University of Nevada, Reno

Shaping Cybersecurity Strategy: China, Iran, and Russia in a Comparative Perspective

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Political Science.

By

Mitra Assoudeh

Dr. Xiaoyu Pu/Dissertation Advisor

August 2020

THE GRADUATE SCHOOL

We recommend that the dissertation
prepared under our supervision by

MITRA ASSOUDEH

entitled

Shaping Cybersecurity Strategy:
China, Iran, And Russia In A Comparative Perspective

be accepted in partial fulfillment of the
requirements for the degree of

DOCTOR OF PHILOSOPHY

Xiaoyu Pu
Advisor

Dr. Leonard Weinberg
Committee Member

Dr. Eric Herzik
Committee Member

Dr. Elizabeth Francis
Committee Member

Dr. Mehmet Tosun
Graduate School Representative

David W. Zeh, Ph.D., Dean
Graduate School

August, 2020

Abstract

Cyberspace has emerged as a new domain for strategic competition among states. How do China, Russia and Iran respond to cyber-threats differently? And why? Through detailed comparative case studies, this dissertation introduces a new cyber-threat assessment model based on neoclassical realism approach in an attempt to explain states' divergent outcomes in threat assessment. In particular, this model identifies how and why states adopt different strategies in response to the growing challenges in the cyber domain. On the international level, while China seeks to rewrite cyber norms and introduce an alternative cyber governance model to replace the current Western-led model, Iran works to export its revolutionary values and to bring about an Islamic awakening and develop a value system competitive with Western morality, and Russia seeks to control Eurasia and dismantle Western democratic systems. Domestically, all three countries retain authoritarian structure. This study makes contributions to broader literature on cybersecurity in two respects: first, this study clarifies concepts and ideas related to cybersecurity and threat assessment; second, this study introduces a cyber-threat assessment model – the Multi-tiered Cyber-threat Model (MCTM) – uniquely based on a neoclassical realist approach to the state and foreign policy.

In memory of my beloved grandparents Rafat and Aref

Acknowledgement

I am indebted to many who helped me complete this research. I am grateful to the political science department for providing me academic support and financial assistance during my study at University of Nevada Reno. My gratitude goes to the graduate school at UNR for their continuous support.

My special thanks to my dissertation committee members – Dr. Leonard Weinberg, Dr. Eric Herzik, Dr. Mehmet Tosun and Dr. Elizabeth Francis – for their constant support and guidance. My deepest appreciation to Dr. Xiaoyu Pu, my dissertation advisor and chair, for his mentorship and encouragement. His invaluable guidelines enriched my study and provided me insights for the future research.

I am grateful to the generous financial support of the Bilinski Foundation that made this study possible.

I want to extend my special thanks to Jana Gering for her editorial help. I am grateful for her friendship and support.

My appreciation also goes to Carol Johnson, as well as Jennie and Dale Pritchett for their support and encouragement.

My deepest gratitude to my husband Eliot, for his love and compassion, also, thanks to Bouquet, Nelly, and Norouz.

Table of Contents

List of Tables

List of Figures

Chapter One: Introduction

1.1 Introduction

The Internet turns 50 this year. From its origin as a U.S. Department of Defense program in 1969, to its adoption as a research tool in 1980s, to its becoming a ubiquitous technology and information superhighway as public good, a combination of technological, social, political, cultural and economic factors has shaped the World Wide Web (Naughton 2016; Tabora 2018). In 1996, during World Economic Forum in Davos, Switzerland, John Perry Barlow, one of the fathers of Electronic Frontier Foundation and often considered the "Thomas Jefferson" of cyberspace, declared the independence of cyberspace from states' sovereignty (Barlow 1996). In a way, Barlow's utopian vision echoed the motto of the Internet Engineering Task Force (est. 1986): *We reject: kings, presidents and voting; We believe in: rough consensus and running codes*. Not a decade past its declaration of independence, cyberspace is enmeshed in every aspect of our socio-economic systems.

Cyber-information systems have become critical infrastructure for the large economic powers of the world. As systems have increasingly transferred operations from physical space to cyberspace, governments and industries – public and private sectors – alike have developed growing concerns about the security risks and how to address them (Lindsay 2012). Barlow's *civilization of Mind in Cyberspace* not only didn't endure its separate sphere, but also turned into a new domain of states' geopolitics and sphere of influence. While the Internet originated in the United States, it has always been seen as a global network that transcends geopolitical territories. As the network has grown,

however, tension between its global nature and local culture, custom, and law has increased. Applying local governance to influence network norms has proved so difficult to control, that fears of inevitable internet 'Balkanization'—the splitting of the global network into local subnets—have been expressed (Naughton 2016).

In 2018, cyber espionage campaigns by countries such as Russia, China, and Iran escalated and targeted objectives in every major region of the globe, based on their respective security and economic needs (M-Trends 2019). A majority of the cyber-attacks affiliated with these three countries were carried out by Advanced Persistent Threat (APT) groups. Most APT groups receive some level of support from an established nation-state, and many are affiliated with China, Iran, or Russia. While the cyber activity carried out by these groups is not unique from the type of activity carried out by most cyber criminals, APT attackers play a longer game, strategizing for months or years to reach objectives, adapting to defensive changes and retargeting victims.[1]

Russia's Soviet Union history, especially the information war against the West, continues to shape its current approach to cyberspace. Almost since the inception of the internet, the Kremlin has advocated for international-level cyberspace regulation with the intention of safeguarding "information space" against foreign interference. This informational aspect is also a central tenet of Beijing's policy, and Tehran is constantly tantalized by the idea of undermining the Western-led international system through subversive information operations and hostile cyber activities.[2]

---

[1] "Advanced Persistent Threat Groups: Who's Who of Cyber Threat Actors". FireEye. Available at: https://www.fireeye.com/current-threats/apt-groups.html

[2] For more information see Fabio Rugge (ed). *Confronting an "Axis of Cyber": China, Iran, North Korea, Russia in Cyberspace*. Ledizioni Publishing, Milano 2018 (Kindle Edition); Dean Cheng. *Cyber Dragon: Inside China's Information Warfare and Cyber Operations: Inside China's Information Warfare and Cyber*

One fundamental difference between authoritarian states like China, Iran, and Russia and that of the US is the definition of a cyber threat. Cyber threats in the United States are defined as both cyber-attacks (offensive operations that disrupt digital and/or physical operations, manipulate users, or delete data), and cyber espionage (intrusions onto protected networks to steal sensitive information) (Clapper 2013). Authoritarian states, however, have different perceptions and approaches to cybersecurity. For instance, China, Iran, and Russia define cybersecurity along lines of their unique interpretation of state sovereignty; specifically, that a state has the right to control the publication of content in the cyberworld as well as in the real world. This interpretation has long created an impasse to international cybersecurity agreements (Ibid). Another point of difference between the West and these authoritarian regimes is how they approach to cyber threats. In contrast to the Western tendency to cyber threats as a technical threat demanding a technical response,[3] to Beijing, Moscow and Tehran propaganda and disinformation tactics are of at least as much strategic importance as infrastructure disruption through technical means (Giles 2016).

