as evidenced with DDoS attacks on Ukrainian critical infrastructure.

One example of implications for the West has been the aftermath of WannaCry/NotPetya, in which an initially Ukrainian targeted attack spread with implications for critical infrastructure across the West. Moreover, given past Russian success in cementing frozen conflicts, including that of Georgia with integrated kinetic and cyber means, it is the evaluation of Sean Kanuck that,

[328] NATO Review. "Russian intelligence is at (political) war." NATO Review. Accessed March 13, 2018. http://www.nato.int/docu/review/2017/Also-in-2017/russian-intelligence-political-war-security/EN/index.htm.
[329] Andrei Soldatov, "Putin Has Finally Reincarnated the KGB." Foreign Policy. Accessed March 15, 2018. https://foreignpolicy.com/2016/09/21/putin-has-finally-reincarnated-the-kgb-mgb-fsb-russia/.
[330] Connell and Vogler, "Russia's Approach to Cyber Warfare", p. 1

also given Russia's need for cognizance in its actual capacity and the risk of over stretch, that further belligerence most likely will occur in the Near Abroad.[331] According to Columbia's Steve Bellovin, Russia's tendency with intrusion sets and related means is to employ them to the maximum of their utility, and to discard said methods when their utility has expired.[332] Therefore, we can expect Russia will be active in group operations across domains, until they see their adversaries parried.

MOST DANGEROUS FUTURE TRAJECTORY

From what we have seen in the most potent employs of Russian information and combined kinetic operations, a considerable point of no return as has been demonstrated in Estonia, Georgia, and the Ukraine. In all three of these instances, Russia has iterated, or it has been determined that, the casus belli are Russian historical memory, its strategic position *vis-à-vis* NATO, or the citing of the interests of ethnic Russians. There is credence to the ethnonationalist argument here, yet it is not our belief that it is not strong enough to provide impetus to the types of strategic investments that Russia has made.

Furthermore, the image of Russia as a power of unemployed criminal hackers has gained credence with the static of Russia among the top five nations of origin for cyber intrusions.[333] It is possible that this interpretation can be put to rest, given the current knowledge of GRU employment of hackers and the Russian desire for dominion over the domain within Russia proper (while directing targeting efforts externally), and especially the best internationally known product of this investment being Yevgeny Kaspersky.

What appears to be the worst-case scenario is articulated by Sean Kanuck, who states that with minimal and shrinking economic and diplomatic common interest and links with the West, Russia will exhibit even less reticence to engage in aggressive behavior.[334] This is an evaluation

[331] Interview with Sean Kanuck, March 27th, 2018, 3:00-3:35 PM, Room 1510, International Affairs Building, Columbia University School of International and Public Affairs.
[332] Lecture by Steven Bellovin, Ph.D., April 2nd, 2018, 11:10AM-1:00 PM, Room 801, International Affairs Building, Columbia University School of International and Public Affairs.
[333] Karatzogianni, "Blame it on the Russians: Tracking the Portrayal of Russians during Cyber Conflict Incidents", p. 130
[334] Sean Kanuck, 2018

seconded by Adam Segal, who includes the possibility for the DNC breach, that if it wasn't error, which is unlikely due to the fact and perception of Russian aptitude in penetration, that it was a sign of Russian disregard of the consequences of their actions.[335] If this were to be the case, then it would be more than reasonable to anticipate the most dangerous scenario to be a Russian doubling-down in the face of confrontation.

In terms of capability, what appears to be the most dangerous scenario follows from Kanuck, in that with every capability that Russia has perpetrated on the West, there was a precedent in its near abroad. Whether through pure information operations in Estonia, hybrid operations in Georgia and Crimea, or infiltration of critical infrastructure systems in Eastern Ukraine. There are parallels in information operations to influence elections, the possibility of clash in flashpoints featuring the Russian Armed Forces, Syria included, as well as the discovered presence of Russian malware in our SCADA systems. As for intent, in addition to Kanuck's assessment of greater willingness to use, Professor Steve Bellovin assesses that the only reason that Russian penetration and information operations were not successful during the French presidential election of 2017 was due to the fact that the Macron campaign placed false "evidence" among scoured servers. Russian hackers obtained and attempted to portray as seized and leaked evidence.[336] This combination of capability, from election breach to SCADA hack, times intent, with less reticence and greater willingness to play fast and loose regardless of risk to others or self, makes this the most potent threat. Which in the worst-case scenario, could result in an intentional devastating offensive destructive attack on our infrastructure.

INFORMING U.S. CYBER STRATEGY

The intent of this section is to determine the gap between capabilities, areas for improvement, and how to proceed with further research in order to gain a stronger understanding of what we must do in order to shore up the cyber national defense.

It is clear in our findings that Russian action, whether pursued directly via GRU or through proxies, is trying to maximize its push for hegemony in what it deems its traditional spheres by

[335] Adam Segal, 2018
[336] Bellovin, 2018

any means necessary, just short of war. This was not only emphasized during the era of the Cold War balance, but remains true today in light of aggressive posturing that attempts to push the boundaries of what is acceptable. Whether it be Ukraine, elections, or NATO itself and its determination to invoke Article V. A considerable portion of this, analogous to Russian practice of *disinformatsia* to sow doubt not only on the battlefield, but in command centers, is perfectly analogous to the Western practice, albeit more restrained, of sowing "fear, uncertainty, and doubt" or FUD. Furthermore, per NDU, there exists the possibility of underestimation of how far the Russian interpretation could proceed, given their penchant to push buttons as well as the generous Cold War definition of cyber that not only includes our network and their information, but both of our C2.[337] As for implications for the US, countering deception in the information space will require an understanding of the means and disguises through which Russians will obfuscate their actions in the domestic space. Moreover, countering the threat will require hardening of soft targets, such as social media and defense against guerrilla cyber operations through proxy TOR servers.

Furthermore, it would behoove us to comprehend how Russians approach systems. Olympic Destroyer proved to be an anomaly, albeit in the guise of a false flag. How Russians typically approach systems is through viewing them as formulas for input and output. They possess the capability to feed their own input for a desired output. Forming the base of social engineering operations that lead to leak disclosures, where the greatest product is not purely a deniable falsehood, but revelation of a secret. Therefore, if our evaluation were that the Russians would start to employ newer capabilities after our discovery, and therefore would be better prepared to anticipate and defend against them, one potential solution would be to employ more honeypot servers to trap actors for forensic purposes. As Steven Bellovin has stated, since the Russians got sloppy, we can count on this as a definite and employ it to our advantage.[338]

Moreover, it will be necessary to adapt to the Russian understanding of deterrence. Per the DIA, the Russian translation of deterrence does not bear its adversaries in mind, but is a reiteration

[337] Richard D. Hooker, Charting a course: Strategic choices for a new administration. Chapter 11: Russia, Government Printing Office, 2017. p. 226
[338] Bellovin, 2018

of active measures.[339] In addition, their idea of strategic deterrence is as true to the Gerasimov doctrine than any other. However, the missing link here is the Russian desire for strategic stability, specifically a vision of stability that aligns with great power balance, and one that reinforces the Russian perception of a multipolar world.

Given the lengths Russians will go to for symbolic measures combined with action that under present definition, reinforced via their literal interpretation of the law, events such as Estonia serve as strategic invitations to Russia, especially as a vector to affect NATO. Moreover, with states ambiguous towards NATO, events such as Georgia highlight the risk present to inviting kinetic warfare along with information. Finally, as the strategic stakes increase with symbolic and strategic importance, we see the lengths Russia will go to, such as SCADA attacks, as evidenced in Ukraine. One factor unites these, however. Without communicated direct response or show to force from the west, Russia will feel emboldened to proceed with impunity. Moreover, should attempts to improve legal definition and agreement on cyber action acceptability fail to deter Russia, it will offer a greater definitive pretext, and less gray area, to respond.

This is a position that not only the US should embrace, but NATO as well. In response to Russian influence operations during the 2016 election, notable steps were taken with respect to diplomatic and judicial retaliation. It is time that these are joined militarily. Atlantic Resolve is just one of many steps taken in the kinetic realm. A potent next step would be to join this with an OCO that imposes cost on Russia and makes them cognizant of not only the lengths to which we will proceed offensively, but what risk they pose to themselves.

Recommended Areas for Future Research

The most recent iteration of the Tallinn Manual has come to account for the duplicitous and evasive ways in which Russia approaches the letter and spirit of the law. Yet will require constant adaptation, as well as corollary adaptation of our ROE and JAG interpretations of LoAC for engagement with discernibly Russian actors in military cyberspace. Furthermore, per Roland

[339] Stewart, "Russia Military Power: Building a Military to Support Great Power Aspirations", p. 23

Hieckerö of the Swedish Defense Research Agency, as has been suggested not only in the context of U.S.-Russian relations, but also in that of multilateral diplomacy, that we are seriously, beyond iteration in manuals, the enumeration of legality of cyber tactics, techniques, and procedures.[340] Any attempt to require Russian definition of acceptability in the rules of war in cyberspace, or defining Tolstoy's *War & Peace*, will also require, for our sake, a definition of Dostoevsky's *Crime & Punishment*. This way, it must be made known to Russia that its intersection of the two and attempts to obfuscate are not only unacceptable, but risk it being exposed to and drawn into a war that it cannot win.

Further research in this area would best encompass a combination of legal analysis, neo-Kremlinology, and cyber deterrence. We have an idea now of how Russia will act in response to threats to its existence and national interests. What we lack is an understanding of how to anticipate and countervail Russian machinations, particularly those of a destructive nature, before they occur. This will require understandings of the cyber version of a Cuban missile crisis. This provides an ideal comparison as it represented the brink of warfare for the nuclear age. We must now formulate a study for response and standoff with the known, such as mutual infiltration of critical infrastructure, as well as the unknown. The disciplines outlined above will provide a greater understanding of the issue as a means to:

1) Catch Russia in the act, as US Ambassador to the UN Adlai Stevenson did to Soviet Ambassador Valerian Zorin on the Security Council floor in 1962,

2) Comprehend Russian military and intelligence leadership and relationships beyond institutions, as the institutions and culture studied here go so far with the personalized style of Vladimir Putin, and whoever shall succeed him, as EXCOMM did with the Khrushchev *communiqués*, and

3) Definitively formulate a plan of action through present and future cyber assets to deter Russian aggression and compel cooperation. As was done through a strategic information of

[340] Heickerö, Emerging cyber threats and Russian views on Information warfare and Information operations. p. 49

operational plans and means to apply network defense principles to kinetic practices such as quarantine.

The elaboration of these studies, and their ability to inform strategic decision-making will be the best point of procedure to anticipate Russian action in preparation of the national defense. These, however, must be compounded with dynamic elaboration in the domain as to best anticipate the next Russian moves in exercise of their national might. The DNC breach was unprecedented in our history as well as Russian history. Past Russian attempts to influence politics were confined to incumbencies and responding to specific policies, but never the electoral process itself. While there is legitimate argument that Estonia, Georgia, and the 2016 election were sufficient wakeup calls, this is insufficient to compensate for failure to anticipate Russian reconnaissance.

Further areas of research would also have to include the probabilities of discovery of existential threats in our systems, as interception rates of Russian intruders are already quantifiable measures which are easier to attribute with each passing day. However, real-time measures do not assist us in anticipating the next possible manifestation of power. Such manifestations could take the form of an executed attack on our critical infrastructure to an event of international significance. Other retaliations could also manifest in a manner least expected, such as exposure of employees of the Intelligence Community as well as assets worldwide in retaliation for expulsion of Russian diplomats and non-official cover officers of the Russian intelligence services. In summation, consideration of these possibilities and developing research on their effects and our current capabilities across DoD and the IC are essential to best anticipate and counter Russian adversarial action.

IRAN

We have armed ourselves with new tools,
because a cyber war is more dangerous than a physical war

-Abdollah Araqi, Deputy Commander of ground forces,
Iranian Revolutionary Guard[341]

INTRODUCTION

Iran's history is important to the national identity as it was once a great empire ruling its neighbors with a mighty military and advanced civilization. This history is invoked repeatedly to stir national pride. This identity was a factor in the evolution of Tehran's cyber activities from a tool to ensure the survival of the political regime in the face of political threats to a tool to supplement Iranian hegemonic expansionist policies.

Another factor in its development of cyber activities is its hostility towards Israel. With the Arab-Israeli conflict being central to modern-time politics in the Arab world,[342] Iran finds it beneficial for its role in the region to assume the image of Israel-bashing leader. In addition, those politics are influenced by Iran's rivalry with its Arab neighbors. Iran's perceived role –locally and in the region- as a "resistance" leader has allowed it to recruit supporters of its cyber activities, including proxies who can use cyber-attacks on Tehran's behalf, which in turn allows it deniability of responsibility.

Iran's modern politics are dominated by the religious clerics regime, which was installed as a result of the 1979 Islamic Revolution. This political version of Shiite Imam-government is particular to Iran, but Iran has been trying to "export" it throughout the region -not only to countries with considerable Shiite population like Iraq, Lebanon, Bahrain and Yemen, but also to countries where Shiites are small minorities, like Syria. The Islamic Revolutionary Guard Corps

[341] "Iran sees cyber attacks as greater threat than actual war". Reuters. Sep. 25, 2012. https://www.reuters.com/article/net-us-iran-military/iran-sees-cyber-attacks-as-greater-threat-than-actual-war-idUSBRE88O0MY20120925

[342] The majority of which has stressed countering Israel as the most important foreign policy pillar.

(IRGC), who is referred to often as the guardian of the revolution, assumes a major part in supervising cyber activities of Iran.

Within a decade of its first connection to the internet in the early 1990's, the Iranian regime, represented by the Supreme Council of the Cultural Revolution, controlled cyber activity in the country. About the same time, the hacking community thrived and contributed to the oppression of political dissidents. With that, the earliest purpose of Iranian cyber programs emerged: the protection and preservation of the political regime.

In 2005, the hardline political wing, represented by former president Mahmoud Ahmadinejad, assumed leadership and expressed animosity toward the West and democratic values. By the next election cycle in 2009, popular dissent, which relied more on new ICT technologies, posed a more serious threat to the hardliners. These popular demands were the beginning of a series of uprisings in the Middle East as the Arab Spring began in late 2010.

The domestic political threat to the regime made the Iranian authorities rely on cyber surveillance as an effective strategic tool to counter the dissent. The success of these strategies became conducive for government-sponsored cyber and hacking capabilities to be developed, including offensive strategies to use these capabilities against external targets, such as the Saudi oil company Aramco and the banking sector in the U.S. Currently, some of these capabilities are finding their way into the hands of allies of Iran in the region, where they are also being employed to quell political dissent.

Defining Iran's Strategic Culture

The regime is in a state of flux, not far removed from the initial fervor of the 1979 Islamic Revolution, the horrific costs of the 1980-1988 war with Iraq, and the consolidation of a new ruling religious elite drawn from the ranks of the nation's Shi'ite Muslim clerics headed by the Supreme Leader Ayatollah Khamenei.[343] The decision-making process since the establishment of the Islamic Republic, led by Shia Ayatollahs, is being shaped by Shia doctrines. This religious

[343] Willis Stanley. "The Strategic Culture of the Islamic Republic of Iran." Prepared for: Defense Threat Reduction Agency. Advanced Systems and Concepts Office. Comparative Strategic Cultures Curriculum. October 2006.

elite leadership consists of a small group of decision-makers belonging to different competing factions, from traditionalists to reformists, who are nonetheless loyal to the Supreme Leader. In order to consolidate the political system after the Revolution, the IRGC was formed based on ideological and religious foundations from the Shia militias that helped the Revolution Leader Ayatollah Khomeini seize power. Since then, the IRGC has been a military arm of the state, whose role has extended to all aspects of activities in Iran. Additionally, the regime is hostile toward the West since the revolution. All these factors have had an important effect in shaping Iran's strategic culture.

INDEPENDENT VARIABLES

HISTORY

Known as Persia until 1935, Iran was an empire that occupied much of Asia Minor and Mesopotamia in ancient times. That empire, whose official religion was Zoroastrianism, was a great military power in the Old World, with several nations under its hegemonic rule. This civilization ended in the seventh century A.D. with the advent of Islam, which emanated from the Arabian Peninsula. Along with that, the majority of Zoroastrianism ended as populations under Persian rule converted to Islam and participated in the demise of the Persian Empire. Although Iran became a Muslim nation and an important center of the Islamic civilization, many note this bitter history as an important element in the Iranian psyche and a factor that has contributed in modern times to shaping Iran's attitude toward neighboring Arab states.

For much of its recent history, Iran was ruled by a monarchy. In his book *Countercoup: The Struggle for the Control of Iran*, Kermit Roosevelt recalls the story of the CIA's most notorious covert action that involved the coup that overthrew Iranian Prime Minister Mohammed Mossadeq in August 1953.[344] That event changed dramatically the course of modern Iranian political history, thereby shaping its strategic culture ever since. The involvement of the United States in this operation was a major factor in shaping the relationship between the two countries and how they behave towards each other.

[344] Kermit Roosevelt. *Countercoup: The Struggle for the Control of Iran*. New York: McGraw-Hill Book Co., 1979.

In 1979, the most defining factor in Iran's modern history took place, namely the Islamic Revolution led by Ayatollah Ruhollah Khomeini, to overthrow the ruling monarchy and force Shah Mohammad Reza Pahlavi into exile. As a result of the revolution, a theocratic system of government was established with ultimate political authority vested in a religious cleric, the Supreme Leader, who is only accountable to the Assembly of Experts, an elected body of clerics. The then-prevailing excellent relations between Iran and the United States suffered irreparable damage as a result of this incident, in which a group of Iranian students seized the U.S. Embassy in Tehran and held more than 100 Americans hostage.

Following the establishment of the State of Israel, Iran developed a close relationship with it based on shared interests in keeping the Soviets out and pan-Arabism down. Various types of diplomatic, military, and trade ties endured for about three decades. Iran was an important source of oil for Israel, but the mutual interests that sustained relations withered after the 1979 Iranian revolution and the Soviet Union's collapse in 1989. This relation turned into bitter enmity to the point of proxy war between Israel and Iran via its client in Lebanon, Hezbollah in 2006.[345]

For most of the 1980s, Iran was involved in a major war with neighboring Iraq. The war eventually expanded to become a major rivalry in the Gulf, as Iraq's president Saddam Hussein often stressed that he is fighting on behalf of Arabs and fending off the Persian threat.[346] This rivalry has continued ever since, especially with another regional power in the Arab Gulf, Saudi Arabia.

GEOGRAPHY

Iran is surrounded by rival powers, whose interests do not align with its own. These include Saudi Arabia, Turkey, Pakistan, and Israel. Iran's neighborhood has been the site of many international conflicts that brought international powers, from the British Empire to the United States and Russia, to the region. Many of the Arab countries in the region became aligned with the United States, which left Iran feeling part of a region with many foes and adversaries.

---

[345] Simon, Steven. "Israel and Iran". *The Sixth Crisis: America, Israel, Iran and the Rumors of War* (2010). http://iranprimer.usip.org/sites/default/files/Iran%20and%20Israel.pdf

[346] Transcript of meeting between Saddam Hussein and Ambassador Glaspie. 15/03/2008. http://www.daralhayat.com:9090/search/SearchServlet?search=glaspie&COMMAND=listItemsInService&SELECTED_SERVICES=DarAlHayat_EN&simple.x=0&simple.y=0

Iran is located in a complicated region at the intersection between the Middle East, Asia Minor, and Central Asia. These regions have had geopolitical issues that spill out to become international threats. A major protracted conflict in the Middle East region has been the Arab-Israeli conflict, in which Iran was not a party, but has extensively used as an excuse for intervening in the region, recruiting Arab proxies and building its military capabilities.

Several countries in the region have connections to Iran, especially through religious minorities that identify with Iran's religious regime and who have relied on Iranian support, becoming its proxies. These include Hezbollah in Lebanon, as well as political and mercenary groups in other countries like Iraq, Syria, and Yemen.