The perspective differences between the West and these three nations in their approaches to cyberspace represents a major, possibly irreconcilable, deadlock. Every state uses cyberspace to protect domestic interests and advance state interests

---

Operations. ABC-CLIO Publishing, 2016; Donara Barojan. *Eight Takeaways from Iranian Information Operations*. The Cyber Edge. 1 April 2019.

[3] States have different priorities regarding cybersecurity; While priorities for a democratic state such as the United States are to secure its global position, intellectual property rights, free trade and open flow of information, for China's cybersecurity strategy, which is in line with its overall strategy, the priorities are the survival of the Chinese Communist Party, internal instability, and promoting economic growth. Here, the issue is cyber-threat, for the United States threats are mainly technical in nature; US does not feel the need to protect its culture by limiting its citizens' access to social media platform. For more information see Lindsay, Jon R. "The impact of China on cybersecurity: Fiction and friction." *International Security* 39, no. 3 (2015): 7-47.

internationally; however, the West perceives the actions taken by these three countries as an indication that they intentionally weaponize the domain of cyberspace in order to upset and/or destabilize, not merely the international order, but real-world infrastructures. The free and open Internet, which to the West represents a "global common" territory, plays host to the same worldview conflicts over human rights and individual freedoms that have been held in various international forums, represents nothing more than a direct threat to the power held by autocratic regimes (Rugge 2018).

As dependency on the internet and the resulting interconnectedness of people and services worldwide increases, societies become more vulnerable to cyberattacks. The growing influence of cyberspace lends a previously unavailable capacity to smaller actors (states or non-states) to influence world politics, and with its low cost of entry, anonymity, and various vulnerabilities, is an important new context in world politics. New information pathways have always influenced the balance of power, but the volatility of the manmade cyber-environment is an unknown quantity (Nye 2010).

The truly serious threats of the future to the stability of cyberspace are increasingly seen in the development of offensive action. While the characterizations of cyber-attacks and cyber-war are still ambiguous in definition, Joseph Nye's (2013) definition states that cyberwar consists of "any hostile action in cyberspace that amplifies or is equivalent to major physical violence." The possibilities of cyber-war start with attacks on critical infrastructure, which almost immediately blurs the boundary between

cyber and physical warfare, as seen in the deployment of Stuxnet[4] by the U.S. acting against Iran's nuclear facilities (Ramicone et al. 2014).

Both dramatic shifts and small changes to structural order affect how states perceive their own place relative to other nations, according to Paul Kennedy. In relationship to one another, the relative strength of leading nations constantly shifts as advantages, opportunities, challenges and threats, technological or otherwise, affect the balance of world affairs (Kennedy 2010). Mary Kaldor defines the new or "post-modern" wars as a lower-intensity type of conflict, as far as physical force. As the idea of defensible *territory* has grown more fluid and blurred the lines between *domestic* and *international* jurisdictions, especially with cyberspace quickly becoming the fifth domain of international relations, Kaldor sees the justification for conflict represented in greater proportion by value/identity-based claims rather than territorial ones (Kaldor 2013).

From Russia's post-Cold War uncertainty over power and global position and China's concerns over global identity, to Iran's interest in ensuring that its self-identified position of power in the Middle East receives proper recognition, questions of self-identity and perception from outsiders bear definite influence on state behavior and policymaking. Defining what these identity factors are and how they influence foreign policy are primary concerns for major states (Kaarbo 2003). Chinese, Iranian, and Russian motivations to gain power and compete with the U.S. and the Western-led liberal international order – albeit, with a much different scope and scale – continues to drive some of the expansion and diversification of threats to the U.S. national security, and it is

[4] Stuxnet worm was created and used allegedly by the US and Israeli governments to use against Iranian nuclear facilities. It disrupted Iranian nuclear enrichment in 2010. It is the first and only known instance of a computer network attack that has caused physical damage beyond international borders.

becoming more apparent how much of this competition – centered on a race for military and technical superiority – is ever more about values, regardless of domain.

This chapter consists of three sections: the first discusses how and why the puzzle of similar systemic pressure and different states' responses arises. How do states with different domestic structure and politics respond to cyber-threats? How do states go about mobilizing resources necessary to implement cybersecurity policies? Why do states perceive cyber-threats and opportunities differently? These are important questions that cannot be answered by the dominant structuralist or liberal institutionalist theories of international relations. Neoclassical realism, on the other hand, has the explanatory power to answer such questions because it expects variation in the responses to systemic changes vis-à-vis states' domestic politics and structure. The second section describes the methodology and research design. The third section discusses cyber threat assessment. I develop a neoclassical realist model for cyber threat identification that shows how states with various domestic situations – in particular, sets of ideational and institutional factors – will respond to threats.

1.2 The Puzzle: Similar Systemic Pressure and Different States' Responses

States' adaptation to systemic changes, and the outcomes of those changes are influenced by the political systems and internal domestic variables. Similar systemic pressures and opportunities can produce different responses based on motivations that are related to systemic or domestic factors. These motivational variations are rarely considered in cybersecurity studies, a shortcoming that we attempt to address in this dissertation.

The U.S.-led post-Cold War order came about because of three key political developments; not least of the three, that the United States had no major global ideology to compete with, following the defeat of communism. In addition, the infrastructure and institutional gaps left by the disintegration of the Soviet Union meant that weaker states were left with no significant alternatives to the U.S.-led West for military, economic, and political resources. The third key development was the rising transnational movement of activism in promoting liberal democratic values. Those same dynamics have more recently worked against the United States; the competing narratives represented by China and Russia embody major ideologies to rival the West. Majority of states, both developing and developed nations, have more options of partnership or patronage to remaining dependent on Western support. And the transnational ideological activism now is often driven by illiberal or extremist – far-left, radical right, or religious fanatic – networks countering the once-solid values of liberal international order (Cooley 2020).

Based on shared democratic and economic interests, European states have been willing to accept US deployment of extraterritorial pressures. Now, while they still benefit to an extent from the stability provided by US hegemony, that very stability in transatlantic relationship networks can represent a form of latent imperialism (Farrell and Newman 2019). Authorities in non-democratic nations like China, Iran, and Russia naturally protest against America extraterritorial pressure including the favor cyberspace technologies give to the US-led Western order, and often use “the myth of security through expansion” to both protect their regime and rhetorically position themselves as defending general societal rights, disguising their parochial interests (Snyder 2013).

The way in which complex domestic political processes in China, Iran, and the United States form an interesting case study for how these systems influence policy outcomes, including cybersecurity. For instance, while both China and Russia are authoritarian regimes, US social media platforms such as Facebook and twitter are simply banned in China while still allowed in Russia. China and Russia both view influence operations as normal cyber-activity, while Western nations consider it to be an elevated security, if not wartime, activity. Despite varied approaches, both nations use such operations to achieve the common goals of suppressing dissent and controlling communications. While Russia's information control methods are based on manipulation tactics and China's are actually more based on censorship, both models exemplify "digital authoritarianism" on the move. Or, on cyberspace, Russia was heavily involved in US presidential elections in 2016 while China was not. One explanation lies in their different targets; China's specific target is, broadly stated, its diaspora. Russia's interference has been more targeted to broad general population segments driven by political and ideological motivations (Jean-Baptiste and Charon 2020). Beijing, Moscow, and Tehran view cyberspace an excellent area to challenge American leadership as well as the liberal international order; thus, they are differentiated by their responses. While China wants to re-write the rules of cyber governance (Sacks 2018), Russia's intention is to disrupt Western political systems and build its own internet (Staedter 2018). Iran's cyber posture is similar to China's, although more regional in scope and at a limited scale.

Russia and China are more ideologically united in their national interests, threat perceptions, and values than they have been since the 1950s, especially in reaction to the

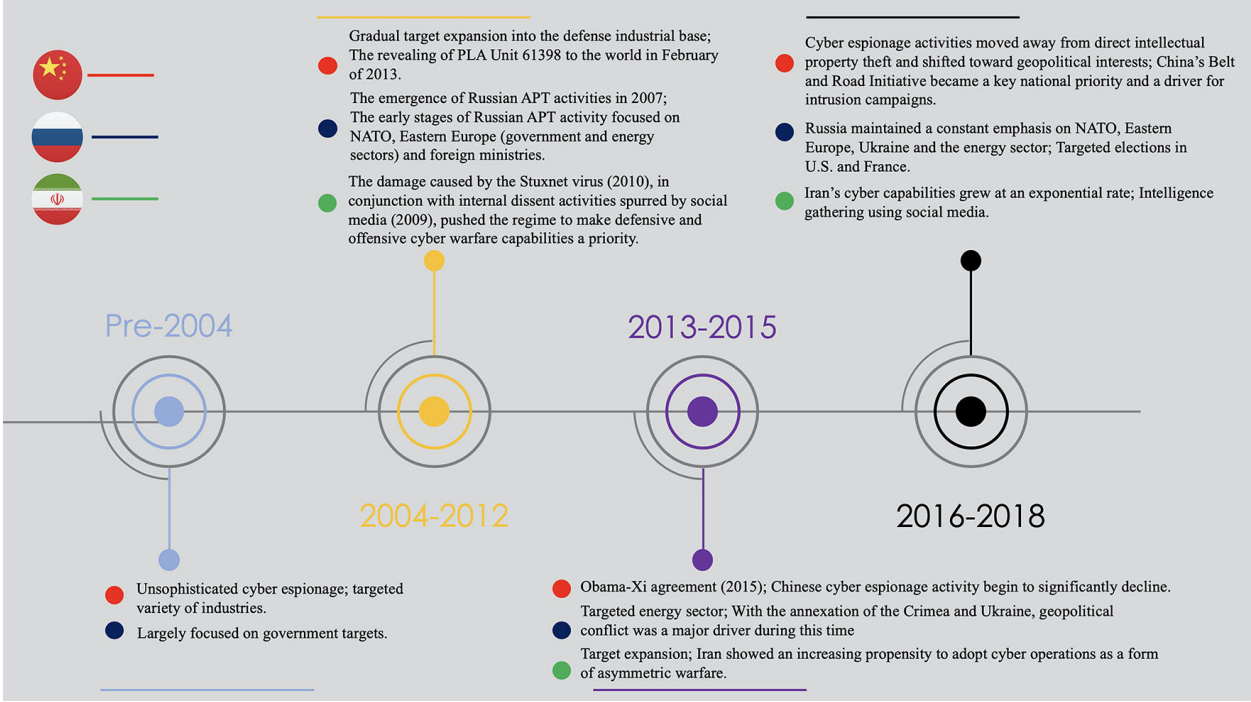
broad Western promotion of democratic values, human rights, and overall U.S.-led unilateralism (Coats 2019). Beijing and Moscow advocate for their authoritarian models and seek to re-shape global governance, including cyberspace, consistent with their image.[5] Not only does Russia's new Ministry of Defense cyber command group continue to mine sensitive computer network information from the U.S. and other nations, Russian-requested changes to the international system for Internet governance directly compromise stated US values, presenting another set of unique challenges (Clapper 2014). Operations in China, meanwhile, clearly reflect the priorities set by leadership across all channels of governance, with an almost-paradoxical facilitation of commerce development paired with an extreme policing of any online behaviors perceived as minor or major threats to regime and social order. China continues to expand its well-known intellectual property theft and network exploitation, while simultaneously challenging the international standard model of internet governance (Segal 2017). In addition to cyber espionage, Iran's cyber activities mainly rely on mass communication platforms for exporting revolutionary values. Regular communications share the message that the Islamic Republic is a rising regional power with growing ideological influence, crediting Iran with inspiring Arab uprisings in 2010, and initiating a wider "Islamic awakening" on par with the revolution of 1979 (Ighani 2013).

As illustrated in figure 1, since 2004, the cybersecurity positions of China, Iran, and Russia have expanded as well as shifted from dedicated espionage, to the protection of value-based interests. China's cyber activities focused on the One Road, One

[5] *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competition Edge*, Department of Defense, Arlington.

Belt/Digital Silk Road as a path to broader influence over local politics of specific interests to China. Iran, at the same time, is more concerned by domestic instability, which has incentivized defensive and offensive capabilities and intelligence-gathering through social media. Russia's cyber-activity has focused on disinformation strategy and its influence over domestic citizens and international democracies, spread to the U.S., NATO, and Eastern Europe.

Figure 1 – Evolution of Cybersecurity Postures[6]



Due to the complex nature of the cyber domain, states develop different strategies in response to this systemic change and they have different approaches for integrating cybersecurity programs into national strategy. In 2011, the United Nations Institute for Disarmament Research surveyed the security capabilities of 133 states, based on open-

[6] Source: Coats, Daniel R., *Worldwide Threat Assessment of the US Intelligence Community*, Senate Committee on Armed Services, January 29, 2019; FireEye, M-Trends 2019.

source documents, and assessed their policies and organizations. Specific areas of the study covered cyber-security infrastructure and response procedures, military protocol for cyber-activity, and whether the state has a plan in place for acquiring offensive cyber capability. While many states are open about law enforcement and cybersecurity arrangements, the nature of open source data revealed a more guarded attitude among states about their cyberwarfare planning and capabilities. The report indicates that 33 states established cyber unites within their military organization (Lewis and Timlin 2011), whereas in 36 other states, the responsibility for cybersecurity is assigned to civilian agencies and the role of military is not clearly defined (Lewis 2011).