POLITICS

Following the election of reformer Mohammad Khatami as president in 1997 and a reformist Majles (legislature) in 2000, a campaign to foster political reform in response to popular dissatisfaction was initiated. The movement floundered as conservative politicians, supported by the Supreme Leader, unelected institutions of authority like the Council of Guardians, and the security services reversed and blocked reform measures while increasing security repression. In June 2013, Iranians elected a moderate conservative cleric Dr. Hasan Ruhani to the presidency. He is a longtime senior member in the regime but has made promises of reforming society and Iran's foreign policy. Since the Revolution and until the time being, internal politics in Iran continue to witness rivalry between reformists and hardliners. However, popular dissent continues to push towards more liberty and openness to the West as well as political, economic, and social reforms.

The regional politics of Iran's neighborhood is influenced by Iran's continued rivalry with its Sunni Arab states and with the State of Israel. One recent regional trend is the strengthening of Israeli ties with the GCC states, stimulated by common hostility to Iran.[347]

As for the relations with the U.S., following the Revolution, U.S.-Iran relations continued to be marked by enmity. The U.S. sided with Saddam Hussein against Iran and the Gulf war led to

[347] Potter, Lawrence. "Saudi Arabia in Transition". Great Decisions. 2017. P. 60.

clashes between the U.S. Navy and Iranian military forces. Iran has been designated by the U.S. as a state sponsor of terrorism for its activities in Lebanon and elsewhere in the world and remains subject to U.S., UN, and EU economic sanctions and export controls because of its continued involvement in terrorism and concerns over possible military dimensions of its nuclear program.

In Iran's international standing and relations, one of the most important factors is Iran's nuclear program. The UN Security Council has passed a number of resolutions calling for Iran to suspend its uranium enrichment and reprocessing activities and comply with its IAEA obligations and responsibilities. In July 2015 Iran and the five permanent members, plus Germany (P5+1) signed the Joint Comprehensive Plan of Action (JCPOA) under which Iran agreed to restrictions on its nuclear program in exchange for sanctions relief.[348]

ECONOMY

Iran's economy is marked by statist policies, inefficiencies, and reliance on oil and gas exports, but Iran also possesses significant agricultural, industrial, and service sectors.[349] The Iranian economy is mostly owned and operated by the state, especially the office of the Supreme Leader Ayatollah Ali Khamenei[350], and many companies are affiliated with the security forces, mainly the Iranian Revolutionary Guard Corps (IRGC).

The international sanctions imposed on Iran have had huge impact on the economy and made Iran face increasing challenges.[351] Nevertheless, those sanctions were targeted and did not do much to stem the steady revenue from oil and gas funding clandestine activities, even those sponsored by the sanctioned entities like the (IRGC).

[348] The World Factbook: IRAN. U.S. Central Intelligence Authority. https://www.cia.gov/library/publications/the-world-factbook/geos/print_ir.html
[349] The World Factbook: Iran. Central Intelligence Agency. Lase updated on Mar. 15, 2018.
[350] Amir Basiri. "Iran And The Revolutionary Guards' Economic Powerhouse". Forbes Magazine. Mar 29, 2017. https://www.forbes.com/sites/realspin/2017/03/29/iran-and-the-revolutionary-guards-economic-powerhouse/#26c4c4e5cf4e
[351] Hakimian Hassan. "How Sanctions Affect Iran's Economy". Council on Foreign Relations. May 22, 2012.

Following the JCPOA agreement, sanctions were lifted, providing large cashflows that Tehran used to fund its activities and policies in the region and beyond.

Religion/ Philosophy

Iran was not a particularly religious country until the 1979 Islamic Revolution of Ayatollah Khomeini forced the population into a strict version of Shiite Islam in public and controlled all aspects of public life. Iran's strategic culture is now mainly shaped to a great degree by the Shiite version of Islam.

The revolution brought Shiite clerics to the helm of the political institutions in the country, who govern according to the Wilayat Al-Faqih, or the Guardianship of the Islamic Jurist, which is central to the Shiite sect of Islam. With the revolution, religion took control of all government institutions, including the military. In addition, religious police and paramilitary units were established. One of the most powerful of which is the IRGC, whose role is to protect the religious revolutionary institution, and which has later become a leading sponsor of Iran's warfare activity.

The effect of the Revolution went beyond the borders of Iran as the religious elite had bigger goals to export the revolution, along with its strict version of interpretation of Islam and politicization of religion, to the region. The obvious targets have been the Arab countries, but since the population of those countries is mostly Sunni Arab, these actions have led to a collision course and caused rivalries that have manifested in different ways.

Iran's Cyberwarfare Strategies and Capabilities

These independent factors have contributed to shaping Iran's strategic culture. They have dictated Iran's foreign policy and military activities in general, and its cyber warfare activities in particular. The result of these factors can be shown in the following aspects of Iran's evolving cyber threat, the nature of which will be further enunciated.

The history of Iran as a major civilization and hegemonic regional power has been reflected in its cyber policies, which seek to leverage its influence in the region. This has manifested in Iranian cyberattacks, many of which have targeted its regional adversaries such as neighboring Arab

Gulf countries and Israel. As Iran has directed its attacks against these adversaries, it has resorted to using proxies in carrying out these activities.

Iran's sour relations with the United States have driven Iran's cyber operations against the U.S. In addition, its presumed role as leader of the "Axis of Resistance" (to Israel) has channeled its aggressive cyber operations against U.S. and Western allies in the region. This presumed role was also used by Iran to recruit cyber operatives from the region to attack Arab nations on the bases of collusion with Israel.

Iran's extensive hydrocarbon resources have been used to support Tehran's ambitions in the region and activities that include cyber espionage and sabotage. This has not been limited to that extent as Iran recently has reportedly exported cyber technology and know-how to its allies in the region, such as the Syrian government, in order to suppress popular demands.[352] Moreover, cyber-attacks initiated by Iran have been often targeted at the oil and gas sectors. The most prominent examples are the cyber-attacks by Iran on the rival Saudi Arabia's oil company Aramco and the attack on Qatar's Ras Gas company. Those attacks were driven by political factors of course, but economic aspects in targeting competing economies and competing oil sectors must also be considered. Additionally, as a guardian of jurisprudence, and by extension a guardian of the state, the Supreme Leader and the Ayatollahs exert major control over guiding the use of cyber as a weapon.

That is reflected in Iran's cyber warfare activities being geared not only to preserve and protect the regime from domestic and foreign threats, but also to go on the offensive against these adversaries. Iran's success in using cyber strategies to quell domestic dissent became the foundation for further development of cyber capabilities and strategies. Recently, it began to find in cyberwarfare an effective addition to its arsenal. Iran's leadership began to consider applications of cyberwarfare as a deterrence weapon against foreign threats to the regime, as well as a way to spy on foreign nations. Thus, both defensive and offensive aspects were followed as Iran used cyber espionage and sabotage tactics.

[352] Michael Gordon. "Iran Supplying Syrian Military via Iraqi Airspace". The New York Times. Sept. 4, 2012.

Today, significant features in the strategic culture of the Islamic Republic of Iran are: strong national cultural identities, dominant leaders, and powerful military organizations as important players in strategic development as well as important receptors for strategic targeting. These features are woven together such that they produce a comprehensive strategic culture that guides and shapes Iran's cyber activities. To explain, both the strong national cultural identity, which is rooted in regional hegemonic ambitions, and the dominance of the theocratic ruling regime lead to a culture in which a powerful military arsenal is a must. Similarly, the powerful national identity and military culture lead to confrontation and rivalries with regional foes, which themselves become part of the strategic culture of Iran.

DEPENDENT VARIABLES

The Iranian strategic culture will be examined, including the role of force in state affairs, the nature of the adversary and of the threat, the efficacy of the use of force, military-civilian relations, the use of non-state actors and proxies, and the legal framework. To summarize, military institutions, namely the IRGC and the Ministry of Interior, are central to all aspects of state affairs, as they direct, finance and supervise cyber warfare. Iran, which is considered a "second-tier cyber power", conducts extensive espionage against the West, and sabotage against the U.S. and its neighboring allies. The Iranian military institutions maintain full dominance on all aspects of life. Iran has been using civil institutions, including universities, to launch attacks, putting to use the culture of strong nationalism, countering Western pressure and sanctions, and "resistance" to the West in order to recruit operatives. In addition, it uses foreign proxies as an attractive option to cause harm while maintaining deniability.

ROLE OF FORCE IN STATE AFFAIRS

Iran has found in cyber warfare an effective tool to inflict damage on its adversaries with minimal commitment of resources and technology, but with substantial effect. In using this tool, Iranian defense planning is also motivated by a desire to enhance the deterrent capability. To this end, Iran has created a force tailored to deter the countries that it believes pose the greatest threat to it.

The Iranian regime has used the context of the conflicts that Iran has been a party in -and the conflicts in the region more generally- to shape and leverage its policies. Therefore, Iran has a declaratory policy of deterrence by punishment as well as denial. It has threatened, for example, to respond to an American or Israeli preventive strike on Iran with a "crushing response" by destroying the Israeli cities and by launching missiles strikes against U.S. bases throughout the region.[353] It has vowed that any attack on Iran would result in the defeat of the enemy's designs. Also, Iran has created a "Passive Defense Organization" to harden and disperse critical infrastructure, to limit the benefits an adversary might accrue from striking them.[354] Most recently, Tehran has been developing its cyber capability into what may eventually become a fourth leg of its deterrent complex, which currently consists of the ability to disrupt maritime traffic in the Strait of Hormuz; conduct unilateral and proxy terrorism on several continents; and launch long-range missile and rocket strikes against targets throughout the region.[355] The potential to cause great harm to the critical infrastructure of its enemies, while maintaining a degree of deniability, likely makes cyber a very appealing option for Iran.[356]

Geography and politics are two factors that influence this dependent variable. To illustrate, Iran will pursue an aggressive regional policy that employs cyber tools that affect its neighbors and the West. While Iran's purpose of cyber warfare is to employ cyber tools to preserve and protect the regime and maintain its power and control in the country, it appears that its intention is also to influence outside forces that affect Iran, whether they are cyber-attacks, or other actions that Iran deems hostile to its interests.

With the comprehensive control that the Iranian regime extends over all political and military aspects in Iran, one arm of the ruling religious institution is the IRGC, which is the central and elite military instrument in charge of protection of the regime and implementation of its most fundamental strategies and policies. In the framework of this strategic role of the IRGC, it

---

[353] Matthew McInnis. Iranian Deterrence Strategy and Use of Proxies. Testimony before the Senate Committee on Foreign Relation. December 6, 2016.
[354] Eisenstadt, Michael. "The Strategic Culture of the Islamic Republic of Iran". Middle East Studies. Monographs. No. 7 November 2015. P. 8.
[355] Eisenstadt, Michael. "Cyber: Iran's Weapon of Choice," *The Cipher Brief*, January 20, 2017.
[356] Anderson, Collin and Karim Sadjadpour. *Iran's Cyber Threat: Espionage, Sabotage and Revenge*. Carnegie Endowment for International Peace. 2018.

assumes the role of leading actor in the control of clandestine cyber activity in the country aimed against domestic and international enemies of the regime.

NATURE OF THE THREAT

The foreign minister of one of Iran's regional rivals called Iran the "most dangerous nation for cyberattacks."[357] In order to understand the scope of this threat and the strategic place that cyber warfare occupies in Iran's defensive strategic culture, it must be studied in a way that highlights the tools that could help achieve Iran's political objectives. Hence, Iran's politics, geography, and history influence this dependent variable.

Iranian cyber strategy could be classified into offensive and defensive sides, each of which must be understood and addressed. As for the offensive strategies, they can be further classified into espionage activities that aim to collect intelligence information about adversaries, mainly the West, and sabotage activities which aim to exact revenge for attacks on Iran and to cause harm to Iran's adversaries in the region.

In light of the high priority that Iran's theocratic ruling regime places on securing its own survival and full control of all sector in the country, Iran's cyber program was initially bent on defending the vitality of the political ruling regime as it targeted internal political opposition with espionage. The focus of the cyber program has then developed -driven by Iran's other strategic culture aspects such as enmity to the West and rivalry with its regional foes- to offensive cyber operations against international and regional adversaries. Thus, cyber capabilities have now become an important weapon in Iran's arsenal. The advantages that this weapon offers are many. For example, it provides less risky means not only to gather information but also to retaliate against any domestic and foreign threats. Therefore, cyberwarfare has become central to Iranian statecraft.[358]

[357] "Saudi foreign minister calls Iran most dangerous nation for cyberattacks". CNBC. 18 Feb 2018. https://www.cnbc.com/2018/02/18/iran-most-dangerous-nation-for-cyber-attacks-says-saudi-foreign-minister.html

[358] Anderson, Collin and Karim Sadjadpour. *Iran's Cyber Threat: Espionage, Sabotage and Revenge*. Carnegie Endowment for International Peace. 2018.

Iran's cybersecurity program has improved steadily. It has matured both in espionage and sabotage aspects. Iran conducts extensive espionage against its neighbors, including Arab states and Israel, where it uses regular distributed denial of service (DDoS) attacks to attack and disable government websites.[359] As Iran underwent cyber-attacks against its infrastructure, including the nuclear facilities, the sense that it is a target of cyberattacks has reflected on its own strategic culture in cyberwarfare. For example, following the Stuxnet cyber-attack, which was designed to target Iranian nuclear facilities in order to wipe computer systems of data, Iran responded by conducting precisely the same sort of attack.[360] Iran's attack, strangely, did not target the originators of the attack against it but rather other states: in specific, the Iranian attack targeted the back-office computer systems of a Saudi Aramco and the Qatari Ras Gas.

In addition to these threats, Iran has recently taken on further steps in posing a more serious threat. In august 2017, a petrochemical company in Saudi Arabia was hit by a new kind of cyber-assault. The investigators believe that the attack was not designed to destroy data or shut down the plant, but it was meant to sabotage the firm's operations and trigger an explosion.[361] Moreover, as part of its assistance to the Assad government in Syria, Tehran has reportedly exported to Damascus training and technology to intercept communications and monitor the Internet in order to track down and oppress political opponents.[362]

In the United States, Iran's cyber activity has included both espionage and sabotage operations that aimed, inter alia, to steal information and funds. This is best demonstrated in the following cases, which were released by the U.S. Justice Department: Seven Iranian nationals were indicted for hacking American banks. One of these individuals was also indicted for trying to hack into the computerized controls of upstate New York's Bowman Avenue Dam on behalf of the IRGC.[363] The Iranian hacker allegedly obtained water-level and temperature information and would have been able to operate the floodgate remotely if it had been operating at the time.[364]

---

[359] Herr, Trey and Laura K. Bate. "The Iranian Cyberthreat Is Real". *Foreign* Policy. July 26, 2017.
[360] Herr, Trey and Laura K. Bate. "The Iranian Cyberthreat Is Real". *Foreign* Policy. July 26, 2017.
[361] Nicole Perlroth and Clifford Krauss. "A cyberattack in Saudi Arabia had a Deadly goal. Experts fear another try". The New York Times. March. 15, 2018
[362] Michael Gordon. "Iran Supplying Syrian Military via Iraqi Airspace". The New York Times. Sept. 4, 2012.
[363] Herr, Trey and Laura K. Bate. "The Iranian Cyberthreat Is Real". *Foreign* Policy. July 26, 2017.
[364] Max Kutner. "Alleged dam hacking raises fears of cyber threats to infrastructure." Newsweek. March 30 2016.

Cybersecurity experts say if the Iranians were able to access its control system, they could also likely get inside systems for more significant infrastructure, such as pipelines, mass transit systems, and power grids.[365] In fact, this operation was part of a plot that also breached or paralyzed 46 of the U.S. largest financial institutions and blocked hundreds of thousands of customers from accessing their bank accounts online.[366]

In assessing Iran's capabilities in the field of cyberwarfare and the methods it uses, it is worth noting that Iran's ICT sector is not among the most advanced and that is why it is not considered a top threat from a cybersecurity standpoint, especially when compared to the capabilities of nations like China, Russia, or the United States. Iran is considered by many as a "Second-tier" cyber power. However, given the importance with which Iran sees its cyber capabilities as a weapon to inflict damage to its adversaries, it choses its targets in a way to maximize the damage and achieve great political and economic effects. Therefore, the incidents involving Iran have been among the most sophisticated, costly, and consequential, invasive and destructive cyber operations in the history of the internet.[367] This is true whether Iran is the target, such as the Stuxnet attack, or the perpetrator, such as the Shamoon virus attack.

EFFICACY OF THE USE OF FORCE

Cyber-attacks usually carry a risk of collateral damage and risk political blowback if the attack ends up causing damages to legitimate sectors, such as the private sector, and if the attacking parties are identified. Nevertheless, Iran does not seem to be deterred by this potential risk. In addition, Iran does not appear to be deterred by the potential for escalatory responses by the nations it targets with cyberattacks.

As a result of the attacks that were traced to Iranian actors, analysts were able to assess that they have the ability to develop cyber-attack tools such as installation of malicious code in counterfeit computer software, blocking of computer communications networks, development

[365] *Ibid.*
[366] Joseph Berger. "A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case". The New York Times. March 25, 2016.
[367] Anderson, Collin and Karim Sadjadpour. *Iran's Cyber Threat: Espionage, Sabotage and Revenge*. Carnegie Endowment for International Peace. 2018.

of viruses and tools for penetrating computers to gather intelligence, and development of tools with delayed action mechanisms or mechanisms connected to control servers.[368] Iran's tools include malware that can disable critical infrastructure, create confusion, distrust, deception, disruption, support or to drive psychological operations that deter hostile activity or otherwise achieve strategic or tactical objectives.[369]

The damage inflicted by cyber-attacks perpetrated by Iranian operatives have been extensive causing material and economic damage comparable to that made by bombs. This is apparent in the following three incidents:

1. In the 2012 attack on Saudi Aramco, 35,000 computers were partially wiped or totally destroyed within a matter of hours. This virus caused huge damage that was described as "a time bomb", which "forced one of the most valuable companies on earth back into 1970s technology, using typewriters and faxes."[370]
2. Similarly, Iranian actors have commonly created malicious domains that have emulated those owned by the American Israel Public Affairs Committee (AIPAC) and have targeted employees of both liberal and conservative Jewish organizations in the United States and elsewhere.[371]
3. In response to a statement made by its CEO suggesting that the U.S. drop a nuclear bomb on Iran, the Iranian government was behind a damaging cyberattack on the Sands Las Vegas Corporation (LVS) in 2014. [372] The attackers seized comprehensive employee information, brought the company's systems to a standstill and wiped out three quarters of

[368] Gabi Siboni, Saooomi Kronenfeld. "Iran's Cyber Warfare". INSS Insight No, 375, October 15, 2012. http://www.inss.org.il/publication/irans-cyber-warfare
[369] Frank J. Cilluffo, Sharon L. Cardash, Cyber Domain Conflict in the 21st Century, 14 Seton Hall J. Dipl. & International Relations 41 (2013).
[370] Zahraa Alkhalisi. "Saudi Arabia Warns of New Crippling Cyberattack". *CNN Tech*. Jan. 26, 2017. http://money.cnn.com/2017/01/25/technology/saudi-arabia-cyberattack-warning/index.html
[371] Anderson, Collin and Karim Sadjadpour. Iran's Cyber Threat: Espionage, Sabotage and Revenge. Carnegie Endowment for International Peace. 2018.
[372] Jose Pagliery. "ran hacked an American casino, U.S. says". CNN Tech. Feb. 27, 2015. http://money.cnn.com/2015/02/27/technology/security/iran-hack-casino/index.html

the company's servers, which insiders estimate cost the company more than $40 million in equipment costs and data recovery.[373]

One of the most important influences on this dependent variable is economy. To illustrate, Iran focuses its targets on its adversaries' main source of revenues in order to cause the greatest damage possible. For example, in the case of Saudi Arabia, Iran targeted the oil sector, the main source of Saudi's revenues. In addition, by attacking energy sectors, Tehran is trying to influence the production of its energy rivals to compensate for what it has lost as a result of international sanctions.