A consideration of domestic politics is essential to a better understanding of states' status concerns on an international level (Pu 2019). International events such as the September 11 terror attacks, the collapse of the Soviet Union, and the Arab Spring, which threatened or upset the global order, have previously generated very different responses from major powers. States' expressed responses to such events will clearly reveal the cultures that either favor civilian or military approaches. Understanding both the reasons why national security cultures undergo changes over time, and the implications of those changes is necessary to understanding the future of international security governance. Why have various major states, for example, responded in such varied ways to major international events, including the end of the Cold War and the global rise of Jihad? These diverse responses of course reflect disparity in resource constraints and other practical terms, but they also may indicate subtle differences in national security culture response preferences, in spite of similar risk and threat assessment. Each national security culture – because of unique elements like national

understanding of external environments, preferred modes of statecraft, interaction patterns, and choice of institution – poses certain barriers and presents certain opportunities to regional and global security governance (Kirchner and Sperling 2010). The subtle link between national security cultures and the preferred security governance response is not well-explored in the literature. This study, by way of contribution, highlights a few features of China's, Iran's, and Russia's domestic politics, which influence their cybersecurity strategic behaviors.

Specific domestic structures and political situations certainly influence the way states assess and adapt to outside changes, and many complex political processes help to balance and direct responses to threats and opportunities. The same pressure on one system might not create the same reaction as in another. The outcome of a state's response to an external environmental change depends on many factors, from the societal structure to the various political and social actors involved (Schweller 2004).

1.3 Research Design: Methods and Case Selection

It is the especial focus of this study to examine why, how, and under what conditions a state's domestic politics and structure – sets of ideational and institutional factors (more details in the following section) - may influence its foreign policy and the elites' threat/opportunity assessment in cyberspace. In each case, systemic constraints filtered through the internal characteristics of a state and affect the way in which officials observe, assess, and respond to potential cyber threats, as well as how officials organize societal resources to support those strategies.

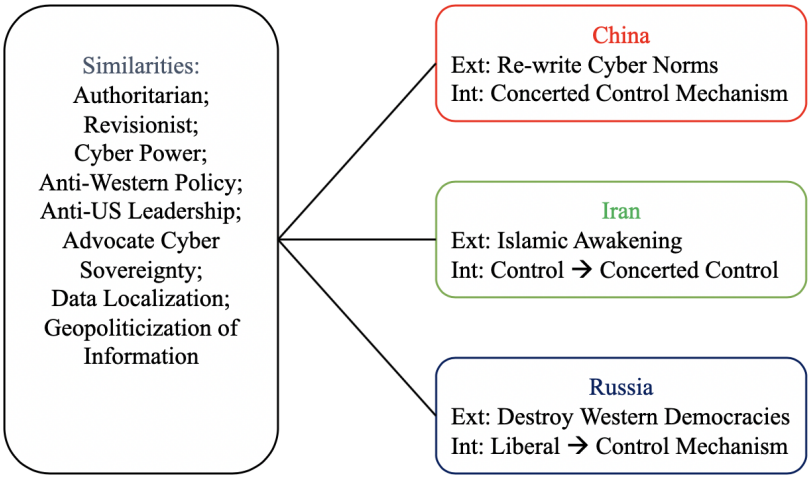
Cyberspace is a relatively new and complex domain. The scholarship on cybersecurity suffers from major theoretical and methodological shortcomings. In the absence of solid theoretical grounds, the majority of the studies are single-case studies. This is a theory testing case for assessing validity of existing neoclassical realist models in the case of cybersecurity, supplemented by a policy recommendation section for the U.S. government officials; this research, however, is the first study to provide a neoclassical realist model for identifying cyber-threats. Neoclassical realism can account for a rich variety of foreign policy determinants and states' responses to systemic challenges (see next section for more details).

I draw on data from both primary and secondary sources. I will also investigate ideational sources of these states cybersecurity postures through content analysis of government documents of official and foreign policy analysis. Primary and secondary sources provide data, while ideational sources of cybersecurity positions are provided by government documentation and foreign policy analysis.

The research design is a most similar cases design, also called Mill's method of difference. The cases explored are China, Iran, and Russia. The most similar cases design is the most appropriate because these three countries share some key characteristics, yet experienced divergent outcomes, i.e. there is variation in the dependent variable: China, Iran, and Russia represent the most-similar cases design, based on key characteristics and divergent outcomes. Contemporary China, Iran and Russia provide a useful set of cases for exploring state's national cyber security policy. Within each case I will examine the specific mechanism of state's cybersecurity behavior. States have different priorities regarding cybersecurity, which result in variations to shaping cybersecurity strategy – the

dependent variable. While priorities for a democratic state such as the United States are to secure its global position, intellectual property rights, free trade and open flow of information, non-democracies such as China, Iran and Russia prioritize their cybersecurity strategy differently. In China's cybersecurity strategy, which is in line with its overall strategy, the priorities are the survival of the Chinese Communist Party, maintaining internal stability, and promoting economic growth. While in the Islamic Republic internal stability and regime survival are important, as is the case in China, promoting Islamic revolutionary values within and beyond borders is another singular priority. Russian foreign policy continues to seek power status within a declared preference for a multipolar world, prioritizing state sovereignty over internal affairs, displaying a heretofore-unforeseen level of antagonization toward Western ideals in a barrage of disinformation. Further, China, Iran, and Russia differ in their authoritarian structure and internet governance; while Freedom House has classified these three countries as consolidated authoritarian regimes, Xi's China is a far more difficult place to be a netizen, to begin with, and secondly, internet governance is handled very differently in each country.

Figure 2 – Most Similar Design: China, Iran, and Russia



China: In addition to domestic oppositions, Chinese espionage operators target some neighboring autonomous regions, such as Taiwan and Hong Kong, which Beijing considers an inalienable part of China. In recent years, China has tested new cyber-related tools and tactics before moving them into worldwide operation, including monitoring neighboring countries' elections and politics, suggestive of an elevated effort to protect overseas interests and an expanded Chinese global influence.

Following a period of reduced activity since 2016, many Chinese APT groups are increasing activity which appears to be linked to state-backed operators with modified TTP's and refreshed malware tools. The uptick in activity also appears to be focused on geopolitical activity and strategic intelligence (M-Trends 2019).

A disproportionate percentage of worldwide cyber-espionage activity is linked to Chinese sponsorship, especially in the direction of the U.S. Government, corporations, and allies. Chinese espionage activity weathers waves of growth and limitation, subject to China's shifting of economic priority, national strategy, and geopolitical posture.

China's international cyber-espionage apparatus probably grew out of the regime's [CCP] internal security concerns, which targeted dissenting elements and extended campaigns over jurisdictions China aims to influence, such as Taiwan, Hong Kong, and Western China. As China gradually improves its ability for cyber-attacks and online information alteration, its potential influence over citizen perspectives, from Chinese to U.S., grows as well. Another additional concern about the potential for Chinese intelligence and security services is the possibility that they might use Chinese info-sec (information security) and technology firms as platforms for systemic global espionage. The Chinese potential for cyber-attack is incredible, even extending to disruptions of major U.S. infrastructure, like natural gas pipelines. Even if disruptions are temporary, the impact could be significant.

Iran: One of the greatest cyber-espionage threats of 2018, judging by scope and scale, was posed by Iran. With intrusive tactics and strategic objectives that run from the immediate Middle Eastern region to worldwide activities, Iran's campaign activity directly supports the regime's interests (M-Trends 2019).

The Iran-nexus cyber-espionage operations have emerged from a regional and internal focus to a sophisticated, cohesive, intelligence-gathering apparatus with global reach and ambitions. Iranian APT operations, over the last ten years or so, have moved from a limited use of social media sites to creating specialized teams to develop impact tools and direct targeting for major social influence. Iranian actors have demonstrated effective cyber-targeting of U.S. Government officials, government organizations, private corporations, and even universities, in order to gain intelligence and prioritize future

cyber-operations. Iran's preparations for cyber-attacks against the U.S. and allies have motivated its capability growth to the point where it is entirely possible for Iran to cause localized, temporary—but potentially damaging—effects, such as disrupting a large corporation's networks for up to days or weeks, as exemplified by its data deletion attacks against Saudi networks in late 2016 and early 2017.

Russia: Moscow's highly capable and effective espionage infrastructure integrates cyber-strategy and influence operations to advance its political and military objectives, and many of the APT groups in Russia have grown from limited observation tactics, to an unmatched aggressive strategy in influence and intrusion operations. The unique effectiveness of the Russian APT threat environment is a product of a vast geopolitical landscape, internal security concerns, and cultural distinctiveness. In search of technical information, military strategy, and insight into government and policy, Russian intelligence and security services are highly motivated to continue targeting U.S., NATO, and Five Eyes partners.

The main catalysts for Russian strategy have been political adversaries, national defense, the Ukrainian conflict, and energy issues. In addition, there is some indication that Russian APT actors are prepared to both execute disruptive attack strategies, and to monitor Russian citizens locally and globally. The powerful cyber-attack assets currently staged by Moscow allow for disruption and damage to both U.S. civilian and military infrastructure during any crisis, including localized, temporary disruptive effects on critical infrastructure. With a goal of gaining the power to leverage substantial

infrastructure damage, Moscow continues to map U.S. critical infrastructure over the long term.

1.4 Organization

Chapter two presents a review of current scholarship on cybersecurity and cyber governance as well as the theoretical framework for the study. Chapters three to five contextualize cybersecurity of China, Russia, and Iran, respectively, within their external and internal environment. Chapter six summarizes the main findings and provides a policy recommendation for the United States. It also presents a cross-case analysis comparing the three cases across cyber threat assessment and cyber governance to explore the underlying factors that influence the states' cyber posture the most.

Chapter Two: Theoretical Framework and Literature

"The importance of cybersecurity revolves around how we define risk and how much risk a government or society is willing to accept".[1]

- James Lewis
Senior Vice President and Director, Technology Policy Program
Center for Strategic & International Studies

2.1 Introduction

Cyberspace has emerged as a new domain for strategic competition among states. As dependency on the internet and the resulting interconnectedness of people and services worldwide increases, societies become more vulnerable to cyberattacks (Lindsay, Cheung and Reveron 2015). The international attention to incidents such as Russia's cyber-attacks on Estonia (2007) and Georgia (2008), Stuxnet (2010), Wikileaks (2010), the Snowden affair (2013), the indictment of China's PLA officers for cyber espionage in the United States (2014), and Russia's disinformation campaign (2016), has changed security priorities for states by recognizing the Internet and cyberspace as a new source of threat (Lewis 2014). However, states' responses to such systemic and borderless challenges remain overwhelmingly national in scope.

The content of the states' national strategies differs widely, and each state drafts its policy around their own awareness and needs, infrastructure protection requirements, and stakeholder engagement. However, various factors complicate effective cybersecurity policy against threats: lack of consensus over the definition of the term 'cybersecurity',

[1] Lewis, J. A. "Cybersecurity and critical infrastructure protection". *Center for Strategic and International Studies*. 2006: 2.

lack of appropriate norms of behavior/a global cyber governance, and the increasing number of cyber-capable actors.

Disagreement on definitions is not uncommon with national security issues as they compete for attention on the public agenda, and what Arnold Wolfers called the "ambiguous concept" (Wolfers 1965) of national security concern is only enhanced when it comes to cyberspace and security. It's difficult for the public to take national security and cybersecurity concerns as a holistic issue, when factors vary so greatly in each situation, and actors' perceptions and/or agendas play a key role in securitization of the issues (Hare 2009).

Threat perceptions influence the views of national leaders on the role of cyberspace in international affairs, also impact national strategies. Threat perceptions are consistent with existing national perspectives on security. In democratic settings, security is more focused on confidentiality and integrity of data, further involving parties ranging from civilian and military elites to private sectors and civil society. However, authoritarian regimes are more concerned with political and cultural security and the engagement of actors other than military or civilian elites is much narrower in scope. In addition, states have different priorities regarding cybersecurity, which result in variations in shaping their cybersecurity strategy. While priorities for a democratic state such as the United States are to secure its global position, intellectual property rights, free trade and open flow of information, non-democracies such as China prioritize their cybersecurity strategy differently – mainly based on regime survival, domestic stability and status recognition.

Ideological divisions among states and/or within political elites represent another significant challenge to developing adequate internet governance that can efficiently identify and respond to cyber threats. So many stakeholders from so many sectors are involved in the conversation (technical communities, private industry, governments with differing goals for cyberspace, and intergovernmental organizations), that effective collaboration on the various political, economic, and governmental challenges is difficult to achieve.

2.2 Contribution and Literature

In seeking to explain the variations of cyber policies and postures, this study makes two contributions to the broader IR literature. First, this project makes contribution to the growing body of literature on the concept of cybersecurity in general, and threat assessment in particular. Second, this study introduces a new cyber-threat assessment model based on neoclassical realism approach; thus, contributes to the extant scholarship on neoclassical realism, the state, and foreign policy.

Cybersecurity

Massive cyber-attacks in Estonia, which targeted government, financial, and telecommunications infrastructure in 2007 shifted global perception of cyber-threats and revealed potential vulnerabilities of advanced information societies to security experts (Tikk, Kaska and Vihul 2010). As global business infrastructure, politics, social, and military activities increasingly utilize and depend on the internet, the topic of cybersecurity as an essential part of national and international security also gains priority (Lewis and Timlin 2011). In particular, every nation is faced daily with the tension of

how to maximize the internet-based economy, while at the same time protecting intellectual property, critical infrastructure, and national security (Hathaway and Klimburg 2012). Official and comprehensive national cyber-strategy, outlining the interests that need protection and the objectives that will guide future actions, are critical in establishing a guiding vision for cyberspace (Joubert 2010).