NON-STATE ACTORS AND PROXIES

Tehran's strong imperialist culture and hegemonic policies lead to sponsor many non-state actors as proxies, and to rely on these proxies in its cyber operations. Given the role of the IRGC in the framework of the strong military leadership, it assumes the role of the entity that supervises such proxies in cyber operations internally and externally. The use of outsourcing allows Iran to maintain distance and deniability about its involvement. This use of proxies is highly effective in maintaining plausible deniability.[374] Nevertheless, there remain certain indications that can link such operations to Iran's sponsors, especially the security apparatus, the Ministry of Intelligence and the IRGC.[375] One of the main sources of influence on this dependent variable is religion. Tehran relies on religion in order to recruit individuals and groups to be among its cyber proxies. Therefore, the main source of Iran's proxies comes today from its Shiite client groups. Likewise, Iran uses the guardian of its Shiite revolution, the Islamic Revolutionary Guard, to supervise the activity of its proxies.

Also local non-state, but state-aligned, actors, mainly local universities and hacking communities, are an important component of Iran's cyber capabilities. This strategy relies on the diversified capabilities and affiliations of those actors. Over the decade that Iranians have

[373] Russell Brandom. "Iran hacked the Sands Hotel earlier this year, causing over $40 million in damage". The Verge. Dec. 11, 2014.
[374] Anderson, Collin and Karim Sadjadpour. Iran's Cyber Threat: Espionage, Sabotage and Revenge. Carnegie Endowment for International Peace. 2018.
[375] Frank J. Cilluffo, Sharon L. Cardash, Cyber Domain Conflict in the 21st Century, 14 Seton Hall J. Dipl. & International Relations 41 (2013).

been engaged in cyber operations, threat actors seemingly arise from nowhere and operate in a dedicated manner until their campaigns dissipate, often due to their discovery by researchers.[376] In recruiting operatives, the IRGC reportedly follows a ruthless process as the targeted recruits are given a choice between joining these operations or being sent to jail. The IRGC openly seeks hackers and utilizes criminals willing to serve state interests.[377] Regionally, Iran relied on groups associated with it to undertake cyber operations, including Hezbollah, the Syrian Electronic Army, and Kata'ib Hezbollah in Iraq, in an attempt to create a "Cyber Shi'ite Crescent."[378]

For example, Iran's support for Hezbollah in the cyber domain is done through the direct training of Hezbollah cyber operators. Iran also offers other forms of support such as providing a media platform to use propaganda about Hezbollah's cyber related influence operations through Iranian state-run news channels. Also, Since September 2010, Iran has hosted Hezbollah officials for "Cyber Hezbollah" conferences, which reportedly included the attendance of Hassan Abbasi, a political strategist and advisor of the IRGC[379].

LEGAL FRAMEWORK

To legitimize actions taken by Iran in its cyber warfare against adversaries, Iran has kept much of its activity secretive. It also tends to highlight non-aligned principles such as state sovereignty and the right to develop technologies for civilian uses. It also portrays the use of cyber tools in the framework of self-defense against perceived repeated and sophisticated attacks by foreign countries.

When faced with the allegations about its use of cyberspace to oppress freedoms, Tehran argues that these allegations are misleading and have nothing to do with the freedom of expression. It also argues that its cyber policies are crafted for securing domestic Internet as it relates to security and sovereignty of states and invokes the fact that it is frequently targeted by vicious

[376] Anderson, Collin and Karim Sadjadpour. Iran's Cyber Threat: Espionage, Sabotage and Revenge. Carnegie Endowment for International Peace. 2018.
[377] Frank J. Cilluffo, Sharon L. Cardash, Cyber Domain Conflict in the 21st Century, 14 Seton Hall J. Dipl. & International Relations 41 (2013)
[378] Paulo Shakaria, Jana Shakarian. *Introduction to Cyber-Warfare, a Multidisciplinary Approach.* Syngress. 2013.
[379] Levi Maxey. "Hezbollah Goes on the Cyber Offensive with Iran's Help". The Cipher Brief. January 30, 2018.

cyber-attacks to justify that it has the right to strengthen its cyber space security.[380] Therefore, the Iranian politics is the main source of influence on this dependent variable.

MILITARY-CIVILIAN RELATIONSHIP

As part of the means that Iran uses to enhance its capabilities in cyberwarfare, it has exploited civilians to boost its resources. Iran is building capacity through several confluent approaches. These include developing a trained cyber force, leveraging alliances, and mobilizing the considerable talent of Iranians in the cyber field.

Iran's decision-making process is obscured, and its cyber capabilities are not controlled by the presidency or any civilian component of the government. Iran has embarked upon a $1 billion cyber program to boost its capabilities: developing new technology, hiring experts, and moving swiftly towards a centralized filtering system. Iran created an Iranian Cyber Army (ICA) reportedly to hack into government and business websites to generate international awareness of its presence.[381] The activity of this cyber army is believed to be overseen by the Intelligence Unit of the IRGC,[382] which claims that these cyber operations rank as the second-biggest cyber army in the world.[383] As such, this cyber army can be used as a highly-organized and well-trained entity to carry complex and dangerous cyber operations against Iran's adversaries and can therefore pose a serious threat to the U.S.

The same Iranian actors responsible for espionage against the private sector also conduct surveillance of human rights defenders, who rely on social media and digital communication platforms for their activity.[384] These attacks on Iranian civil society often foreshadow the tactics

[380] "Iran rejects UN criticism of its cyber security rules". Reuters. Oct. 12, 2012. https://www.reuters.com/article/iran-security-un/iran-rejects-un-criticism-of-its-cyber-security-rules-idUSL1E8LP8YD20121025

[381] Frank J. Cilluffo. "The Iranian Cyber Threat to the United States". Statement to the US House of Representatives Committee on Homeland Security. Apr. 26, 2012. P. 5.

[382] Ilan Berman. The Iranian Cyber Threat. Statement before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies. March 20, 2013.

[383] Frank J. Cilluffo, Sharon L. Cardash, Cyber Domain Conflict in the 21st Century, 14 Seton Hall J. Dipl. & International Relations 41 (2013).

[384] Caught in a Web of Repression: Iran's Human Rights Defenders Under Attack". *Amnesty International*. https://www.amnesty.org/en/latest/campaigns/2017/09/iran-human-rights-defenders-caught-in-a-web-of-repression/

and tools that will be employed against other targets and better describe the risks posed by Iranian cyberwarfare.

ASSESSMENT OF IRAN'S POTENTIAL FUTURE DISPOSITION

In order to assess the potential future disposition of Iran in connection with cyber warfare, three issues must be considered. First, the future of the JCPOA and the impact of this future on the relationship of Iran with the West, in particular the United States. Experts argue that following the JCPOA, cyber threats emanating from Iran decreased;[385] however, the withdrawal would precipitate the opposite trend. In fact, the Iranian leadership has indicated that it would consider all options in the case of the withdrawal of the U.S. from the JCPOA[386]. One of those available options is cyber operations. Second, the threats to the survival of the theocratic regime. Third, Iran's regional hegemonic ambitions. Based on these factors, the most likely and the most dangerous trajectories will be as follows.

MOST LIKELY FUTURE TRAJECTORY

In all likelihood, Iran will continue to develop its cyber capabilities and expand the network of proxies from traditional ones to include newly recruited proxies, such as Iraqi groups being supported by Iran. Domestically, the IRGC and associated entities will continue espionage activities against its citizens to ensure a successful oppression of any popular protests that could make use of cyberspace against the regime. Regionally, Iran's cyber warfare will follow in the footsteps of its military and power projection in the region and beyond. Relying on the IRGC and affiliated proxy Shia client groups, it will continue to focus its sabotage efforts against its neighboring Arab countries, including targets crucial to U.S. interests such as ARAMCO in an effort to counter its adversaries and expand its interventionist policies. Globally, it will focus its efforts on espionage operations aiming to collect data in order to influence public opinion through propaganda following the Russian experience in 2016 presidential U.S. elections. For the same reasons, Iran's cyber espionage operations against the United States may target social media sites, such as Twitter and Facebook, and Government institutions that holds troves of

385 Morgan Chalfant. "Experts say US should expect more Iranian cyberattacks". The Hill. January 5, 2018.
386 "FM: Iran may quit Nuclear deal if US withdraws". Fares News Agency. September 29 2017.

personal data. Further, in retaliation to the recent statements made by President Trump against Iran's destabilizing activity in the region, the Iranian regime may target businesses belonging to the President's family and relatives. In the trajectories of targeting the West and the U.S., Iran is expected to rely on domestic and regional proxies.

Most Dangerous Future Trajectory

The most dangerous scenario includes much more extensive and dangerous damage targeting U.S. domestic infrastructure and disruption of U.S. military operations. To illustrate, since Iran relies heavily on the energy sector and often targets this sector, the U.S. energy sector is expected to be the target of Iranian sabotage and espionage. Although most of Iran's activities in the West has been for data mining or financial benefit, and that its most severe attacks were focused on the region, a cyber-attack on vital infrastructure facilities, such as nuclear facilities or energy plants, in the United States cannot be ruled out completely. There have already been prior indicators of such intent when an Iranian hackers linked to IRGC were sanctioned for conducting denial-of-service attacks against U.S. banks between 2011 and 2013.[387]Furthermore, since Iran, its proxies and allies are becoming the target of Westerns military operations such as the recent military operation conducted by the U.S., the U.K., and France on Syrian military facilities, Iran may choose to escalate further and target the United States bases in the region by cyber-attack operation aiming to disrupt the U.S. military operations in Syria, Afghanistan and Iraq, for example. Such operations are complicated and requires expertise and vast technical resources. Therefore, Iran may rely mainly on its elite cyber force, the "Passive Defense Organization."

Informing U.S. Cyber Strategy

As stated above, since it is expected that Iran would likely focus its cyber-attacks attention on the energy sector, it becomes necessary to realize the importance of allowing additional monitoring of facilities and internet connected equipment to prevent any fall and failure. Coordination with the relevant government entities, such as the Department of Energy, is crucial. In addition, the focus of Iran's cyberspace activity is directed against the West, including

[387] Morgan Chalfant. "Experts say US should expect more Iranian cyberattacks". The Hill. January 5, 2018..

the United States and, therefore, requires appropriate defensive arrangements, beginning with an up-to-date doctrine of cyberspace defense.

Moreover, and since Iran's neighbors are a primary target of its cyber warfare, it would be advisable to highlight the importance of this field to encourage the Arab States to strengthen their cyber capability in order to face the Iranian threat.

Recommended Areas for Future Research

Future policy planning and related research should take into account the possible future trajectories outlined above and focus on the ways to effectively address the implications to the United States, including possible means and methods to deter attacks that might pose a threat to infrastructure, the energy sector or American interests, directly or indirectly. In addition, it is crucial to encourage civil targets such as universities and the private and media sectors, to examine ways Iran or its operatives could target personal information as part of any possible misinformation campaigns to undermine American society and its values.

Further, and since Iran has exported its cyber capabilities and expertise to its allies in the region, such as the Assad regime or Hezbollah, within the context of political oppression, where this technology and know-how was used for massive misinformation and propaganda, it is a cause for concern that it can be used by other actors for both espionage, sabotage, and misinformation campaigns against the West, and the U.S. in particular. Therefore, it is essential to conduct research into the possible misuses of Iranian cyber expertise and technology for new threats in areas such as propaganda and misinformation using social media. Nonetheless, since some of Iran's previous attacks, such as the attack on a Saudi petrochemical company, are believed to have intended to cause deadly cyber-attack , it is recommended that future studies examine whether such deadly attacks are possible and whether Iran is capable of developing such capabilities.

DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA

The respected marshal has told us that if we add an idea to an egg … we can break the stone with that egg.

-Om Yun Chol, North Korean weightlifter
2012 Olympic Gold Medalist

INTRODUCTION

North Korea's broad strategic culture can be characterized as aggressive and offensive oriented – directed primarily by Kim Jung-Un's personal deposition buttressed by the Ju-Che ideology[388]. Hence, DPRK's stance towards every state affairs including cyber are ultimately heavily influenced by how Kim Jung-Un understands the situation and how he perceives as 'relevant context'. Because cyber-attacks are most likely directly order by Kim Jung-Un, it is important to understand the North Korean leadership's perspective while also taking into consideration the unique and isolated nature of DPRK in order to comprehensively estimate what North Korea will do with cyber.

DEFINING DPRK'S STRATEGIC CULTURE

North Korea is a totalitarian regime that has been led by the 'art of tyranny' over the course of the three Kim's: Kim Il-Sung, Kim Jung-Il, and Kim Jung-Un. Due to the state's unique birth as a result of the Korean Peninsula separation at the end of World War II in 1945, DPRK is heavily influenced by the geopolitical waves that engulfed it after the sudden liberation from culture-wiping Japanese rule. While the U.S. administered the southern half of the Korean peninsula, the Soviet Union administered the Northern region, where Kim Il-Sung spearheaded the creation of a new state, the DPRK, a stage where he pursed his own personal political agenda after being the soviet-designated premier.

[388] Juche can be characterized as independence or self-reliance (Charles K. Armstrong, "Juche and North Korea's Global Aspirations", North Korea International Documentation Project Working Paper #1, Woodrow Wilson International Center for Scholars.

Since then, DPRK developed a unique strategic culture which is characterized below by Ph.D. Hwang Il Do[389]:

- Imperialistic threats from the United States or Japan are overwhelming; North Korea is under constant threat from them; and international institutions like the United Nations are built for the interest of imperialist countries;
- Diplomatic measures can't buy any object and only armed conflict is absolutely important;
- The power of optimistic will or solid ideology is more important than physical capability;
- Asymmetric strategy, tactics, and weapon systems to attack the enemy's rear or core are preferred; and
- When the objective situation is unfavorable, showing off the offensive attitude pays off.

INDEPENDENT VARIABLES

HISTORY

The overarching perception shared by every North Korean resident is the perception of 'us'[390] and 'them'. This perception has been shaped by carefully executed political initiatives over decades, and also a product enabled due to the DPRK's unique Chosun history.[391] 'Us', to North Koreans, refers to the decedents of the Chosun dynasty who suffered invasions by 'them'.

Chosun is also the spelling of the first two characters (조선) of the DPRK's Korean name: 조선 민주주의 인민 공화국– next four letters represent 'Democratic (민주주의), the next two represent 'People (인민)', and the last three letters represent 'Republic (공화국)'. Although not included into their English country name, the historic sense of Chosun remains in the official state title, showing the state's great ties to the past.

South Koreans associate themselves significantly less with 'Chosun' and merely remember it as a historic past when "Kings and Queens ruled the lands with swords being the main weaponry

[389] Hwang Il-Do, "Framing North Korea's Strategic Culture From *With the Century*", May 29, 2013
[390] Derived from 'Uri' from 'Uriminzokkiri', state-controlled website that provides news from North Korea's Central News Agency. 'Uri' translates into 'us' in English.
[391] Chosun Dynasty (1392 – 1910) consolidated Korea's national boundaries and distinctive cultural practices.

of war". While the North still associates itself with 'Chosun', South Koreans have a widely used phrase that goes "Are you from Chosun Dynasty?"- similar to an English equivalent of "where did you dig up that old fossil?" implying that to whomever the phrase refers to is an old, outdated person. This comparison shows how North Korea's sense of historic identity remained relatively uninfluenced since Japanese occupation, compared to other open economies and nations more culturally connected with the West. The significance behind North Korea's association with the historic past is that it allows for an easier embedding of the 'us' and 'them' mentality, a perception that also buttresses the 'Ju-che' ideology.

Figure 1. (Left) Traditional 'Chosun' clothing worn as the main attire for daily news anchor in North Korea, (Right) More Westernized South Korean daily news anchor.

Before the birth of the current regime and the conceptual 'us' and 'them' divide amongst North Koreans was the sudden historic event of the Korean Peninsula becoming independent from the Japanese colonization in August 1945. Historically, the Korean peninsula has suffered from invasion from empires of the north (China) and from the South (Japan). Just before the division of the Korean peninsula, independence was fought for against the Japanese by multiple liberation armies, but it was ultimately heavily influenced and brought about by defeat of Japan to the U.S. Previous Japanese occupational operations in the region played a key role in the formation of the DPRK as a state as Japanese ruling in the region resulted in a 'vulnerable society'[392] that gave birth to the Kim family and Kim Il-Sung establishing a unified military to safeguard the Kim family and the North Korean elite society.

[392] Vulnerable society in essence means Northern region of the Korean peninsula was deprived of intellectuals, institutions, and economy. Explained further in the politics section.s

The conceptual spectrum that characterizes 'them' encompasses i) the United States of America, ii) capitalist societies, and iii) South Korea, with its embracing of what North Korea perceives as 'western cultural invasion'. In the end, all entities characterized as 'them' share the underlying sentiment of being a 'threat' – clear intent and capability to harm members of North Korean just as they experienced in the past 'invasion' by the U.S. and by the Japanese. In addition, because North Korean residents have a long history of daily interactions with the military has led them to share the same perception and mindset that they are under constant threat.

The aforementioned perception has been embedded into every resident's mind in North Korea throughout the past three Kims' political initiatives and have resulted in a state wide shared view towards the 'outsiders' as being characterized as adversarial and a threat - down to the individual level. Such perception and view of 'us' and 'them' has led to the current indoctrination of the idea that maintaining a powerful military is the most important function of the state as server to the people. Although being relevant in the international stage is important for DPRK's political elites, detachment to external threat actors and their advocates such as the UN is therefore conceived essential to ensuring the safety of the North Korean society by residents. This reality allows the leadership a relatively easy society to control.

GEOGRAPHY

Geographically, after Japan declared surrender in August 15, 1945, the Koreans were divided into 'North Koreans' and 'South Koreans' where the 38th parallel acted as the dividing line. The division was enforced by the U.S. Army that governed the southern part of the peninsula from September 9th 1945 to August 15th of 1948, and by the Soviet Army that ruled the Northern part of the Korean peninsula from September 9th 1948 until the establishment of the DPRK government.

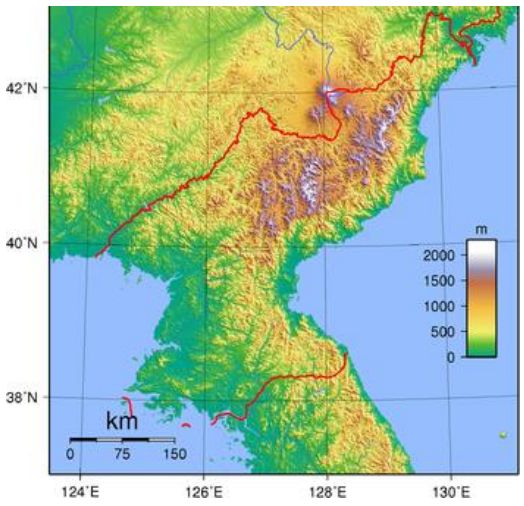


Figure 3 –Map of North Korea showing 80% being highlands and mountainous (unfit for agriculture)

The northern part of the Korean peninsula is composed of 80% mountainous ranges rendering the nation highly incapable in achieving the state's agricultural self-sufficiency objective. Most of the population lives in the plains and low lands. North Korea's agricultural environment can be described as "catastrophic" [393] due to soil erosion, depletion, and increased flooding, in turn caused by over-farming and accelerated deforestation. Based on satellite imagery, it has been estimated that 40% of forest cover has been lost since 1985.[394]

POLITICS

DPRK's politics are dominantly about the Kim family. The Kim family always needed to dominate domestic politics[395] and their biggest threats were regime-cleavage by either outside force or coerced abdication by internal politics.

For North Korean political elites, war exists to provide the level of tension required to sustain the current domestic power structure. War plays an important role in ensuring political stability over the three Kim generations and social systems have been convoluted to a degree where show of force by the leadership is necessary in order for that leader to retain power. As so, the DPRK has

[393] David J. Tenenbaum, "International Health: North Korean Catastrophe.", January 2005, US National Library of Medicine, National Institutes of Health, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1253723/
[394] Raven, Peter (2013-09-09). "Engaging North Korea through Biodiversity Protection". Science & Diplomacy. 2 (3). Archived from the original on 2013-10-29.
[395] Kongdan Oh, Ralph C. Hassig, "North Korea's Nuclear Politics.", September 1, 2004, Brookings Article. https://www.brookings.edu/articles/north-koreas-nuclear-politics/

been pursing hostile foreign policies which ultimately led to the creation of nuclear arsenals. Although continued investment toward nuclear capabilities forced the DPRK to be placed into a gridlock situation where further external display of force is needed, despite its real intentions being internal show of force, rendering it incapable of maneuvering without attracting further international sanctions.[396]

An in-depth overview of how each Kim retained power not only helps understand how the DPRK's political structure has been constructed around the Kim family's power sustainability, but it also helps to understand how each Kim perceived different situations they faced while succeeding power as well as during their reigns as 'Great Leader', 'Dear Leader', and 'Young General.'

Table 1. Comparison of the Three Kim Systems and Performances[397]

		Kim Il-sung	**Kim Jong-il**	**Kim Jong-un**
SYSTEM	Addressing	Great Leader	Party Centre Dear Leader	Young General Supreme Leader
	Title	General Secretary of the Party President Supreme Commander	General Secretary of the Party **Chairman of National Defense Commission** Supreme Commander	Chairman of the Party **Chairman of State Affairs Committee** Supreme Commander
	Ruling Apparatus	KWP (Politburo) **Central People's Committee**	KWP (Secretariat) **National Defense Commission**	KWP (Political Affairs) **State Affairs Committee**
	Ideology	Juche Idea	Kimilsungism	Kimilsungism-Kimjongilism
PERFORMANCE	**Policy**	**Building Socialism and Communism (Balanced Role of Party, Cabinet, and Military)**	**Military First Policy (Emergency Control, Reduced Role of Cabinet)**	**Party Centered Rule (Balanced Role of Party, Cabinet, and Military)**
	Leadership	To the people	**Behind Curtain** **Close Aide** Reports Politics Gift Politics	**Increased Transparency** **More Public Show** Reports Politics Gift Politics
	Power Background	**MountPaekdu Line (Anti-Japanese Guerrillas, 1st Revolution Generation)**	**Ryongnam Hill Line (Party+1st Revolution Generation)**	**Generation, Class Replacement**

[396] David E. Sanger, David D. Kirkpatrick, Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More.", The New York Times, October 15, 2017, April 13, 2018, https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html

[397] Hyung-Seog Lee, Kwang-Jin Kim, Thomas Fingar, Yong Suk Lee. "Analyzing the Structure and Performance of Kim Jong-un's Regime". Research Brief of the Shorenstein Asia-Pacific Research Center at Stanford University and the Institute for National Security Strategy. June 2017

KIM IL-SUNG

As shown in the last row of Table 1, 'Kim Il-Sung (first Kim)', gained power at the onset from the anti-Japanese sentiment of the people. Before the time of Kim's campaigning to rise to the top was Japan's colonization operations. They utilized the Northern Korean Peninsula region as an industrial zone focused on supporting the Japanese Emperor's Military against their adversaries, including the current Chinese. Such power background allowed Kim's political campaign to be centered around the idea that building socialism and communism can bring recovery to the economically, socially, and morally deprived colonial *status quo*.

The Japanese education policy of carving out traditional language, culture, and other endogenous heritage with the end goal of 'cultural take over' rendered Kim Il-Sung to confront a 90% illiteracy rate among adults in 1947, when he embarked on his 'People's Economic Development Plan' initiative. Kim Il-Sung obtained sufficient political power to pursue such initiatives after he, with the support from the Soviet Union, managed to out compete other regional political parties and dispersed existing armed groups scattered across the northern peninsula.

Kim Il-Sung's *'Establish the Party, Establish the Military, Establish the Nation'* political agenda initiated with the residency of Soviet Army in Northern Korean Peninsula, followed by the establishment of the 'People's Military' in August 1945. During the period, the military served the party and party's objectives, and hence the two were not as ideologically assimilated as they are now. During the execution of his education policy, Kim Il-Sung geared towards fighting the 90% illiteracy rate to start instilling to the people the greatness of his accomplishments. Kim Il-Sung's propaganda buttressed with educational policies designed around empowering him has placed the formal general as a legendary figure and enabled Kim Jong-Il to work with the military to dominate the party.

Figure 3 – (Left) North Korea Propaganda Designed to re-incite hatred toward Japanese and their killing of Koreans. Historic pictures of civilians and women being victim is used as a background. (Right) General Kim Il-Sung depicted as liberator from the Japanese occupation.

KIM JONG-IL

Along with the fall of the Soviet Union was the rise of the military elites in the North Korean political scenes. Kim Jong-Il, the son of Kim Il-Sung rose to power by pursuing the 'Military First Policy,' which enabled a reduced role of the party cabinet and steep status rise of military generals in the power structure. This was necessary as Kim Jong-Il lacked the political capital his predecessor derived from the wide spread anti-Japanese warrior brand.

Kim Jong-Il rose to the top with the support from the military and allowed them deeper involvement in political affairs and the governing of the state. This has also contributed to the current stark perception among the North Koreans of 'us' and 'them' amongst the North Koreans, where you are either a friend or a foe.

The fall of the Soviet Union also led to North Korea reinforcing their 'Ju-Che' ideology, where the centerpiece is the Party and Military leader – Kim Il-Sung and his 'ryeongdoja'[398] status. The concept of 'ryeongdoja' was formed as North Korea had to survive the devastating outcomes of the Cold War and also to consolidate power around Kim Il-Sung. Throughout his rule, Kim Jong-il emphasized that the "military is the centerpiece in accomplishing the self-sufficiency revolution and is the pillar of the state," all the while emphasizing that the lack of "ideological

[398] 'ryeongdoja' is defined as the 'supreme leader' but is also used widely in all occasion where North Korea has performed better than other nations in order to attribute the success to the 'great leadership' of Kim Jung-un

mental arming" and the "military's separation from national politics" were the two reasons for the Soviet Union's downfall.

Kim Il-Sung and his efforts to lead by military might and military-minded civil society has ultimately resulted in the current grid-lock situation due to South Korea's economic development along with the presence of the U.S. military rendering the North Korean military efforts to take over the peninsula unfruitful. The domestic sociopolitical outcome of Kim Il-Sung efforts was the continuation of the Kim family's rule and escalated threat perception shared across the North Korean military and civilian society.

Kim Jung-Un

Kim Jong-Un, faced with the job to rule a state built around military mindset, assumed power by maximizing his capabilities of exerting physical power and instilling fear. Broadcasting the arrest of his uncle Jang Song-taek, the right-hand man of deceased Kim Jung-Il, and the machine-gunning execution that followed is a representation of efforts by Kim Jong-Un to be perceived as a 'strong man' and a person to not be meddled with. The main audience was no doubt domestic political power elites and military generals. The event was significant as it led to diplomatic backlash from China where Jang Song-taek was trusted as a key man between the two states.[399] Kim Jong-Un's pursuit to assassinate his brothers residing under foreign protection also represents his deliberate and continued efforts to gain and retain power in a state where his predecessors left as extremely 'aggressive' by having pursed a 'military-first' policy.

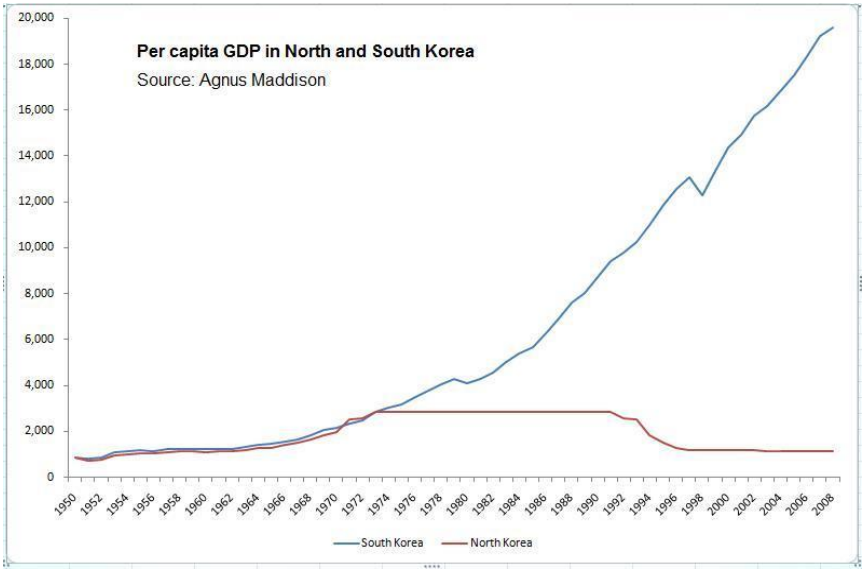
Such political need to focus adversarial sentiment across the society and the military has led to a characterization of 'them' in line to past Japanese colonization era. Not only that, as described previously, the pressure to address changing international circumstances such as the collapse of the Soviet Union and South Korea surpassing North Korea in the economic and military domains has forced not only the North Korean Kim leaders but also the policymaking elite class to

[399] This has also been demonstrated when China refused to engage in talks with North Korea shortly after the execution of Jang Song-taek. Series of event followed that led to the most recent Kim Jung-un's remarks that Japan is a ten-year enemy but China is a hundred-year adversary.

continue policies that constantly invoked the international society to isolate the state. The policy failures of the leading class have been continually masked from the mass population in North Korea and propaganda that emphasizes the adversarial nature of the constructed 'enemy', 'them', persists to be carried out across the nation.

Figure 4- North Korean propaganda designed to incite hatred towards US military. Victims drawn are the helpless woman and children while the oppressor is the US military.

ECONOMY



The North Korean economy is a centrally planned economy where role of market was suppressed in full by the government.[400] The fall of the Soviet Union negatively impacted North Korea's economic status,[401] as national production was concentrated towards waging war

[400] This has been changing over the last few years after numerous reporting on market activities across DPRK.
[401] Bluth, Christoph (2008). Korea. Cambridge: Polity Press. p. 34.

against South Korea for unification, a long-lasting mission of the Kim family. Having to realign foreign relations in respect to strengthening economic ties after the failure suffered from the dependency on the Soviet Union, the DPRK's economy has been sustained with assistance from Russia and China. As the two nations have the incentive to use North Korea as a buffer to avoid further expansion of 'Western influence' represented by Japan and South Korea. Although North Korea had a similar GDP per capita to South Korea until the mid-1970s, it is now one of the poorest nations in the world due to continued economic sanctions and lack of technologies to exploit its natural resources. Conditions being so, the second most important concern of policymaking elites has always been economic development.[402]

Former U.S. Secretary of State Rex Tillerson stated on January 2018 that international sanctions towards North Korea are "really starting to hurt" [403] despite a number of nations not implementing full measures toward the combined efforts. Failure to sustain economically sound conditions of the state is pressing for the North Korean elites as they have been on the issue for decades and they are addressing the issue by all means possible: the DPRK even sends civilians as cheap laborers to foreign nations in exchange for internationally banned weapons.

RELIGION

Religion is strictly banned in North Korea, where members of the Kim family are de facto 'gods'. It was imperative that the government establish the Ju-Che ideology as the only belief system in order to maximize its ability to influence the people. As the Japanese had already acted on similar course of action during the colonization era, Kim Il-Sung had little difficulty in eradicating what was very little religious activities in North Korea. Kim Jung-Il and Kim Jung-Un followed the continued efforts to intensify the belief that portrayed the Kim family as de facto 'gods' while suppressing other belief systems.

[402] First key concern of the policy making elite and the Kim family would be the continuation of the power structure.

[403] Reuters World News, "Tillerson: Evidence sanctions 'really starting to hurt' North Korea", David Brunnstrom, January 17, 2018, https://www.reuters.com/article/us-northkorea-missiles-tillerson/tillerson-evidence-sanctions-really-starting-to-hurt-north-korea-idUSKBN1F62UV

"There's a five-decade history here (DPRK RGB) and a lot of institutional and operational memory… These people learned under tough, hardened spymaster and operations chiefs"

-Michel Madden, Founder and Director of NK Leadership Watch and Visiting Scholar to US-Korea Institute at SAIS, Johns Hopkins

PHILOSOPHY

Ju-Che ideology is a philosophical thought that is a centerpiece to every social facet in North Korea. 'Ju-Che' translates as 'self-reliance' and asserts that North Korean's must act as "masters of the revolution and construction" which will enable a stronger nation that can achieve true socialism.[404] Historic failure of the Soviet Union left the North Korean government to stand on its own in respect to D.I.M.E[405]. There was a great need to motivate the mass public to achieve such goals of the state and Ju-Che ideology justified the government's extraction of labor under Kim's directives. In relation to Kim Jung-Un, the Ju-che ideology also acts as a shackle to 'prove his worth': Kim Jung-Un, being the third Kim to succeed an isolated state, has a strong need to prove or at least convey to the public that the old idea of 'self-reliance' is still relevant and that he is the only one able to lead the nation towards it.

DPRK'S CYBERWARFARE STRATEGIES AND CAPABILITIES

Continued pursuit of an aggressive set of military policies placed the North Korean elites at a grid-lock situation against South Korea, the U.S., and the international society, which meant that they could not take any more military action without escalating the situation. The perception of the sharply divided 'us' from 'them' and the DPRK's pursuit of offensive-oriented policies have forced the international community to purse multi-disciplinary policies that most recently led Kim Jung-Un to engage with the U.S. via South Korean intelligence and diplomat ministers. The Chinese declaration that they would not respect their past agreement to support North Korea in time of war against the U.S. has left Kim Jung-Un with little room to maneuver in addressing domestic power retention issues, which were mainly challenged by the failing of the state to provide food and economic stability.

[404] Juche Idea: Answers to Hundred Questions. Pyongyang: Foreign Languages Publishing House. 2014.
[405] Diplomacy, Information, Military, Economic – the four instruments of national power.

Historically, the pursuit of aggressive military policies not only consolidated power, but also overwhelmed South Korea. However, because of the existence of the US military base in South Korea and the economic surpassing of South Korea, it is now a clear fact that North Korea has no rational hopes of achieving their party's grand mission to unite the Korean peninsula by military might. As so, efficacy of conventional use of force have been undermined to the maximum extent without risking engaging in full-fledged war. Continued investment in nuclear capabilities, which the Kim family and the North Korean elites perceive as the only means to be secure from U.S. regime cleavage, has rendered the ever more agitated international community spearheaded by the U.S.

Because exercising conventional capabilities would escalate the situation out of control for the North Korean leadership, it was necessary that the party and the military find a solution to enhance the efficacy of use of force in a method that does not escalate the current status quo. Such perception and need of the ruling class has resulted in unexpectedly sophisticated cyber capabilities to be developed, which surprised the western cyber security experts during the SWIFT and WannaCry hacking incidents.

DEPENDENT VARIABLES

ROLE OF FORCE IN STATE AFFAIRS

To this day, showing force has played a significant role in the continuation of the power structure in North Korea -as regular citizens and the majority of the military have been, for the past six decades, brought up to believe that war is always around the corner and that the state leadership is protecting the nation from the constant threat from 'them'. The history that the North Korean government has been recognizing and teaching is one that is riddled with an endless fight for survival -where Korean ancestors fought for survival from 'barbarians' invading from the north (China) and pirates from the south (Japan). This distinct perspective does not hold true for cyber in the case of North Korea.

As aforementioned, war in conventional sense is no longer a viable option from the perception of North Korean policymaking elites as any further escalation of tensions may lead to the end of

Kim's regime. Hence, a shift to a realm where that is possible has been pursed whether by showing force to the outside or to the inside of the nation. Show of force is important domestically for the DPRK elites, but the current economic and diplomatic difficulty experienced by the DPRK is also making the show of force to the outside world more and more important for the elites. In this respect, the cyber domain offers the North Korean leadership a new war-capable-zone which not only allows it to be effective in respect to meeting the regime's economic needs via cyber means like industrial espionage, but also in the aspect of diplomacy where through cyber, the DPRK can place itself in a more relevant position to the Western countries.

North Korean cyber offensive capabilities have recently been considered by the international community to be far more superior than previously perceived. According to the U.S. Federal Bureau of Investigations (FBI), Sony suffered from cyberattacks that sabotaged its digital assets because the company planned to release an American film that undermined the North Korean leader. [406] The SWIFT system suffered from cyber intrusions that led to fraudulent transactions which ultimately helped alleviate the DPRK's economic difficulties. Such successful campaign instances provide the North Korean Reconnaissance General Bureau, the internationally attributed entity behind the cyberattacks, the necessary justification to continue their cyber activities as well as further invest in enhancing their capabilities.

NATURE OF THE THREAT

North Korea's leader Kim Jung-Il and Kim Jung-Un is referred to as 'spiritual father' and the state is referred to as the 'father land' by the government propaganda. However, the last decade has revealed that the 'father' being incapable of bringing food home will have to result in violence to retain power –such which systematically forces the policy to be more aggressive. For Kim Jung-Un, who was facing such realities, the cyber domain has proven to be an excellent tool to address the issue at hand.

[406] Some private firms and non-governmental cyber security assert that FBI's claims are based on dead end connections, it is assumed that FBI's attribution is accurate as they may posses' information undisclosed to the public.

For example, Sony, tried to release a movie title 'The Interview' which was themed around mocking the North Korean regime – such a film was an existential threat and would have damaged the Kim family's domestic reputation when the movie eventually flows in through the black market to North Korea. Former President Barack Obama stated in the December 19, 2014 end-of-the-year press speech that Sony made a mistake in pulling the film after experiencing damages from cyber sabotage which ultimately led to pulling the plug to premier the movie. President Obama said that producers should "not get into a pattern where you are intimidated by these acts." To North Korea, such remarks by the President of the United States and behaviors from the private sector companies would have been clear signals that their cyberattacks pressed where it hurt for their archenemies.