Contrary to its increased adoption by scholars and practitioners, there is no consensus over the definition of the term 'cybersecurity' and its constituent elements. Choices in definition and terminology (such as 'cybersecurity' vs. 'internet security') reveal not only different policy goals, but their roots in the fundamentally different worldviews of various nations – for instance, Chinese terminology for cybersecurity is 'information security' (Chang 2014). Some scholars, including Daniel Schatz, Rabih Bashroush, and Julie Wall from University of East London, attempted to understand the scope and context of the various connotations of the term 'cybersecurity' and, drawing on various semantic analysis of authoritative and relevant uses of the term (industry, government, and academic), proposed a more improved definition:

> The approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyber space. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users (Schatz, Bashroush and Wall 2017, 66).

A recent study by experts at the NATO Cooperative Cyber Defence Centre of Excellence shows as of 2012 "more than 50 nations have published some form of a cyber strategy *defining what security means* to their future national and economic security initiatives"

(Klimburg 2012, 12).[2] Analysis of the terms 'cyber security' and 'national security' in official documents may be a rough one, as national and linguistic differences, as well as the lack of agreement on definitions of those terms may prevent direct comparison. The term 'national security,' in particular, is defined even in government documents with some inherent flexibility. National cybersecurity discussions still involve military capability and international power-projection, but the tone of these discussions increasingly shifts toward managing risks instead of seeking ways to exploit those risks to advance global power.

While the priorities and objectives of each nation's cybersecurity strategy must be determined by those nations, interconnected issues such as stakeholder engagement, capacity building, cyber-governance, cyber-crime, and cyber-defense are some universal considerations (Sabillon, Cavaller, and Cano 2016). A *Geneva Center for Security Sector Governance* working paper identifies three major responsibilities for states with respect to cybersecurity: political, organizational, and legal (Schreier, Weekes, and Winkler 2015). Foremost among political responsibilities of the state are a cybersecurity policy consistent with the national security strategy and international cooperation to establish global norms for cyber governance. The prime organizational responsibility of the state is to take every possible measure to secure critical infrastructure to allow an appropriate response capability in case of any threat, especially as all levels of government increasingly rely on cyber networks dependent on well-maintained and secure IT systems. Indeed, infrastructure and IT resources need to increase as or more quickly to

[2] Emphasis is mine.

keep pace with the frequency and sophistication of cyberattacks, and this requires a level of organization that crosses national, regional, and local boundaries. Legally, a state is responsible for a nation's critical infrastructure and the criminal law framework that safeguard's civilian privacy and liberty.

Scholars and practitioners identify different rules and mandates/perspectives in order to provide guidance for states' national cybersecurity policies. A legal adviser at the NATO Cooperative Cyber Defence Centre of Excellence identifies ten rules to confront cyber threats (Tikk 2011): The territoriality rule; the responsibility rule; the cooperation rule; the self-defense rule; the data protection rule; the duty of care rule; the early warning rule; the access to information rule; the criminality rule; and the mandate rule. These ten rules outline key concepts and areas that must be included or addressed in a comprehensive legal approach to cybersecurity. They are intended to raise awareness about existing legal complications involving cyber security and the ways to overcome them, to serve as a focus for debate and coordination within and across disciplines, and to inform well-grounded proposals for additional legislation on the international level.

According to Alexander Klimburg, the Director of the Global Commission on the Stability of Cyberspace Initiative and Secretariat and Director of the Cyber Policy and Resilience Program at the Hague Centre for Strategic Studies, national cybersecurity doesn't represent a single subject area, but as a complex and deep issue, it can be split into five distinct areas to be addressed by different government departments. Although the five areas are simply different pieces of the same problem, each has developed its own language and priorities. These mandates include: Internet Governance and Cyber Diplomacy, Cyber Crisis Management and Critical Infrastructure Protection (CIP),

Military Cyber Operations, Intelligence/Counterintelligence, and Counter Cyber Crime. Klimburg's five mandates provides government agencies with a potential cybersecurity-related distribution of tasks and responsibilities (Klimburg 2012). Jason Healey, a senior research scholar at Arnold A. Salzman Institute of War and Peace Studies, Colombia University, and his co-author, Eric Luiijf, a cybersecurity consultant, supplement Klimburg's approach by three additional cross-mandates that work across all the mandates equally. They include Coordination, Information Exchange and Data Protection, and Research and Education (Luiijf and Healey 2012). Healey-Luiijf cross-mandate approach due to its focus on coordination and information exchange might mitigate national security tensions that might arise between civilian and military units and/or intelligence community and law enforcements as each of these four governmental agencies differs in their aims, structure, and culture (Klimburg and Healey 2012).

Finally, built on the prior research (discussed above), a NATO Cooperative Cyber Defence Centre of Excellence report identifies five security dilemmas associated with cyber power that needs to be addressed and balanced in a state's national cyber policy (Hathaway and Klimburg 2012):

1. Economic Prosperity vs National Security
2. Critical Infrastructure – Modernization vs Protection
3. Public-Private Partnership
4. Data Protection vs Information Sharing
5. Freedom of Expression vs Political Stability

Economic Prosperity vs National Security: Ensuring the ability of a nation to sustain and increase economic activity through using information and communication (ICT) technologies is a key objective for cyberspace security endeavors. Protecting activities

such as e-commerce, finance, and e-government is considered a high priority and it represents a common universal goal for the overall prosperity of many societies, a theme which is high in priority to the national cybersecurity strategies worldwide (Brangetto and Aubyn 2015).

The traditional 'security dilemma' of international relations theory, that both a nation's security strength and weakness may generate negative adversary responses, doesn't work quite the same way with national cybersecurity dilemmas, where economic and social costs are associated with either a strong or a weak cybersecurity posture. Nations face a constant tension not only of how to take advantage of the economic benefits of ICT, while simultaneously protecting privacy and intellectual property, securing infrastructure, and defending national interests and borders. As connectivity between individuals, businesses and markets demands greater security, increased capability, and better services, many national governments are struggling to identify the right mix of policy intervention and market support (Hathaway and Klimburg 2012).

An increasing number of consumers and businesses participate in internet e-commerce transactions; internet disruptions and shutdowns threaten not only this growth, but additionally they weaken innovation, and undermine confidence in a nation's economy. The disruption caused by connectivity problems increases in impact as online business transactions increase in proportion of global economic activity (West 2016).