According to a former head of South Korean National Intelligence Service, Kim Jung-Un has proclaimed that "cyber, along with missiles and nuclear weapons, is a one-size-fits all weaponry that ensures our army the ruthless damaging capabilities". If the former head of South Korean National Intelligence Service was speaking the truth, it would be hard to doubt that expansion of cyber activities and investment in TTP capacity building would have been required of the DPRK government agencies as the Kim family's words are the *de facto* law and basis for policy formulation. Currently, cyber capabilities are deemed nurtured to meet Kim Jung-Un's expressed vocal expectation via structured education plans by the state:

1. Computer education at 'Middle School for Scientifically Talented: GeumSung 1 and GeumSung 2 in Pyeongyang' (평양의 과학영재학교인 금성 1,2 중학교)

2. 3-5 year higher education to be trained as 'cyber warriors' at 'Command Automation University: Mirim University' or '223CP: Moranbong University' (미림대학이라 불리는 지휘자동화대학 or 223 연락소라 불리는 모란봉대학)

3. Some 'cyber warriors' are trained at Kim Il-Sung University

Given such backgrounds, when Kim Jung-Un commanded to expand Bureau 6: Technology and Cyberterrorists in August 2012, an organization under Reconnaissance General Bureau [407] (RGB),[408] into the Strategic Cyber Command, it was swiftly implemented by the head of the RGB, Kim Young-Chol.[409]

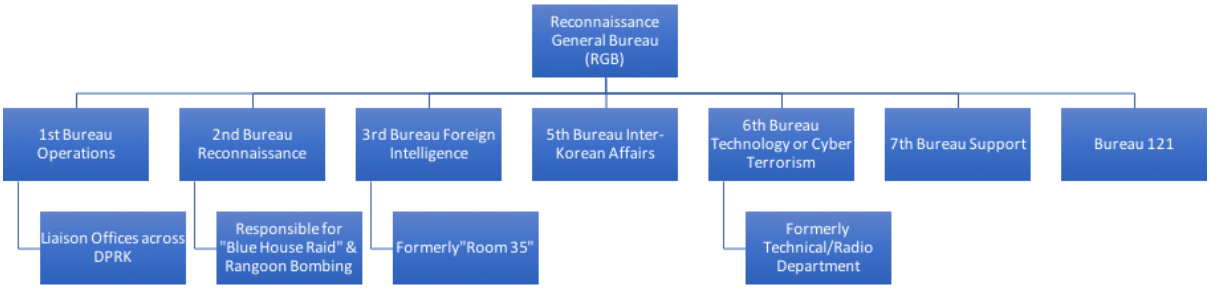


Figure 5- RGB organizational chart, compiled with information from The Korea Herald, 38 North, and CSIS.[410]

The RGB, also known as Unit 586, has been attributed to be the epicenter of the DPRK's cyber operations and has a long unique organizational culture. Subordinate to the DPRK's Korean People's Army, the RGB was formed in 2009 after a large restructure of several state, military, and party intelligence elements.[411]

The RGB inherited its predecessor organizations' culture of being resourceful, clandestine, and extreme. It can be said to have been the principal organization responsible for assassination attempts,[412] hijackings, plane bombings,[413] and kidnapping since the 1950s. The organization

[407] The general bureau is an integration of the reconnaissance department of the North Korean defense ministry, the "operations department" which developed infiltration routes for secret agents and "Room 35" in charge of international intelligence under the Workers' Party –"Reconnaissance General Bureau is heart of N.K. terrorism", Kim So-Hyun, May 26, 2010, The Korea Herald.
[408] Unit 586 is another name for RBG used on official occasions by DPRK
[409] Kim Yong-chol is head of national intelligence of DPRK and was appointed by Kim Jung-Un after the death of his predecessor Kim Yang-gon's questionable car accident. He was attributed to be the mastermind behind the attacking and sinking of South Korean navel ship in 2010.
[410] "North Korea Is Not Crazy," Insikt Group, June 15, 2017. https://www.recordedfuture.com/north-korea-cyber-activity/
[411] Recorded Future Insikt Group, "Report: North Korea Cyber Activity", July 25, 2017.
[412] Blue House Raid in January 20, 1968 against South Korean President Park Chung Hee
[413] Korean Air Flight 858 bombing in November 29, 1987

has also been considered as the advance guard for drug smuggling, counterfeiting, and such criminal activities.

Cyber operations being carried out by an institution with such organizational history will with high confidence maintain a similar mindset towards cyber and its utility as a means to an end. Historically, the RGB's unique sub-culture prioritizes the accomplishment of state goals over all else: this will continue to hold true for cyber activities as well, where the RGB is the primary implementor of North Korean cyber operations.

The cyber domain has proven to Kim Jung-Un and to the policymaking elites to be a realm which can be exploited without attracting uncontrollable tension or escalation. Kim Jung-Un and the elites serving the Kim family cannot stop taking advantage of the opportunities in the cyber domain due to internal politics and because cyber activities bring hard cash home. Because unspoken opinions of the DPRK's elite ruling class are more important than that of mass public, the elites' and Kim's reliance on cyber will intensify unless Kim Jung-Un finds the cyber realm no longer beneficial in respect to justifying his 'right to rule'.

EFFICACY OF THE USE OF FORCE

The cyber domain has proved to be the most efficient realm for the DPRK's military to carry out state sponsored operations that delivered to the needs of the regime in terms of economics and not escalating the tensions. According to Chris Inglis, the former deputy director of the U.S. National Security Agency (NSA), cyber is a tailor-made instrument of power for North Korea.[414] Most representatively, 'Lazarus', a group of hackers recognized across the cyber industry to be behind the Sony Pictures hack and WannaCry ransomware attack, has also been attributed by numerous private cyber shops with multiple campaigns against cryptocurrency exchanges in South Korea (exchange name: Coinlink).

[414] David E. Sanger, David D. Kirkpatrick, Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More.", The New York Times, October 15, 2017, April 13, 2018, https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html

Such campaigns directly benefit the financial state of the North Korean government while suppressing the potential for escalation of financial sanctions. In the end, advanced persistent threat capabilities of DPRK allowed industrial espionage, global cryptocurrency ransomware, and sabotage of specific companies lessened the pain of the regime having to provide to the mass public which shows that cyber domain offensive is directly aligned to the interest of North Korea.

Non-State Actors and Proxies

North Korea has been known to utilize a proxy in the assassination of Kim Jung-Un's brother at Macau. The poisoning of such an important individual, which would surely attract international attention, showed that North Korea will utilize proxies even in utmost important. However, the current gridlock has rendered the use of conventional force to result in significant retaliation including economic sanctions which greatly damage the North Korean leadership's domestic position.

In the cyber domain, cyber security experts only place four nations above North Korea's cyber capabilities (Russia, China, Iran, and the U.S.) and so North Korea would seem likely to have the least amount of incentive to utilize proxies or non-state actors in the cyber realm –as proxies' lack of skill in masking network intrusion or similar amateur failings would not serve even the most basic clandestine requirements from cyber campaigns and operations of the DPRK.

On the other hand, if the non-state actors or proxies can provide higher level of sophistication in achieving cyber offensive objective, North Korea would not hesitate to utilize such opportunities as they have been known to leverage proxies before. Although cyber activities or use of proxies have never been actually admitted by the DPRK, there seems to be confidence amongst the cyber domain experts that the DPRK has been utilizing proxies and non-state actors to maximize its benefitting from the cyber domain:

"North Koreans earn foreign money by developing software in China and performing hacking activities to collect national industrial secrets at the same time."[415]

-Seo Sang-ki - Chairman of Intelligence Committee, National Assembly, South Korea

"Chinese and North Korean soldiers exchange malicious codes and attack techniques created by Pyongyang."[416]

- Kim Hung-kwang, President of the North Korea Intellectuals Solidarity

In case that the above statements are true, they indicate that the DPRK is not just capable of working with non-state actors and proxies, but also indicates that it will almost certainly leverage non-state actors and utilize proxies to the maximum capacity in order to continue denying their involvement in cybercrime.

Although it is widely known that the DPRK carries out cyber operations in China, India, Malaysia, New Zealand, Nepal, Kenya, Mozambique, and Indonesia,[417] their presence is known to be very complicated to track as members of North Korean cyber operations mask themselves as software outsourcing companies, game developers, as well as disguise as employees of local companies. Obfuscation technologies including wide adoption of virtual private networks (VPN) and virtual private servers (VPS) to accomplish tasks such as large data transfer seems to already have been set as best practices for overseas North Korean hackers.

North Korea's use of proxies is further incentivized by the increasing rate of defection by the population who interacts with the outside 'them' world. Laborers dispatched to foreign nations by governmental efforts to bring home foreign currency has led to the realization of the discrepancy in reality by the civil individuals with foreign engagement. Individuals belonging to such population, despite extreme care of the North Korean government to keep things under

[415] Daniel Schearf, "North Korea's World Class Cyber Attacks Coming from China," *VOA News* (November 21st, 2013). Available at: https://www.voanews.com/a/north-koreas-world-class-cyber-attacks-coming-from-china/1795349.html

[416] Tim Maurer, "Cyber Mercenaries: The State, Hackers, and Power," Camrbidge University Press (December 21st, 2017), p. 132

[417] Recorded Future Insikt Group, "Report: North Korea Cyber Activity", July 25, 2017.

control, either choose to defect or end up spreading the sense of discrepancy once they are back in North Korea. In the cyber-warrior's case, they have more incentives to defect as they know they will be treated better elsewhere. The DPRK recognizing this has been known to send their hackers aboard under strict supervision and watch from other non-cyber operators.

LEGAL FRAMEWORK

Rule of law or legal egalitarianism does not exist in North Korea. Approximately 40% of legal statutes have been edited since Kim Jung-Un's reign started.[418] Due to the government's carefully curated social acceptance to power hierarchy, the notion of equality that is central to all socialist ideology is in reality completely disregarded.

Members of the civil society accept the discrimination between unofficial social rank as natural -a characteristic that has been passed onto the society due to the closeness with the military. Although North Korea asserts the idea of equality amongst all 'comrades', it goes no further than empty rhetoric that serves to justify concentration of power to a single individual –the three Kims.

Kim Jung-Un has prioritized cyber capabilities at par with missiles and nuclear warheads and that has generated more than sufficient legal grounds for North Korea to further invest in cyber capabilities. Investment towards gaming up North Korea's cyber capabilities began with Kim Il-Sung; after watching the American "shock and awe", it is reported that Kim Jong-Il warned his military that "if warfare was about bullets and oil until now, warfare in the 21st century is about information."[419] Kim Jung-Un took it more strategic when he declared that "Cyberwarfare, along with nuclear weapons and missiles, is an 'all-purpose sword' that guarantees our military's capability to strike relentlessly." Such 'supreme teachings'[420] of the de facto gods have led to not only to the justification for the state to further invest in cyber capabilities, but also to

[418] Mok Yong Jae, "Expert 'After Kim Jung-Un assumed power, 40% of legal statute have been edited'", December 7, 2017, Radio Free Asia. (목용재, "전문가 '김정은 집권 후 40% 가량 북 법령 개정'")
[419] David E. Sanger, David D. Kirkpatrick, Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More.", The New York Times, October 15, 2017, April 13, 2018, https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html
[420] According to Naver's Korean to English dictionary, 훈시 or 'teachings' used in this paper refers to 'To give an order or request to one's subordinate regarding matters that require attention when handling one's own mission'.

approach cyber as a key offensive tool of the DPRK government against their enemies. Cyber, for North Korea, was given birth by the father for the son to wield with the exclusive purpose of serving the state's interest. The lack of a legal framework that checks and balances the Kim family's power domination does not exist -on the contrary, because the legal framework revolves around hardening Kim's power, as long as Kim Jung-Un sees utility in cyber, the DPRK's cyber activities will not stop.

MILITARY-CIVILIAN RELATIONSHIP

In the DPRK, advance information communication technologies (ICT) is a distinct tool available only to select individuals in the state. Nationwide adoption of ICTs that fosters exchange of information amongst civilians has been systematically discouraged by the state to preserve their propaganda. The two aspects come together and enable the government to have an exclusive use of ICT mainly to achieve broad state objectives through the cyber domain.

Also, the DPRK's cyber capabilities and manifestation of those capabilities are exclusively administered by the RGB, which is one of the most heavily guarded and isolated facilities in North Korea –widening the divide between civilian and military's access to ICTs and cyber. Hence, it is highly improbable that civil hacktivism exists in North Korea. The 'cyber warriors' were originally trained overseas –mainly in China- and are well separated[421] from the rest of the society in order to perform to their maximum as well as to limit their identities being exposed to the outside world –even the domestic world. The reality that most residents in North Korea do not have access to open internet as well as sophisticated computing machines supports such realities. Although events of North and South Korean hackers collaborating with facilitation by

[421] JD Work, Professor of 'Cyber Threat Intelligence' course, Columbia University.

ethnic Korean hackers in China have been reported to exist behind data breach ATM malware attack in March 2017[422] –there doesn't seem to be any trend in activities similar to that nature.

The aforementioned characteristics of the state with military and civil societies that are very coupled together have undoubtedly necessitated from the leadership a socially perceived 'adversaries' to focus public attention on. To the civil society and to the military, the clear adversaries are 'them': the imperialist U.S. and its partner South Korea.

International Organizations established by 'them' according to 'their rules' are no different in adversarial nature and are conveyed equally threatening to the overall wellbeing of the North Korean society. However, regardless of the military and civil society's perception of the adversary, the leadership's and elites' real threat can be said to lay in their own making.

Because they have been masking their policy and ideology failures for far too long, the discrepancies between the reality of the world and how it is depicted by the North Korean government to the people now exposes the ruling class to the risk of the 'general population doubting claims and statements by the government'. Here lies the DPRK's vulnerability towards free flow of outside information. If open internet propagates and there is free flow of information, especially information which objectively represents the poor performance of the DPRK relative to the global economy, materializes in North Korea –the leadership of the government would crumble from the inside.

Because North Korea's self-sufficing, and hostile military-minded policies set by leaders who refused to relinquish power attracted international isolation, the North Korean society and its culture have been closed off from developments the world has faced. Such phenomenon, alongside the continued misinformation fed to the public to consolidate the Kim family's power have given birth to rising disbelief in the leadership at provinces where central government lacks strong reach and oversight. The North Korean government's ability to deliver provisions is the

[422] Mitch Haszard, "Threat Actor Groups of the Korean-language Underground.", October 26, 2017, Cybercrime Blog, Flashpoint. https://www.flashpoint-intel.com/blog/korean-language-underground/

key factor in remote provinces and the failure of the state and the policymaking class has forced informal market activities to spread despite extreme suppression by authorities.

Such increasing internal damage to the credibility and sustainability of power structure is a real threat to the North Korean elites and international sanctions against the state intensifies the problem.

ASSESSMENT OF DPRK'S POTENTIAL FUTURE DISPOSITION

MOST LIKELY FUTURE TRAJECTORY

Encompassing previous detailing of North Korea's inclination to cyber offensive, beyond the obvious continuation of current activities, one of the top three most likely future trajectories of Pyongyang elites would consider installing malware that can lay dormant in U.S. critical infrastructure systems,[423] but that can effectively take down the system from its building-block level and up when invoked. Critical infrastructure, such as the three core U.S. electricity grids, are clear high value targets to cyber intrusion.

Although electricity market experts assert that due to the distributed control system nature of the grid a complete shut down of power grid may seem unrealistic, it must be taken into consideration that the RGB learns from foreign actors and the Ukrainian case serves as a great example for North Korean strategists to concept out a new APT.[424]

Cyber-Kinetic attacks can pose advanced capability to render critical damage in the 'Industrial Control System Network (ICSN)'[425]which encompasses the electricity system. Malware that penetrates into the ICSN can allow the human behind the keyboard to figure out how the infiltrated electricity grid system is engineered and cause direct physical harm to key

[423] President Barack Obama - in his executive order 13636 which calls for buttressing of the current critical infrastructure cyber security- defined critical infrastructure as 'systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.'

[424] Richard Clarke, Robert M. Lee, Kevin Mandia, Liam O'Murchu. "What is the Extent of the Problem?", The 2017 Conference Energy Grid Cybersecurity Threats & Solutions, March 3-5, 2017, http://gridcybersecurity.org/

[425] "Types of Industrial Control System", Definition, Trend Micro, https://www.trendmicro.com/vinfo/us/security/definition/industrial-control-system

components that make up the electricity distribution network. Cyber land mines, which can also be planted into ICSN, can bring down a power grid with a stroke of a key from the attacker.

In the United States, which has three major girds, if an attacker knocks out the ICSN network of any one of those three or even a major portion of those three, it is estimated that the power could be out for weeks, months, and up to a number of years for civilians and government alike. A single grid power out would lead to tens of millions of Americans being deprived from all kinds of other communications, medical supplies, and availability of just about everything we need to sustain 'normal' life and culture.

Because actual trigger of dormant malware would be a clear act of war, the DPRK would most likely only plant the malware as a fallback for the regime and, with high confidence, never pull the trigger unless Kim Jung-Un's life is directly threatened.

Second most likely is, with rise of the cloud computing industry, hijacking of computing infrastructure, including hacking of Amazon Web Services accounts of poorly secured programmers can become a lucrative exploit for North Korean hackers who are very cost sensitive.[426] Individual developers with inappropriately loose cyber security policy allocation by Identity Access Management (IAM) or self-imposed can expose themselves to a watering-hole attack regarding educational materials on operating PaaS or IaaS which have risen in population over the years amongst developers. Account credential theft can benefit the DPRK in multiple ways including, utilizing the computing resources to mine cryptocurrencies, leverage for botnets, and mask malicious deployment. It is highly probable that individual server operators across the world whose main expertise are not on the servers are all potential targets for North Korean hacker groups in this regard.

Last of the three most likely future trajectories is Kim Jung-Un and the RGB's investment toward long term (15~30 years) cyber-content capacity building. Content is key as it is central to the media industry and the public's consumption of information. The RGB has a long history of

[426] Jodl Mardesich, "Developers, Check Your Amazon Bills For Bitcoin Miners", April 15, 2014, readwrite, https://readwrite.com/2014/04/15/amazon-web-services-hack-bitcoin-miners-github/

experimenting their cyber capabilities in South Korea in terms of manipulating the public sentiment. Currently, due to what deems to be intelligence failure, former directors of National Intelligence Service of South Korea were arrested alongside charges of bribery. The two have been working to counter what they claim is North Korean influence by operating South Korean counter action team.

North Koreans and South Koreans have been fighting for the public's attention on numerous platforms, including Facebook, Twitter, Naver, and Daum [427] on political sentiments and controversial issues via pre-worded commenting, identifying suspicious ids, and directly communicating with the public. Although controversial, the undeniable fact is that the DPRK is aware of platforms and their utility for social manipulation in democratic states.

In this respect, the Russian interference in the American election would also have been a benchmark learning experience for RGB strategists. Considering the above along with the longevity nature of totalitarian regime policies, it is possible to hypothesize that North Korean strategists would seek to influence a democratic state's public opinion by indirectly affecting one of the five blocks in the digital media value chain.[428]

The digital media value chain segments are creation → management → distribution → awareness → activation, and North Korea can concentrate their cyber capabilities in influencing either the creation segment of the value chain or the management. For example, the RGB can work to create original content that is designed around mockery of existing elected policymakers -it would not only significantly undermine the RGB's target individual, but it would also act to discourage policy makers to 'meddle' with North Korea.

MOST DANGEROUS FUTURE TRAJECTORY

The most dangerous future scenario would be North Korea wrongly being accused of a cyber offensive and being cornered into a kinetic act of war resolution. Most recently, North Korea had been attributed to Olympic Destroyer malware outbreak which aimed to sabotage the Winter

[427] Naver and Daum are top internet portals in South Korea
[428] Dorian Benkoil, Adjunct Professor at Columbia University School of International and Public Affairs

Olympics held at Pyeongchang, South Korea. However, this has been proven false by Kaspersky Lab engineers, who strongly assert that Lazarus (North Korean cyber warriors) didn't write the code despite their appearance to look so.

"We can say with 100 percent confidence that the attribution to Lazarus is false…It is not possible to completely understand the motives of this action, but we know for sure that the creators of Olympic Destroyer intentionally modified their product to resemble the Bluenoroff samples produced by the Lazarus group."

- Kaspersky's technical report

Such false accusation caused by the difficult nature of the cyber domain could systematically force the North Korean leadership into activating the first scenario of the aforementioned 'Most Likely Trajectory' – an execution of attack on critical infrastructure would directly lead to escalation of tension rapidly and uncontrollably for either states. North Korean elites have structured their society in a way that leaves them with limited response decision choices in exchange for continuation of power stability –such dynamics can be extended to the cyber domain and should be considered as the most dangerous trajectory possible.

Undermining Kim Jung-Un's leadership within North Korea would also be a personal red line for Kim Jung-Un. Although seemingly unassociated with cyber, impossible cases such as the U.S. pressuring Kim Jung-Un via enabling free flow of information for the mass population would be detrimental to sustainability and safety of the regime. According to Kim Heung Kwang, who defected after majoring in computer science at Kimceck Industrial College in North Korea, the DPRK's intranet is fully compatible with the worldwide internet. Kim Jung-Un, however, does not allow landlines to be connected.[429] If in any highly improbable case where North Korea is enabled access to the current Western internet, the free flow of information would render Kim Jung-Un to retaliate via triggering the aforementioned malware in U.S. critical infrastructure.

[429] Jung Yong, "North Korean Internet, Up to Kimg Jung-Un's mind", Radio Free Asia, https://www.rfa.org/korean/weekly_program/bd81d55c-itc640-acfcd559ae30c220/fe-jy-030820181723 46.html

INFORMING U.S. CYBER STRATEGY

Cyber has been proven to be an efficient tool to clandestinely reach out and accomplish financially motivated state campaigns while at the same time not escalating the tensions uncontrollably. Past reactions by WannaCry victim Sony, successful hacking of SWIFT system, and the hacking of Japanese cryptocurrency exchanges have directly benefited North Korea financially and incentivized the regime to continue the activities.

North Korea's key decision makers have anticipated and confirmed that cyber offers high utility in pursuing larger policy goals[430] and further even more aggressive cyber activities seem highly probable. More hackers having been assigned to money raising operations rather than intelligence collection, signals that North Korean policy makers are concentrating cyber capabilities to counter geopolitical pressure including economic sanctions from US, Japan, and South Korea.[431]

For U.S. Cyber Command, drawing a clear online red line seems imperative as the nature of the DPRK's cyber operations render it nearly impractical to tackle via counter cyberattack. Because most cyber campaigns are either political or economically driven with the end goal being meeting objectives of the state, a potential solution to dampening cyber activities can be directly negotiating with key policymaking elites of North Korea.

The DPRK will continue to be far less vulnerable to cyber-retaliation while their cyber offensive capabilities have been tailor-made under 'supreme teachings' of Kim Jung-Il and Kim Jung-Un. That, coupled with the reality that North Korean cyber operations are carried out clandestinely in third-party nations makes the situation seem as if fighting against a 'ghost': the ghost can't be hunted or hurt but it can hurt you.

Such operational characteristics originate from North Korean cyber being founded by the RGB, where extreme and critical campaigns, such as presidential assassination or airplane bombings,

[430] James Andrew Lewis, "The Likelihood of North Korean Cyber Attacks.", September 7, 2017, Center for Strategic and International Studies Commentary.
[431] StrategyPage, "Information Warfare: Cyber War Slaves Serve The Mighty Kim.", March 11, 2018, StrategyWorld.com.

are masterminded and executed. As much as the DPRK's brinkmanship regarding nuclear threats seems crazy but actually are rational and highly calculated, RGB's cyber offensive will be as extreme and well-thought out with the end goal being undermining, misinforming, and disadvantaging the 'American imperialists.' This implies that the U.S. must also be as comprehensive in their approach to cyber defense as DPRK's cyber offensive is. Undermining, misinforming, and disadvantaging the U.S. involves targeting not only mass population and private companies, but also targeting specific individuals that may be advantageous to leverage against the U.S. government entities such as Cyber Command or high rank officials of private financial firms. Such comprehensive and combined (kinetic and cyber) offensives by DPRK will require more private-public collaboration, as well as higher awareness from those in leadership positions to address effectively.

Personal disposition of the dictator will be manifested in cyber as his 'expressed will' would be directly reflected into cyber offensive policies with minimum filter from the policymaking elites. Not only that, due to distinct power structure of the totalitarian regime, Kim Jung-Un's order to execute a full scale cyberattack to critical infrastructure can materialize into executed code in a matter of minutes.

Recommended Areas for Future Research

Kim Il-Sung, Kim Jung-Il, and Kim Jung-Un's speeches and texts are considered as 'supreme teaching' and serve as the legal basis of policy making. Their words are carefully curated, and content of the Kim's voices are buttressed by systematic idolization via symbols and portraits that are installed in every town, and every home. Intentional eradication of religion by the Party played a great role in idolization of the Kim family and carefully chosen vocabularies for propagandas allowed not only consolidation of power, but also the words of Kim Jung-Un to effectively serve as the law within North Korea. Authoritative 'teachings' and speeches by the North Korean leaders, carries skewed weight of importance in understanding the legal affairs of North Korea.

Taking into consideration the skewed weight of importance of the DPRK leadership's public statements, it is recommended that U.S. Cyber Command set up an automated process that

allows comprehensive understanding of what the DPRK leadership states. For instance, according to a natural language processing analysis paper by members of the Seoul National University using advancement in machine learning, 69 of the DPRK's new year statements consist of only 18 topics and the specific topics' importance rises and falls according to the North Korean government's policymaking environment, which takes into consideration domestic and foreign affairs of the state.[432]

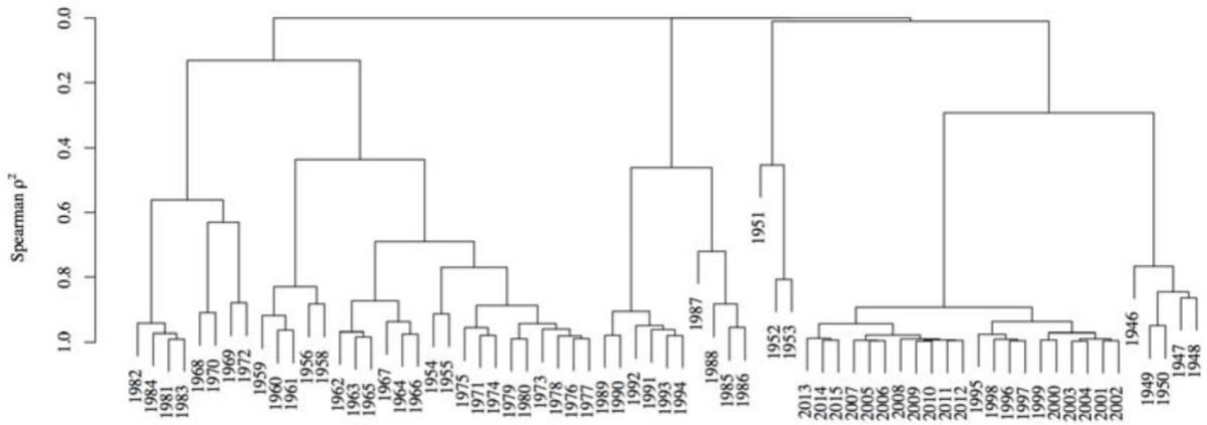


Fig. 6- New Year Address clustering structure diagram via correlation coefficient analysis: Cluster analysis diagram shows significance in DPRK regime-level political changes.

- Left to the center of the diagram represents low level of changes (during the Kim Il-Sung regime);
- The spike in the middle of the diagram in 1951 to 1953 represents the Korean War;
- The right side of the diagram from 2013 to 2002 represents Kim Jung-Il to Kim Jung-Un regime; and
- Far right cluster from 1946 to 1950 represents immediately before the outbreak of the Korean war.

According to the authors, specific key word appearance in the 'New Year Address' had high correlation with changes in the DPRK state level, such as the outbreak of the Korea war, rise of Kim Il-Sung regime, the USS Pueblo incident, and nuclear development and atomic audit issues,

[432] Jong Hee Park, Park Eunjeong, Jo, Dong-Joon. "Text Analysis of North Korean New Year Addresses, 1946 - 2015)". Seoul National University.

rise of Kim Jung-Il, and rise of Kim Jung-Un. These show that New Year Addresses reflect political changes in respect to DPRK.

Caveat acknowledged by the researchers is that the New Year Address is more about informing on how the DPRK leadership 'feels' about the past and present –and that users of such analysis must take caution in futures analysis. It is recommended that in order to accurately predict the DPRK leadership's intents imbedded in the New Year Address documents, the analysts must take into consideration 1) the DPRK's official stances; 2) Chosun central news; and 3) Labor News, and place the New Year Address as the centerpiece of the comprehensive analysis.

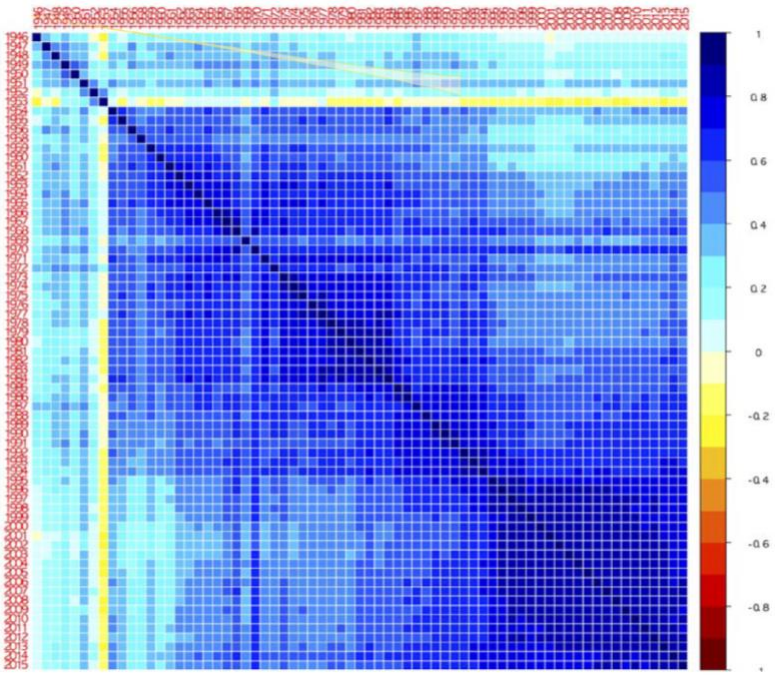


Fig. 7- Pearson correlation amongst North Korean Leadership's New Year Addresses from 1946 to 2015: Text analysis using Pearson correlation in 69 New Year Address Statements and 6,415 morpheme words (Smallest grammatical unit of a language meaning it is the smallest meaningful unit of a language.) mentioned in the addresses by DPRK's Leaders.

According to key terminology frequency and meanings attribution analysis to three key vocabularies mentioned in the DPRK leadership's New Year Addresses: 1) American (미제), 2) Southern Chosun (남조선 Republic of Korea), and 3) Nuclear (핵) contents of New Year Address documents are closely correlated to the DPRK foreign policies towards the U.S. and South Korea as well as towards the nuclear affair. This allows inference of how the DPRK leadership 'feels'

towards the issues. In relation to cyber, automated analysis like this can reveal how the DPRK leadership 'feels' towards state affairs that are seemingly unrelated to cyber but acts reciprocally in the cyber domain.

Extending upon the emphasis on importance of understanding the leader of North Korea -in order to decompose the cyber issue, future research can be structured around parsing Kim Jung-Un's public speeches, publication and track changes in the dictators thought over time, and in association with cyber incidents. Along with further research on domestic cyber defense capabilities, especially on electricity grid and implementation of smart cities, such research efforts can allow decision makers to concentrate limited cyber assets to actionable programs against potential North Korean cyber intrusion if the most dangerous scenario occurs.

COMMON THEMES AND GENERAL IMPLICATIONS FOR THE U.S.

This report conducted deep analysis on China, Russia, Iran, and North Korea delving into their strategic culture, how they understand the cyber domain, and projecting what their most likely and most dangerous futures will look like. Each case study produced distinct findings, but common elements within each were present. Imbedded within all four state's strategic culture is the dominating influence of an authoritative leader, animosity towards the West, and a strong patriotic/nationalistic response to perceived slights. Throughout the course of this project, the paramount element that manifested amongst each is the use of the cyber domain as an equalizer in the following four areas.

1. All four states analyzed in this report desire prestige or relevance on the international stage, and have developed Cyberwarfare strategies around achieving this objective;
2. For each of the cases, the understanding of the cyber domain is coupled with the state's understanding of Information Warfare (IW);
3. All four cases share the desire for sustaining their regimes; and
4. For each of the cases in this report, cyber capabilities have become an extension of their asymmetric warfare capability. Of particular importance is their use of proxies and the civil sector for achieving this means.

Within this mindset of equalization, the control over information is an integral part of all four state's cyberwarfare strategies, both domestically (defense) and internationally (offense). The cyber domain is being used to further drive animosity for the West amongst its citizens and has enhanced all four nation's ability to conduct military operations as a means to project power for coercion, while still remaining just short of the threshold for military response. These states see the cyber domain as a vail of deniability for actions that might evoke negative repercussions against them.

Capitalizing on cyber's plausible deniability, China, Russia, Iran, and North Korea are able to employ non-state actors and proxies as legitimate conductors of operations that would normally evoke a response from the United States, while still claiming to adhere to international laws and norms. So far, offensive cyber operations have coincided with perceived national slights.

By obfuscating the motivations behind these cyberattacks, each state has been able to claim that patriotic hackers conducted these operations without any government or military coordination. Stemming from each state's authoritative regime is the concept of cyber war being integrated into their concept of total war. This integration is most clearly seen when looking at Russia's hybrid warfare operations, where cyber was used as a precursor to kinetic operations. By centering their cyberwarfare strategies around the idea of total war, these states have created a consistently effective asymmetric mechanism to undermine the U.S. and its Western allies. Weaponizing the cyber domain has created a means for all four states to gain information advantages over adversaries, while still maintaining plausible deniability.

By developing their cyber capabilities along with advanced technologies, each state has been able to lessen its dependence on the West and establish itself as a model for states wishing to do the same. Their use of the cyber domain as a means to gain advantages over countries with superior military capabilities is evident from their attempts to achieve information dominance in industrial sectors, critical infrastructure, and intelligence agencies. Offensive cyber operations attributed to these states have been geared towards intelligence gathering, disruption, and industrial intellectual property theft. As these operations have traditionally fallen under accepted espionage behavior, the response options to these incidents remains limited. By employing the cyber domain in such an asymmetric manner China, Russia, Iran, and North Korea, have avoided military pressure, accelerated their economic advancement, and enhanced their ability to develop and deploy new military capabilities, both conventional and in cyber.

Based on these common themes we recommend three areas for which U.S. Cyber Command needs to be aware:

1. When predicting the future cyber behavior of these four states, accounting for their acute sensitivity to regime stability is paramount. Any activity conducted by the U.S. that might be perceived as disruptive to these regimes, such as the U.S. continuing to pull economic levers as a means to influence these four nations, there is a high likelihood they will respond via the cyber domain. This response may present itself as an offensive operation or in a defensive information control operation. As there are already questions

around whether the 2015 cyber agreement between the U.S. and China has actually had any impact on Chinese economic cyberattacks, the current trade war could easily push China to resume these industrial espionage operations. If the recent comments around the Iran nuclear deal are perceived by the Iranian regime as legitimate threats that will lead to newly imposed sanctions, Iran may retaliate with cyberattacks against economic targets associated with the U.S. Our earlier analysis of Iran has illustrated this vindictive behavior is well within the realm of possibility for Iran. North Korea has been able to offset some of the financial effects of economic sanctions imposed on them through cyber operations. Economic cyber activity will continue and potentially expand for North Korea especially as tensions with the U.S. rise. Over the past ten years, Russia has ramped up its use of offensive cyberattacks and has become embolden in its targets, as seen in the recent Democratic National Convention (DNC) hack and election meddling. As relations between the U.S. and Russia continue to deteriorate and the effects of newly imposed sanctions are felt by Russia, the likelihood of them resorting to a cyber response is extremely high.

2. Defending against operations conducted by these states will continue to be a challenge for Cyber Command because of their willingness to employ the civil sector and proxies in the cyber domain. As illustrated in our analysis, these four states have integrated cyber into all aspects of the state. Because of this asymmetric behavior the U.S. is faced with enemies that are drastically different than itself. These non-state actors provide the adversaries with greater control and flexibility in the domain. Proxies also adhere to their own ideals and motivations, meaning they operate according to different rules. Traditional or excepted norms for state behavior do not apply to these actors. This should be the greatest area of concern for United States Cyber Command. This plays an important role in assessing threats to America's critical infrastructure because of the pervasive Russian presence. China also seems to have started shifting focus from intellectual property theft to a more highly precise offensive targeting of critical infrastructure. In addition to the threat posed by Russia and China, Cyber Command

must be on the look out for Iranian and North Korean threats to critical infrastructure as well. Due to the lack of ICT infrastructure, threats posed from these two states is of particular importance. Since both states are relatively insulated from a U.S. cyber response, they perceive themselves as having a low level of vulnerability in this domain.

3. Preparation for continued contention over the cyber domain must take into account the potential second and third order effects of peripheral diplomatic and military incidents spilling over into the cyber domain. The recent kinetic action against the Assad regime by the United States and its allies has real potential to cause cyber actors sympathetic to the regime to retaliate against the United States, Israel, or Western interests. We cannot rule out the possibility that Russia or Iran would use their cyber capabilities to attack the United States in retaliation for the recent missile deployment in Syria. The cyber domain offers opportunity for any of the four states evaluated in this report to capitalize on this or some future incident to once again hide behind a proxy to attack the United States with little blowback on itself. As spill over incidents continue to rise, the cyber repercussions to future operations will have to be a considered before they are conducted.

BIBLIOGRAPHY

APPROACH AND METHODOLOGY

George, Alexander L. and Andrew Bennett, *Case Studies and Theory Development in the Social Sciences*, MIT Press (United States, 2005)

Gerring, John, "The Case Study: What It Is and What It Does," in Carles Boix and Susan C. Stokes, *The Oxford Handbook of Comparative Politics*, Oxford University Press (United Kingdom, 2009)

Johnston, Alastair I., "Thinking About Strategic Culture," *International Security*, Vol. 19, No. 4 (Spring, 1995), pp. 32-64, available at: https://www.jstor.org/stable/2539119?seq=1#page_scan_tab_contents (last consulted: January 2018)

Snyder, Jack L., "The Soviet Strategic Culture: Implications for Limited Nuclear Operations," Rand (United States, 1977), available at: https://www.rand.org/content/dam/rand/pubs/reports/2005/R2154.pdf (last consulted: January 2018)

CASES

CHINA

"Advanced Persistent Threat Groups." FireEye, 2018. https://www.fireeye.com/current threats/apt-groups.html.

Albert, Eleanor. "China-Taiwan Relations." Council on Foreign Relations (blog), December 7, 2016. https://www.cfr.org/backgrounder/china-taiwan-relations.

"APT 1: Exposing One of China's Cyber Espionage Units." MANDIANT, 2013. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

Carvalho, Raquel. "Cyberattackers Hack Website of Hong Kong Pro-Democracy Party Demosisto." South China Morning Post, September 9, 2017. http://www.scmp.com/news/hong-kong/law-crime/article/2110477/cyberattackers-hack-website-hong-kong-pro-democracy-party.

Cassella, Megan. "China to Slap Tariffs on 128 U.S. Goods." POLITICO (blog), April 1, 2018. https://politi.co/2pVQj9L.

Chen, Titus C. "China's Reaction to the Color Revolutions: Adaptive Authoritarianism in Full Swing." Asian Perspective 34, no. 2 (2010): 5–51.

Cheng, Dean. "Winning Without Fighting: Chinese Public Opinion Warfare and the Need for a Robust American Response." Backgrounder. Washington, DC: The Heritage Foundation, November 26, 2012. /global-politics/report/winning-without-fighting-the-chinese-psychological-warfare-challenge.

———. "Winning Without Fighting: The Chinese Psychological Warfare Challenge." Backgrounder. Washington, DC: The Heritage Foundation, April 11, 2013. /global-politics/report/winning-without-fighting-the-chinese-psychological-warfare-challenge.

"China." 500 miles. United States: Google, ORION-ME, SK Telecom, ZENDRIN, 2018. https://www.google.com/maps/place/China/@27.8781788,87.199404,4z/data=!4m5!3m4!1s0x31508e64e5c642c1:0x951daa7c349f366f!8m2!3d35.86166!4d104.195397.

Cho, Yoonyoung, and Jongpil Chung. "Bring the State Back In: Conflict and Cooperation Among States in Cybersecurity." Pacific Focus 32, no. 2 (August 1, 2017): 290–314. https://doi.org/10.1111/pafo.12096.

Clover, Charles. "Xi's China: Command and Control." Financial Times (blog), July 26, 2016. https://www.ft.com/content/dde0af68-4db2-11e6-88c5-db83e98a590a.

Delaney, Robert. "US Urged to Act Immediately to Save Its Systems from the 'Growing Threat of Chinese Cyber Theft.'" South China Morning Post, April 20, 2018.

http://www.scmp.com/news/china/article/2142513/us-urged-act-immediately-save-its-systems-growing-threat-chinese-cyber.

Denning, Dorothy. "Cyberwarriors." HIR: Harvard International Review, May 6, 2006. http://hir.harvard.edu/article/?a=905.