State authorities disrupt internet for many reasons, including protecting government authority, reducing dissidence, resisting potential terrorism, and protecting local businesses. Disruptions, whether legitimate or illegitimate, have become a more common response to real or perceived threats to political stability and economic interests

(Howard, Agarwal, and Hussain 2011). A Freedom House report indicates the rise of internet shutdowns even in countries as democratic as India. In particular, since Narendra Modi's government gained power in 2014, the frequency, range, and duration of internet shutdowns has increased. During riots and protests, telecom networks were disabled in order to temporarily stop the spread of 'disinformation and inciting of violence.' A New Delhi-based think tank, the Indian Council for Research on International Economic Relations, reported that the shutdown hours between 2012 and 2017 totaled over 16,315 hours, and cost more than $3 billion (Bahree 2018). The Brookings Institute study of internet disruptions in 19 countries (authoritarian and democracy) from 2015-2016, conducted by Darrell West, identifies six major categories of disruption; national (the most frequent shutdown category), subnational, national mobile, subnational mobile, national app or service, and subnational app or service, which, cost those countries $2.4 billion during the study period (West 2016).

Critical Infrastructure – Modernization vs Protection: In addition to serious repercussions for a state's reputation and economic interest, cyber-attacks aimed at critical infrastructures raise concerns over public safety. Cybersecurity and protecting critical information infrastructure have now become so essential to the well-being of citizens, that it demands a coherent, strong, and continuous response from the government to secure cyberspace, reduce risk, gain national advantages, and mine the opportunities to improve knowledge and capability (Schreier et al 2015). The internet does not enjoy a homogenous infrastructure, rather its backbone comprises of a collection of

interconnected networks – high-tech based market driven grids arranged (mainly) by the private sectors with significant public policy implications (DeNardis 2014).

The economic prosperity vs. national security debate (discussed earlier) is also driven by the tension between the forces pushing for infrastructure modernization and economic stimulus, and the forces pushing for critical infrastructure defense (Hathaway and Klimburg 2012). Because interconnection agreements go largely unseen as private contracts, there is little oversight or regulation; an element that is unique to Internet interconnective relationships, which have developed with very little government oversight. While Internet and cyberspace development is often compared to telecommunications innovation, the latter was developed under highly involved state regulatory mechanism (DeNardis 2014). When it comes to regulation, governments must be concerned first with overall public security and safety across many infrastructures, while private organizations are compelled first and only by shareholder concerns. Those who own and operate interests within infrastructures must participate in standards definition and implementation in order to meet regulatory requirements, as a minimum. While a government must sometimes intervene to set requirements for essential services and meet citizen needs, intervention policies must balance carefully to avoid creating additional obstacles to the progress of innovation, information, and economic growth (Hathaway and Klimburg 2012).

Public-Private Partnership: Cybersecurity as an economic asset tends to be viewed as the domain of private corporations, despite the fact that certain cybersecurity solutions represent a public good (as discussed in the previous section). A general lack of

understanding about the public good element of cyberspace might explain the general unwillingness to share information and strategy, even among legislative initiatives (Brangetto and Aubyn 2015). The private sector has effectively become the major service provider of the internet; it represents a critical feature of modern national cyber strategy (NCS), responsible for the major research, design development, and the manufacture of much of the software and hardware of ICT (Hathaway and Klimburg 2012).

States alone do not have sufficient resources to cope with modern security challenges, including cyber threats and asymmetric warfare. Informal security complexes, especially public-private partnerships, have increasingly been a part of the responses. In such governance networks, cooperation is extended between states and a variety of other actors ranging from private sector and non-governmental organizations to international institutions. With this great variation in governance come gaps in our understanding, as well as questions regarding consistency, transparency, and accountability (Buckland, Schreier, and Winkler 2010).

Oversight institutions, such as parliamentary committees or ombudsman offices, are mainly concerned with the public authorities and agencies (e.g. intelligence communities, armed forces, security sectors, and justice system) over which they have direct responsibility and supervision of services and activities. The link between the varying governance organizations is one of both responsibility and oversight. A public-private partnership to improve national cybersecurity, even if funded by government agencies, falls outside of both conventional agency boundaries and the oversight of governmental chain of command, where there is limited or no supervision. Thus, control,

transparency, and oversight become more challenging when a public-private cooperation is forged in a cyber-domain.

Public-Private Partnership over cyber security imposes three types of complexities that intensify democratic governance challenges in a variety of ways: network, technical, and legal. Due to network complexity – the anonymity and diversity of actors involved in cyber-attacks – oversight bodies (e.g. parliamentary committees), often with limited ability, have difficulty keeping track of relevant actors, gaining knowledge of their existence and identity, or even acquiring legal rights to do so. Due to technical complexity – cyber security challenges are highly technical – oversight bodies are often less well-informed and do not have the complex expertise required to truly oversee them, in particular when private sector with expert forces and higher pay is involved. Due to legal complexity – including rights to privacy and freedom of expression – the responsibility and control of oversight is increased by public-private cooperation and the associated legal questions.

Data Protection vs Information Sharing: Following the Snowden affair (BBC News 011214), which revealed the vast US surveillance program on foreign governments and embassies, both adversaries and allies including eavesdropping on Chancellor Angela Merkel's cell phone, European authorities and public figures have advocated and sponsored variety of technical and non-technical solutions in order to achieve *technological sovereignty*, from constructing new undersea cables to revising data protection standards. Keeping any data from being processed through the physical infrastructure of other nations initially seems like an ironclad protection against state

surveillance, but that security is increasingly less sure. The legal barrier in some countries for intelligence agency data collection and use is very low, and will continue to reduce security, if measures forcing data localization become more stringent. The economic benefits of the internet economy cannot be fully realized while citizens' service expectations of the free exchange of information are in conflict with government policy for data protection and privacy preservation (Hathaway and Klimburg 2012).

Extreme restriction on the global flow of information was seen to be one potential solution to the post-Snowden reality of NSA spying on information. Concerned nations began to require local storage of user data from companies, and insist local internet routing within geographical borders, and sometimes pushed for governments and local users to use local companies and indigenous technologies for email, social media and cloud computing instead of global ones. Calls for data protection often were phrased in sovereignty-driven language, especially in regard to data sovereignty. In this context, the common themes of internet fragmentation and technology balkanization have become increasingly prevalent (Mueller 2017a).

Some countries, to gain cyber sovereignty, occasionally raise the idea of seceding from the global Internet in favor of a national internet—most specifically Russia and Iran. However, the concept of a national internet to date has not shown any difference between a technically separated internet, and one that is technically compatible, but extremely filtered, as China's is. Is a "national internet," then, simply a restriction of access, or is it an isolated substitute? National Internet initiatives, upon closer inspection, are often more a product of political rhetoric or support for domestic content distribution; it is rare that they are actually separated in technical terms (Mueller 2017b).

Freedom of Expression vs Political Stability: Cybersecurity discussions should include a deep understanding of the challenge and impact of cyberspace as a platform, where a significant amount of relationships between states and their citizens now occur (Sabillon, Cavaller, and Cano 2016). The ways and means by which dissenting movements are organized has certainly been changed by digital media and online social networking applications. Civil movement leaders can now leverage applications and content systems online to organize and track collective action, raise local and international awareness, and share political perspectives with global audiences (Hussain 2016). Some experts insist that a cybersecurity policy should address fundamental human rights and the impacts of the policy on citizens' civil liberties, others would prioritize measuring a state's international participation levels before and after such policies are implemented (Brangetto and Aubyn 2015).