DeVore, Marc R., and Lee Sangho. "APT(Advanced Persistent Threat)s and Influence: Cyber Weapons and the Changing Calculus of Conflict." The Journal of East Asian Affairs; Seoul 31, no. 1 (Spring/Summer 2017): 39–64.

Economy, Elizabeth C. "Beijing's Silk Road Goes Digital." Council on Foreign Relations (blog), June 6, 2017. https://www.cfr.org/blog/beijings-silk-road-goes-digital.

Erie, Matthew. "Sovereignty, Internationalism, and the Chinese In-Between." East-West Center, International Graduate Student Conference Series, February 19, 2004, 1–19.

Ford, Christopher A. An Interview with Christopher A. Ford. Interview by Mengjia Wan, November 1, 2016. http://www.nbr.org/research/activity.aspx?id=718.

Godwin, Paul H.B., and Alice L. Miller. "China's Forbearance Has Limits: Chinese Threat and Retaliation Signaling and Its Implications for a Sino-American Military Confrontation." Edited by Phillip C. Saunders. Institute for National Strategic Studies: National Defense University Press, China Strategic Perspectives, April 2013.

Greenberg, Andy. "China's Golden Cyber-Shield." Forbes, July 31, 2007. https://www.forbes.com/2007/07/30/china-cybercrime-war-tech-cx_ag_0730internet.html#64b45e3f483c.

Griffiths, James. "How China Used the US Bombing of Its Belgrade Embassy to Win a PR Victory." Public Radio International, May 5, 2014. https://www.pri.org/stories/2014-05-05/how-china-used-us-bombing-its-belgrade-embassy-win-pr-victory.

Han, Rongbin. "Manufacturing Consent in Cyberspace: China's 'Fifty-Cent Army.'" Journal of Current Chinese Affairs 44, no. 2 (June 29, 2015): 105–34.

———. "The 'Voluntary Fifty-Cent Army' in Chinese Cyberspace." China Policy Institute: Analysis (blog), February 29, 2016. https://cpianalysis.org/2016/02/29/the-voluntary-fifty-cent-army-in-chinese-cyberspace/.

Healey, Jason. "Beyond Attribution: Seeking National Responsibility in Cyberspace." Cyber Statecraft Initiative: Atlantic Council, February 22, 2012. http://www.atlanticcouncil.org/publications/issue-briefs/beyond-attribution-seeking-national-responsibility-in-cyberspace.

———. Discussion on Cyberspace Analogies and Strategic Culture. In Person Interview Conducted At: Columbia University School of International and Public Affairs (SIPA), March 26, 2018.

———. "Dynamics of Cyber Conflict Class 7." presented at the Dynamics of Cyber Conflict Course, Columbia University School of International and Public Affairs, March 5, 2018.

Hess, Pamela. "China Prevented Repeat Cyber Attack on US." UPI, October 29, 2002. https://www.upi.com/China-prevented-repeat-cyber-attack-on-US/51011035913195/.

Hienz, Justin. "Chinese Cyber Attacks Are Looting U.S. Private Sector." Defense Media Network (blog), June 26, 2012. https://www.defensemedianetwork.com/stories/chinese-cyber-attacks-are-looting-u-s-private-sector/.

Hjortdal, Magnus. "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence." Journal of Strategic Security 4, no. 2 (Summer 2011): 1–24.

Hvistendahl, Mara. "Hackers: The China Syndrome." Popular Science, April 23, 2009. https://www.popsci.com/scitech/article/2009-04/hackers-china-syndrome.

Iasiello, Emilio. "China's Cyber Initiatives Counter International Pressure." Journal of Strategic Security 10, no. 1 (2017): 1–16. https://doi.org/10.5038/1944-0472.10.1.1548.

———. "China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities." Journal of Strategic Security 9, no. 2 (Summer 2016): 45–69.

Johnson, Colonel Kenneth D. China's Strategic Culture: A Perspective for the United States. Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2009. https://permanent.access.gpo.gov/websites/ssi.armywarcollege.edu/pubs/display.cfm-pubID=924.htm.

Johnston, Alastair I. Cultural Realism: Strategic Culture and Grand Strategy in Chinese History. Princeton, N.J.: Princeton University Press, 1995.

Jones, Bruce. "Containment, Competition, and Cooperation in US-China Relations." Edited by Ryan Hass, Tarun Chhabra, and Bruce Jones. Brookings Institution, November 21, 2017. https://www.brookings.edu/wp-content/uploads/2017/11/fp_20171121_china_interview.pdf.

Kania, Elsa. "Careful What You Wish For - Change and Continuity in China's Cyber Threats." Real Clear Defense (blog), April 5, 2018. https://www.realcleardefense.com/articles/2018/04/05/careful_what_you_wish_forchange_and_continuity_in_chinas_cyber_threats_113284.html.

Kania, Elsa B. "Cyber Deterrence in Times of Cyber Anarchy - Evaluating the Divergences in U.S. and Chinese Strategic Thinking." In 2016 International Conference on Cyber Conflict (CyCon U.S.), 1–17. Washington D.C.: IEEE, 2016. https://doi.org/10.1109/CYCONUS.2016.7836619.

Kanuck, Sean. Discussion on Strategic Goals of China, North Korea, Russian, and Iran in Cyberspace. Phone Interview Conducted At: Columbia University School of International and Public Affairs (SIPA), March 26, 2018.

Killalea, Debra. "China's 30-Year Deadline to Rule the World." News.com.au, October 20, 1017. http://www.news.com.au/finance/work/leaders/chinas-30year-deadline-to-rule-the-world/news-story/70f62a5bc0e4580b83d5ca89a2479e94.

Kim, Sam. "China Hacks U.S. Firms for Financial Information, FireEye Says." Bloomberg.Com, April 4, 2018, sec. Politics. https://www.bloomberg.com/news/articles/2018-04-04/china-hacks-u-s-firms-for-financial-information-fireeye-says.

Kiselycznyk, Michael. "Civil-Military Relations in China: Assessing the PLA's Role in Elite Politics." Edited by Phillip C. Saunders. Institute for National Strategic Studies: National Defense University Press, 2010. https://permanent.access.gpo.gov/gpo16358/ChinaPerspectives-2.pdf.

Klein, Samuel. "Beyond Capabilities: Investigating China's Military Strategy and Objectives in Cyberspace." The Cyber Defense Review, December 3, 2016. http://cyberdefensereview.army.mil/The-Journal/Article-Display/Article/1136045/beyond-capabilities-investigating-chinas-military-strategy-and-objectives-in-cy/.

Knake, Robert K. "A Cyberattack on the U.S. Power Grid." Council on Foreign Relations, April 3, 2017. https://www.cfr.org/report/cyberattack-us-power-grid.

Knake, Robert, and Adam Segal. "How the Next U.S. President Can Contain China in Cyberspace." Journal of International Affairs; New York 70, no. 1 (Winter 2016): 21–28.

Koerner, Brendan. "Inside the OPM Hack, the Cyberattack That Shocked the US Government." WIRED (blog), October 23, 2016. https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

Lai, David. Learning from the Stones [Electronic Resource]: A GO Approach to Mastering China's Strategic Concept, Shi. Carlisle, PA: Army War College, Strategic Studies Institute, 2004. https://permanent.access.gpo.gov/lps51974/LPS51974.pdf.

Lampe, Evan. "Cultural History of Reading." In Modern China, edited by Gabrielle Watling, 1:305–23. Westport, CT: Greenwood Press, 2008. http://go.galegroup.com.ezproxy.cul.columbia.edu/ps/i.do?p=GVRL&u=columbiau&id=GALE%7CCX2441100023&v=2.1&it=r&sid=summon&authCount=1.

Lee, Sangkuk. "China's 'Three Warfares': Origins, Applications, and Organizations." Journal of Strategic Studies 37, no. 2 (February 23, 2014): 198–221. https://doi.org/10.1080/01402390.2013.870071.

Lewis, James A., and Simon Hansen. "China's Cyberpower: International and Domestic Priorities." Special Report: ASPI. Australia: Australian Strategic Policy Institute, November 2014. https://www.files.ethz.ch/isn/185655/China%27s%20cyberpower_%20international%20and%20domestic%20prioritie.pdf.

Lubman, Stanley. "Mao and Mediation: Politics and Dispute Resolution in Communist China." California Law Review 55, no. 5 (November 1967): 1284–1359. https://doi.org/10.2307/3479330.

Lyall, Nicholas. "China's Cyber Militias: China's Cyber Power Is in the Grip of Dual Trends - Pluralism and Centralization." The Diplomat, March 1, 2018. https://thediplomat.com/2018/03/chinas-cyber-militias/.

Margonelli, Lisa. Oil on the Brain: Adventures from the Pump to the Pipeline. New York: Nan A. Talese/ Doubleday, 2007.

Mark, Emily. "Legalism." Encyclopedia. Ancient History Encyclopedia (blog), January 31, 2016. https://www.ancient.eu/Legalism/.

Maxey, Levi. "China Pivots Its Hackers from Industrial Spies to Cyber Warriors." The Cipher Brief (blog), April 2, 2017. https://www.thecipherbrief.com/china-pivots-its-hackers-from-industrial-spies-to-cyber-warriors.

Nathan, Andrew J. "China's Geography and Security Goals." Columbia University. Asia For Educators, 2009. http://afe.easia.columbia.edu/special/china_1950_china_geosec.htm#internal.

Osborne, Charlie. "China Reveals Existence of Cyber Warfare Hacking Teams." ZDNet (blog), March 20, 2015. http://www.zdnet.com/article/china-reveals-existence-of-cyber-warfare-hacking-teams/.

Pines, Yuri. "Legalism in Chinese Philosophy." In The Stanford Encyclopedia of Philosophy, edited by Edward N. Zalta, Spring 2017. Metaphysics Research Lab, Stanford University, 2017. https://plato.stanford.edu/archives/spr2017/entries/chinese-legalism/.

Ping Li, Peter, and Monsol Young. "How to Approach the Ancient Chinese Wisdom? A Commentary Concerning Sun Tzu's The Art of War." Management and Organizational Review, Dialogue, Debate, and Discussion, 13, no. 4 (December 2017): 913–20. https://doi.org/10.1017/mor.2017.60.

Pollpeter, Kevin. "Part II Military Strategy and Institutions, Chapter 6: Chinese Writings on Cyberwarfare and Coercion." In China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, 32. Oxford University Press, 2015. http://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780190201265.001.0001/acprof-9780190201265-chapter-6.

"PROJECT CAMERASHY: Closing the Aperture on China's Unit 78020." Vienna, VA: Threat Connect and Defense Group Inc (DGI), 2015. https://cdn2.hubspot.net/hubfs/454298/Project_CAMERASHY_ThreatConnect_Copyright_2015.pdf.

Russell, Jon. "China's Web Censors Go into Overdrive as President Xi Jinping Consolidates Power." TechCrunch (blog), February 27, 2018. http://social.techcrunch.com/2018/02/26/chinas-web-censors-go-into-overdrive-as-president-xi-jinping-consolidates-power/.

Saalman, Lora. "Pouring 'New' Wine into New Bottles: China-U.S. Deterrence Relations in Cyberspace." Seton Hall Journal of Diplomacy and International Relations 17, no. 1/2 (2016 2015): 23–35.

Sacks, Samm. "How Will China Retaliate beyond Tariffs?" Center for Strategic & International Studies. Commentary (blog), March 29, 2018. https://www.csis.org/analysis/how-will-china-retaliate-beyond-tariffs.

Segal, Adam. "An Update on U.S.-China Cybersecurity Relations." Council on Foreign Relations (blog), November 17, 2017. https://www.cfr.org/blog/update-us-china-cybersecurity-relations.

———. Discussion on Chinese Strategic Culture and Cyberspace. Phone Interview Conducted, March 28, 2018.

———. "How China Is Preparing for Cyberwar." Christian Science Monitor, March 20, 2017. https://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0320/How-China-is-preparing-for-cyberwar.

"Shanghai Cooperation Organization." Resources. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), July 29, 2014. https://www.ccdcoe.org/sco.

Simcox, Frank W. "Flexible Options for Cyber Deterrence." Research Paper. Maxwell AFB Montgomery AL: Air War College Center For Strategy and Technology, February 11, 2009. http://www.dtic.mil/docs/citations/ADA539892.

Snyder, Jack. Discussion on Strategic Culture. In Person Interview Conducted At: Columbia University School of International and Public Affairs (SIPA), March 5, 2018.

"Some Background Notes on Mao Tse-Tung's Philosophy of Force." Office of Research and Analysis. United States Information Agency, October 28, 1960. https://hv.proquest.com/pdfs/103376/103376_002_0925/103376_002_0925_From_1_to_19.pdf.

Stewart, Scott. "Guanxi: How Business Is Done in China." Stratfor: Worldview, April 27, 2017. https://worldview.stratfor.com/article/guanxi-how-business-done-china.

Stokes, Mark A., Jenny Lin, and L.C. Russell Hsiao. "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure." Project 2049, November 11, 2011. https://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf.

Sun, Bin, and Lionel Giles. Sun Tzu on the Art of War: The Oldest Military Treatise in the World. Champaign, Ill: Project Gutenberg, 2016. https://ezproxy.cul.columbia.edu/login?qurl=https%3a%2f%2fsearch.ebscohost.com%2flogin.aspx%3fdirect%3dtrue%26db%3dnlebk%26AN%3d2011517%26site%3dehost-live%26scope%3dsite.

Thornburgh, Nathan. "The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)." Time Archive: 1923 to the Present, September 5, 2005. http://www.cs.washington.edu/education/courses/csep590/05au/readings/titan.rain.htm.

Tiezzi, Shannon. "China's 'Sovereign Internet.'" The Diplomat, June 24, 2014. https://thediplomat.com/2014/06/chinas-sovereign-internet/.

Trachtman, Joel P. "Integrating Lawfare and Warfare." Boston College International and Comparative Law Review; Newton 39, no. 2 (2016): 267–82.

Tzu, Sun. Sun Tzu On the Art of War,the Oldest Military Treatise in the World,. Translated by Lionel Giles. London: Luzac & Co., 1910. http://hdl.handle.net/2027/uva.x030339883.

Wai-chi, Rodney Chu. "The Dynamics of Cyber China: The Characteristics of Chinese ICT Use." Knowledge, Technology, & Policy 21, no. 1 (March 2008): 29–35. https://doi.org/10.1007/s12130-008-9043-y.

Waldman, Thomas. "Politics and War: Clausewitz's Paradoxical Equation." Parameters; Carlisle Barracks 40, no. 3 (Autumn 2010): 1–13.

Warikoo, Arun. "Cyber Warfare: China's Role and Challenge to the United States." Himalayan and Central Asian Studies; New Delhi 17, no. 3/4 (December 2014): 61–72.

WeiWei, Zhang. "For China's One-Party Rulers, Legitimacy Flows From Prosperity and Competence." Philosophy + Culture Center. Berggruen Institute, March 1, 2017. http://philosophyandculture.berggruen.org/ideas/for-china-s-one-party-rulers-legitimacy-flows-from-prosperity-and-competence.

"What Is Guanxi?" World Learner Chinese. Accessed March 20, 2018. http://www.worldlearnerchinese.com/content/what-guanxi.

Work, JD. Discussion on Chinese, North Korean, and Russian Conduct in Cyberspace. In Person Interview Conducted At: Columbia University School of International and Public Affairs (SIPA), March 19, 2018.

Worrall, Simon. "Why Is Confucius Still Relevant Today? His Sound Bites Hold Up." National Geographic. National Geographic News, March 25, 2015. https://news.nationalgeographic.com/2015/03/150325-confucius-china-asia-philosophy-communist-party-ngbooktalk/.

"Xi Expected to Be Written Into Chinese Constitution." Bloomberg News, January 19, 2018. https://www.bloomberg.com/news/articles/2018-01-19/xi-jinping-thought-to-be-written-into-chinese-constitution.

Zeng, Jinghan, Tim Stevens, and Yaru Chen. "China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty.'" Politics & Policy 45, no. 3 (June 1, 2017): 432–64. https://doi.org/10.1111/polp.12202.

Zetter, Kim. "Google Hack Attack Was Ultra Sophisticated, New Details Show." WIRED, January 14, 2010. https://www.wired.com/2010/01/operation-aurora/.

RUSSIA

Aelkus. "The Risks of Underpromising Cyberpower." Essays. Accessed March 15, 2018. http://aelkus.github.io/essays/cyberpower.html.

Ambrosio, Thomas, Challenging America's global preeminence: Russia's quest for multipolarity. Taylor & Francis, 2017.

Astakhova, L. V. ,"The concept of the information-security culture." Scientific and Technical Information Processing 41.1 (2014): 22-28.

Ash, Lucy, "How Russia outfoxes its enemies." BBC News. January 29, 2015. Accessed March 13, 2018. http://www.bbc.com/news/magazine-31020283.

Bacon, John, "Russia Bars Navalny Presidential Bid." Accessed March 14, 2018. https://uw-media.usatoday.com/video/embed/108918976?sitelabel=reimagine&continuousplay=true&placement=uw-smallarticleattophtml5&pagetype=story.

Barkan, Elliott Robert, ed. Immigrants in American history: Arrival, adaptation, and integration. Vol. 1. ABC-CLIO, 2013.

BBC News, "Timeline: Chechnya," BBC News, January 19, 2011. http://news.bbc.co.uk/2/hi/asia-pacific/country_profiles/2357267.stm.

Bumiller, Jason and Thom Shanker. "Panetta Warns of Dire Threat of Cyberattack on U.S." The New York Times, October 11, 2012, sec. World. https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

Butcher, Clifford F. "Port Arthur was "the Pearl Harbor of 1904"." The Milwaukee Journal, January 19, 1942. Accessed March 14, 2018. https://news.google.com/newspapers?nid=1499&dat=19420119&id=-e4ZAAAAIBAJ&sjid=8SIEAAAAIBAJ&pg=4412,1516787.

Central Intelligence Agency. "The World Factbook: RUSSIA." Library. March 27, 2018. Accessed April 02, 2018. https://www.cia.gov/library/publications/the-world-factbook/geos/rs.html.

Connell, Michael and Sarah Vogler. Russia's Approach to Cyber Warfare. Center for Naval Analyses Arlington United States, 2017.

Crowell, Steven, "Existentialism", The Stanford Encyclopedia of Philosophy (Winter 2017 Edition), Edward N. Zalta (ed.), URL = <https://plato.stanford.edu/archives/win2017/entries/existentialism/>.

Department of Homeland Security and Federal Bureau of Investigation. "GRIZZLY STEPPE – Russian Malicious Cyber Activity." NCCIC Publications. December 29, 2016. Accessed March 21, 2018. https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY STEPPE-2016-1229.pdf.

Department Of State. The Office of Electronic Information, Bureau of Public Affairs. "United States Relations with Russia: After the Cold War," June 4, 2007. https://2001-2009.state.gov/r/pa/ho/pubs/fs/85962.htm.

Detsch, Jack, "How Russia and Others Use Cybercriminals as Proxies." Christian Science Monitor, June 28, 2017. https://www.csmonitor.com/USA/2017/0628/How-Russia-and-others-use-cybercriminals-as-proxies.

Dunning, Chester SL., Russia's First Civil War: The Time of Troubles and the Founding of the Romanov Dynasty. Penn State Press, 2010.

Editors of the Encyclopedia Britannica, "Russo-Japanese War | Causes, Summary, Map, & Significance." Encyclopedia Britannica. Accessed March 14, 2018. https://www.britannica.com/event/Russo-Japanese-War.

Eko, Lyombe S., New media, old regimes: case studies in comparative communication law and policy. Lexington Books, 2012.

Epstein, Mikhail, "The phoenix of philosophy. On the meaning and significance of contemporary Russian thought." Symposion: A Journal of Russian Thought 1 (1996): 35-74. <http://www.emory.edu/INTELNET/rus_thought_overview.html>

Etling, Bruce, Karina Alexanyan, John Kelly, Robert Faris, John G. Palfrey, and Urs Gasser. "Public discourse in the Russian blogosphere: Mapping RuNet politics and mobilization." (2010).

Evtuhov, Catherine. The cross & the sickle: Sergei Bulgakov and the fate of Russian religious philosophy. Cornell University Press, 1997.

Flook, Kara, "Russia and the Cyber Threat." Critical Threats. Accessed March 14, 2018. https://www.criticalthreats.org/analysis/russia-and-the-cyber-threat.

Friedman, Thomas, "Opinion | Is Putin a C.I.A. Agent?" The New York Times, sec. Opinion. Accessed April 3, 2018. https://www.nytimes.com/2018/04/03/opinion/putin-cia-weakening-russia.html.

Galeotti, Mark, "Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'?." Small Wars & Insurgencies 27, no. 2 (2016): 282-301.

Galeotti, Mark, "I'm Sorry for Creating the 'Gerasimov Doctrine'." Foreign Policy. March 05, 2018. Accessed March 13, 2018. http://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/.

Galeotti, Mark. "The 'Gerasimov Doctrine' and Russian Non-Linear War." In Moscow's Shadows. September 17, 2017. Accessed April 03, 2018. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

Galeotti, Mark, "Putin's Secret Weapon." Foreign Policy. Accessed March 14, 2018. https://foreignpolicy.com/2014/07/07/putins-secret-weapon/.

Halperin, Charles J., Russia and the Golden Horde: the Mongol impact on medieval Russian history. Vol. 445. Indiana University Press, 1987.

Hazanov, Alex and Yakov Feygin. "Analysis | Russia Hacked Our Election Because the Spies Took Over." Washington Post, August 2, 2017, sec. Made by History Analysis Analysis Interpretation of the news based on evidence, including data, as well as anticipating how events might unfold based on past events. https://www.washingtonpost.com/news/made-by-history/wp/2017/08/02/russia-hacked-our-election-because-the-spies-took-over/.

Healey, Jason, "Preparing for Cyber 9/12." Atlantic Council. Accessed March 14, 2018. http://www.atlanticcouncil.org/publications/issue-briefs/preparing-for-cyber-9-12.

Hendley, Kathryn. "Who are the legal nihilists in Russia?." Post-Soviet Affairs 28, no. 2 (2012): 149-186.

Herd, Graeme P. "The Russo-Chechen Information Warfare and 9/11: Al- Qaeda through the South Caucasus Looking Glass?" European Security 11, no. 4 (Winter, 2002).

Heickerö, Roland, Emerging cyber threats and Russian views on Information warfare and Information operations. Defence Analysis, Swedish Defence Research Agency (FOI), 2010.

Hill, Fiona, "The Real Reason Putin Supports Assad," Foreign Affairs, March 25, 2013

Hooker, Richard D., Charting a course: Strategic choices for a new administration. Chapter 11: Russia, Government Printing Office, 2017.

Hromadske International,. "Donbass: Europe's Latest Frozen Conflict." Hromadske International, November 14, 2014. https://medium.com/@Hromadske/donbass-europes-latest-frozen-conflict-38e91aedb4a9.

Interview with Jason Healey, March 26th, 2018, 3:00-3:40 PM, Room 1337, International Affairs Building, Columbia University School of International and Public Affairs.

Interview with Sean Kanuck, March 27th, 2018, 3:00-3:35 PM, Room 1510, International Affairs Building, Columbia University School of International and Public Affairs.

Interview with Jack Snyder, Ph.D., March 5th, 2018, 6:10-8:00 PM, Room 501A, International Affairs Building, Columbia University School of International and Public Affairs.

Interview with Adam Segal, Ph.D, March 28th, 2018, 3:00-3:30 PM, Room 1336, International Affairs Building, Columbia University School of International and Public Affairs.

Interview with Joshua D. Work, March 19th, 2018, 8:00-9:00 AM, Lehman 1, Lehman Social Science Library, International Affairs Building, Columbia University School of International and Public Affairs.

Isserson, Georgi Samoilovich. The Evolution of Operational Art. Translated by Bruce W. Meaning. 1930 ed. Fort Leavenworth, KS: Combat Studies Institute Press, 2013. Accessed March 13, 2018. http://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/OperationalArt.pdf

Joffe, Josef, "The First Totalitarian." The New York Times, October 19, 2017, sec. Book Review. https://www.nytimes.com/2017/10/19/books/review/victor-sebestyen-lenin-biography.html.

Joseph-Grant, Henry, "Russia's Top Religious Official Sprays Holy Water on Computers to Prevent Cyber Attacks – Irish Tech News." Accessed May 2, 2018. https://irishtechnews.ie/russias-top-religious-official-sprays-holy-water-on-computers-to-prevent-cyber-attacks/.

Khodorkovsky, Mikhail, "Opinion | A Problem Much Bigger Than Putin." The New York Times, September 12, 2017, sec. Opinion. https://www.nytimes.com/2017/09/12/opinion/putin-russia-mikhail-khodorkovsky.html.

Kmita, Ewelina, "Jak Przekonać Naród? Propagandowa Wielka Wojna Ojczyźniana - Histmag.Org." Accessed March 21, 2018. https://histmag.org/Jak-przekonac-narod-Propagandowa-Wielka-Wojna-Ojczyzniana-16049.

Lafleur, Thomas M., Mikhail Frunze and the unified military doctrine. ARMY COMMAND AND GENERAL STAFF COLL FORT LEAVENWORTH KS, 2004. < http://www.dtic.mil/get-tr-doc/pdf?AD=ADA429032>, pp. 1-114

Lewitter, L. R.,"Peter the Great, Poland, and the Westernization of Russia." Journal of the History of Ideas 19, no. 4 (1958): 493-506. doi:10.2307/2707919.

Luchenko, Ksenia, "Why Do the Russians Trust the Church Set up by the KGB? | Opinion." Newsweek, February 10, 2018. http://www.newsweek.com/why-do-russians-trust-church-set-kgb-802635.

Ludwig, Gerd. "Why Many Young Russians See a Hero in Putin." Magazine, November 8, 2016. https://www.nationalgeographic.com/magazine/2016/12/putin-generation-russia-soviet-union/.

Malukov, Alexander. "Raffi Aslanbekov." Physiognomy of the Russian Internet. 2013. Accessed March 15, 2018. https://translate.google.com/translate?sl=auto&tl=en&js=y&prev=_t&hl=en&ie=UTF-8&u=http://ezhe.ru/fri/30/&edit-text=&act=url.

Matthews, Owen, "From Russia With Malware." Newsweek. March 28, 2016. Accessed March 13, 2018. http://www.newsweek.com/2015/05/15/russias-greatest-weapon-may-be-its-hackers-328864.html.

McClintock, Bruce, "Russian Information Warfare: A Reality That Needs a Response," RAND Corporation, July 21, 2017. https://www.rand.org/blog/2017/07/russian-information-warfare-a-reality-that-needs-a.html.

Migacheva, Katya and Bryan Frederick, eds., Religion, Conflict, and Stability in the Former Soviet Union. Santa Monica, CA: RAND Corporation, 2018. https://www.rand.org/pubs/research_reports/RR2195.html.

Ministry of Defense, Russian Federation, "Doctrine of Information Security of the Russian Federation." Accessed March 13, 2018.

http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.

NATO Review. "Russian intelligence is at (political) war." NATO Review. Accessed March 13, 2018. http://www.nato.int/docu/review/2017/Also-in-2017/russian-intelligence-political-war-security/EN/index.htm.

opennet.net, "Internet Censorship Listed: How Does Each Country Compare?" the Guardian, April 16, 2012. http://www.theguardian.com/technology/datablog/2012/apr/16/internet-censorship-country-list.

Orlov, Alexander. "The Theory and Practice of Soviet Intelligence." Central Intelligence Agency. August 04, 2011. Accessed March 12, 2018. https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol7no2/html/v07i2a05p_0001.htm.

Paganini, Pierluigi, "Russia Is Going to Pass the New Anti-Terrorism Bill, Many Are Skeptical." Security Affairs, June 30, 2016. http://securityaffairs.co/wordpress/48871/laws-and-regulations/russia-anti-terrorism-bill.html.

Pantsov, Alexander. The Bolsheviks and the Chinese Revolution 1919-1927. Routledge, 2013.

Perkovich, George, and Ariel E. Levite, eds. Understanding Cyber Conflict: Fourteen Analogies. Georgetown University Press, 2017.

Piotrowski, Marcin A., 'Russia's Security Policy', in Janusz Bugajski (ed.), Toward an Understanding of Russia: New European Perspectives (New York: Council on Foreign Relations, 2002).

Radio Free Europe/Radio Liberty, "Twenty Years After: Key Players In Russia's October 1993 Crisis." RadioFreeEurope/RadioLiberty. Accessed March 14, 2018. https://www.rferl.org/a/russia-players-1993-crisis/25125000.html.

Roberts, Geoffrey, Stalin's general: the life of Georgy Zhukov. Random House Incorporated, 2012.

Rohozinski, Rafal, "Mapping Russian cyberspace: Perspectives on democracy and the net.", United Nations Research Institute for Social Development, Discussion Paper No. 115, (1999)

Ruffin, M. Holt. The Post-Soviet Handbook: A Guide to Grassroots Organizations and Internet Resources. University of Washington Press, 2018.

Rumer, Eugene, Roy Godson, Clint Watts, and Kevin Mandia, testimony of, Disinformation: A Primer in Russian Active Measures and Influence Campaigns, 115th Cong., 1-15 (2017) https://www.hsdl.org/?view&did=802222

Savodnik, Peter, "The Secret Source of Putin's Evil." The Hive. January 09, 2017. Accessed March 12, 2018. https://www.vanityfair.com/news/2017/01/the-secret-source-of-putins-evil.

Seiden, Daniel, "Kaspersky Could Allow Russian Spying, U.S. Tells Court." Bloomberg Big Law Business, 6 February 2018, Accessed March 15, 2018. https://biglawbusiness.com/kaspersky-could-allow-russian-spying-u-s-tells-court/.

Shu, Catherine, "Putin passes law that will ban VPNs in Russia." TechCrunch. July 30, 2017. Accessed March 13, 2018. https://techcrunch.com/2017/07/30/putin-passes-law-that-will-ban-vpns-in-russia/.

Soldatov, Andrei, "Putin Has Finally Reincarnated the KGB." Foreign Policy. Accessed March 15, 2018. https://foreignpolicy.com/2016/09/21/putin-has-finally-reincarnated-the-kgb-mgb-fsb-russia/.

Sprang, Maj. Ronald W., USA. "The Evolution of Russian Operational Art." Small Wars Journal. Accessed March 13, 2018. http://smallwarsjournal.com/jrnl/art/evolution-russian-operational-art.

Stearns, Peter N., Michael Adas, Stuart B. Schwartz, and Marc Jason Gilbert. World civilizations: The global experience. Pearson, 2014.

Taylor, Brian D., Politics and the Russian army: civil-military relations, 1689-2000. Cambridge University Press, 2003

The Economist, "On Putin's Terms." The Economist, November 14, 2008. https://www.economist.com/node/12622987.

Thomas, Dr. Michael L. and Dr. Dennis J. Bellafiore. "Geospatial Intelligence and Cyberspace." Cyber-Geography in Geospatial Intelligence. 2017. Accessed March 14, 2018. https://www.e-education.psu.edu/geog479/node/557.

Thompson, Ewa, "REFLECTIONS ON ERRORS IN SOME WESTERN INTERPRETATIONS OF FYODOR DOSTOEVSKY'S THE BROTHERS KARAMAZOV." Rice University, <http://www.owlnet.rice.edu/~ethomp/Dostoevsky%20&%20Philosophy.pdf>

Triandafillov, Vladimir, The nature of the operations of modern armies. No. 5. Psychology Press, 1994.

United States. Defense Intelligence Agency. Military Power Publications. Military Power Publications. Compiled by Lt. Gen. Vincent Stewart, USMC. 2017. Accessed March 14, 2018. http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf.

Wishnick, Elizabeth, "In search of the 'Other'in Asia: Russia–China relations revisited." The Pacific Review 30, no. 1 (2017): 114-132.

IRAN

Paulo Shakaria, Jana Shakarian. *Introduction to Cyber-Warfare, a Multidisciplinary Approach*. Syngress. 2013.

Kermit Roosevelt. Countercoup: The Struggle for the Control of Iran. New York: McGraw-Hill Book Co., 1979.

The World Factbook 2017. Washington, DC: Central Intelligence Agency, 2017. https://www.cia.gov/library/publications/the-world-factbook/index.html

Katzman, Kenneth. Iran's Foreign and Defense Policies. Technical Report. Congressional Research Service Washington United States. (2017) http://www.dtic.mil/dtic/tr/fulltext/u2/1027350.pdf.

Anderson, Collin and Karim Sadjadpour. Iran's Cyber Threat: Espionage, Sabotage and Revenge. Carnegie Endowment for International Peace. 2018.

Gabi Siboni, Sami Kronenfeld. "Iran's Cyber Warfare". INSS Insight No, 375, October 15, 2012. http://www.inss.org.il/publication/irans-cyber-warfare.

Frank J. Cilluffo, Sharon L. Cardash, Cyber Domain Conflict in the 21st Century, 14 Seton Hall J. Dipl. & International Relations 41 (2013).

Simon, Steven. "Israel and Iran". The Sixth Crisis: America, Israel, Iran and the Rumors of War (2010). http://iranprimer.usip.org/sites/default/files/Iran%20and%20Israel.pdf

Transcript of meeting between Saddam Hussein and Ambassador Glaspie. 15/03/2008. http://www.daralhayat.com:9090/search/SearchServlet?search=glaspie&COMMAND=listItemsInService&SELECTED_SERVICES=DarAlHayat_EN&simple.x=0&simple.y=0

"Saudi foreign minister calls Iran most dangerous nation for cyberattacks". CNBC. 18 Feb 2018. https://www.cnbc.com/2018/02/18/iran-most-dangerous-nation-for-cyber-attacks-says-saudi-foreign-minister.html

Potter, Lawrence. "Saudi Arabia in Transition". Great Decisions. 2017. P. 60.

Herr, Trey and Laura K. Bate. "The Iranian Cyberthreat Is Real". Foreign Policy. July 26, 2017.

Matthew McInnis. Iranian Deterrence Strategy and Use of Proxies. Testimony before the Senate Committee on Foreign Relation. December 6, 2016.

Eisenstadt, Michael. "The Strategic Culture of the Islamic Republic of Iran". Middle East Studies. Monographs. No. 7 November 2015.

Eisenstadt, Michael. "Cyber: Iran's Weapon of Choice". The Cipher Brief. January 20, 2017.

Morgan Chalfant. "Experts say US should expect more Iranian cyberattacks". The Hill. January 5, 2018.

Joseph Berger. "A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case". The New York Times. March 25, 2016.

Max Kutner. "Alleged Dam Hacking Raises Fears of Cyber Threats to Infrastructure," *Newsweek*. March 30 2016.

"FM: Iran may quit Nuclear deal if US withdraws". Fares News Agency. September 29 2017.

Michael Connel. "Deterring Iran's Use of Offensive Cyber: A Case Study". CNA Corporation. Washington. 2014.

Kirk, Jeremy. "Iranian Cyber Army running botnets, researchers say". Computer World. Oct. 25, 2010.

Frank J. Cilluffo. "The Iranian Cyber Threat to the United States. "Statement to the US House of Representatives Committee on Homeland Security. Apr. 26, 2012. P. 5.

Caught in a Web of Repression: Iran's Human Rights Defenders Under Attack". Amnesty International. https://www.amnesty.org/en/latest/campaigns/2017/09/iran-human-rights-defenders-caught-in-a-web-of-repression/

Zahraa Alkhalisi. "Saudi Arabia Warns of New Crippling Cyberattack". CNN Tech. Jan. 26, 2017. http://money.cnn.com/2017/01/25/technology/saudi-arabia-cyberattack-warning/index.html

Riley Walters. "Cyber Attacks on U.S. Companies in 2016". The Heritage Foundation. Dec. 2, 2016.

"Iran rejects UN criticism of its cyber security rules". Reuters. Oct. 12, 2012. https://www.reuters.com/article/iran-security-un/iran-rejects-un-criticism-of-its-cyber-security-rules-idUSL1E8LP8YD20121025

The World Factbook: Iran. Central Intelligence Agency. Lase updated on Mar. 15, 2018.

Amir Basiri. "Iran And The Revolutionary Guards' Economic Powerhouse". Forbes Magazine. Mar 29, 2017. https://www.forbes.com/sites/realspin/2017/03/29/iran-and-the-revolutionary-guards-economic-powerhouse/#26c4c4e5cf4e

Hakimian Hassan. "How Sanctions Affect Iran's Economy". Council on Foreign Relations. May 22, 2012.

Willis Stanley. "The Strategic Culture of the Islamic Republic of Iran". Prepared for: Defense Threat Reduction Agency. Advanced Systems and Concepts Office. Comparative Strategic Cultures Curriculum. October 2006.

Michael Gordon. "Iran Supplying Syrian Military via Iraqi Airspace". The New York Times. Sept. 4, 2012.

Nicole Perlroth and Clifford Krauss. "A cyberattack in Saudi Arabia had a Deadly goal. Experts fear another try". The New York Times. March. 15, 2018

Jose Pagliery. "ran hacked an American casino, U.S. says". CNN Tech. Feb. 27, 2015. http://money.cnn.com/2015/02/27/technology/security/iran-hack-casino/index.html

Russell Brandom. "Iran hacked the Sands Hotel earlier this year, causing over $40 million in damage". The Verge. Dec. 11, 2014.

"Iran sees cyber attacks as greater threat than actual war". Reuters. Sep. 25, 2012. https://www.reuters.com/article/net-us-iran-military/iran-sees-cyber-attacks-as-greater-threat-than-actual-war-idUSBRE88O0MY20120925

Ilan Berman. The Iranian Cyber Threat. Statement before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies. March 20, 2013.

DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA

"Historical Evolution of North Korea's Monolithic Political System and Its Main Characteristics." *Understanding North Korea: Indigenous Perspectives,* edited by Jongwoo Han, and Jung Tae-hern, Lexington Books, 2013.

"North Korea Cyber Activity." *Recorded Future Insikt Group.* July 25, 2017 https://go.recordedfuture.com/hubfs/reports/north-korea-activity.pdf

Cho, Hwa Sung, "An Empirical Study on North Korea's Strategic Culture and Negotiating Strategy," *The Korean Journal of International Studies* 49(5), 2009.12, 149-171.

Fingar, Thomas, *et al.,* "Analyzing the Structure and Performance of Kim Jong-un's Regime," *Shorenstein Asia-Pacific Research Center* at Stanford University and the Institute for National Security Strategy. June 2017

Hong, Yong-Pyo, "North Korea's Strategic Culture and Threat Perception: Implications for Regional Security Cooperation," *Korea Observer,* Vol. 42, No. 1, Spring 2011, pp 95-115.

Hwang, Il Do, *Framing North Korea's Strategic Culture From With the Century*, Yonsei University

Hymans, J. E. C. 2008. "Assessing North Korean nuclear intentions and capacities: a new approach."

Journal of East Asian Studies, 8: 259-292.

Son, Hyo Jong, "Nuclear Dilemma of North Korea: Coexistence of Fear and Ambition– North Korea's Strategic Culture and its Development of Nuclear Capability –," *The Korean Journal of Defense Analysis.* Vol. 29, No. 2, June 2017, 195 — 211.

Tellis, Ashley J., et. al., "Understanding strategic cultures in the Asia-Pacific," *Strategic Asia* 2016–17

Yeong, Jean Mi, Political Languages in the Kim Jong-un Era: Political Symbols and Discourses, Ewha Institute of Unification Studies.

Youngchul, Chung, "Nationalism in North Korea and Acculturation: North Korean Acculturation in Kim, Jong-un Era," *The Journal of Cultural Policy 31-2.* Sogang University.