The internet and new technologies may be just as easily used to target, silence and deny access to citizens as it may be used to enhance freedom and progress. The lines that authoritarian regimes draw when it comes to technology and cybersecurity may seem extreme, but what they truly show is that the very freedoms people enjoy globally because of information and communication technology (ICT) are very much at risk, and that political freedom is closely tied to freedom of communication (Hathaway and Klimburg 2012). Ever since activists expanded to consider internet resources in advancing collective goals against authoritarian governments, each regime has responded in distinct ways. The most essential and cheapest reaction is to harass or jail activists themselves, while ignoring the sites, applications, and Internet record. Regimes that choose this route are "response regimes." Some governments go beyond response and

develop extensive architectures of filtering, monitoring, and/or censorship to extend barriers between regular users and politically or culturally sensitive destinations on the internet. These "control regimes" seek to control a majority of information, mobilization, and the sites themselves, while knowing that individually committed actors can circumvent censorship. The third type of regime, "cordon regimes," emerged in the 2000s. Similar in goals and behavior to control regimes, it had the additional feature of creating contender social media and information sites which sought to present regime answers to the social and informational questions citizens were expressing (Faris 2015).

Not all internet shutdowns and cybersecurity-related incidents are the result of authoritarian state censorship, nor are they easy to classify as legitimate or illegitimate. In fact, one of the early instances of internet censorship happened in a Western democratic country as early as 1995, when German prosecutors demanded that an Internet Service Provider block sex-related content for 4 million worldwide subscribers. Since that time at least 606 incidents of government intervention in digital network connections have occurred, and roughly half were enforced by authoritarian regimes. China, Tunisia, and Turkey while representing both authoritarian and democratic regimes, hosted the highest number of incidents. Typically, it is during times of especial political pressure, such as election unrest or military incursion, that certain members of the elite or ruling class are willing to interfere with information infrastructure to influence civil society movements (Howard, Agarwal, and Hussain 2011).

States' Engagement in Cyber-Attacks: The literature on cyber security identifies three ways states might engage in cyber-attack: national forces, volunteer forces, and

mercenaries. If any new capability is needed, states traditionally redistribute existing resources within the state, or sometimes by creating a new body specifically to manage the task, ensuring that activities stay under government control. For instance, in 2009 and in response to the increased number of cyber-attacks, the United States created the CYBERCOM unit within its military domain. The Cyber Command example is merely an abstract—a force like this could take many forms, from traditional military units to intelligence forces or high science teams. Following the United States, many states – including China, Iran, and Russia – created similar units within their military organizations. What such units have in common is professional membership and a clear link to the state, which ensures, at least in part, cooperation with the military or government branches.

Interestingly, states with advanced cyber capabilities independent from their political system benefit from some sort of cyber militia too. While in a democratic system such as the United States, operational domain and the duties of the 780th Military Intelligence Brigade is better defined and clearer, non-democracies do not reveal much information about their cyber militia units. Since the mid-1990s, political activists have adapted to the medium of the internet, growing into coalitions of like-minded 'hacktivists' who have formed more organized groups around patriotic, ideological, and/or political ties, taking up arms against opposing groups or states. Cyber-militia can take the form of loose coalitions, or groups of highly organized hackers, activists, technicians, or security experts. Regardless of size, most of these groups are defined by a common motivation to take defensive or offensive actions, independently or under state direction, against an adversary to further the objectives of their own states. Political

hackers and cyber militias play an increasingly significant role in cyber conflicts, grouped around political, patriotic, or ideological commonalities. These ad-hoc groups are not governed by state oversight and can sometimes escalate conflicts without that accountability (Applegate 2012).

Hackers in the past tended to be lonely specialists looking for a challenge, but today cyber-attacks are often carried out with some kind of purpose in mind. While criminals typically seek financial gain from cyber-attacks, activists look to support a particular ideology, and this is the main segment that can be a source for volunteer cyber-militia (Ottis 2009). While the US Cyber Militia might be more interested in retaliation and offensive operation within military domain, cyber militia groups in China, Iran, and Russia seek financial gain and advocate the ideology of their respective regimes. The latter is mainly pursued by college students and instructors. While the majority of the scholarship on cyber security focuses on offensive militia forces, the operational mode of academic-based cyber militia is mainly passive-offense, meaning that they serve to propagate ideological ends with an offensively focused rhetoric.

Cyber forces can be assembled and managed by persuading existing hackers to work for the state, or by setting up a front organization to run teams in proxy for the government. States can guide supporters in individual actions without relying on an organization at all. The global reach of the Internet allows for an ease of connection that lends itself to the formation of "cyber tribes," ranging from hobby groups to organic groups of cyber militias. The Forum allows communication, group learning, and allows likeminded people to use cyber-attacks in the name of a political goal or ideology. Cell members are likely to know each other in real life, versus the anonymity of the Forum. Trust is critical, since their activities are likely to be illegal, so a lengthy vetting

procedure naturally limits the size of the group. A more traditional hierarchical structure can also organize a volunteer force, an approach more suited for cohesive groups who have a chain of command in place, for example, the PLA in China and the IRGC in Iran include militia-type units. This model allows for both anonymous and identified membership groups (Ottis 2011).

Cyber Governance

Decentralized nature of cyberspace, making its governance a significant case study on a multi-stakeholder scenario; where, balance of power constantly shifts among the governing partners – ranging from governments and international institutions to private industry and civil society. The participant stakeholders in cyber governance not only vary in terms of their power, influence and standing, but also in terms of their views about the purpose and potential of the resource they hold in common – cyberspace (Jayawardane 2015).

Cyber threats, while certainly more complex, generally thrive under some common conditions. At times, the current gaps in effective governance trip up efficient responses, especially when coordination between different entities is needed; similarly, the variety of potential attack trajectories and technical vulnerabilities complicate policymaking. This complication can be increased when nations are actually competing to advocate their different approaches to cybersecurity; because cyberspace boundaries are not established by the same limits of national sovereignty, accurate responses to specific threats is more difficult. Within the private sector, the adoption of security best practices has been somewhat impeded by the lack of regulatory agreement, which makes

the fast evolution of various cyber threats even more dangerous. And when attacks do occur, the legal ambiguity of cyberspace regulation and policy makes prosecution and accountability difficult to enforce (Shackelford 2014). Thus, establishing cross-stakeholder coordination, institutionalizing cyber norms, and fostering cooperation across all parties involved will effectively mitigate cyber threats.

States seeking a robust democratic cybersecurity governance must address four main challenges. First, states should adopt the development of an internationally consistent legal framework and good democratic implementation practice. Second, they should develop effective mechanisms for oversight, transparency, and accountability. Third, states need to create cybersecurity units to protect public institutions, the private sector and citizens in cyberspace. Fourth, governments must ensure that existing institutional culture, civil management, and leadership attitudes are supportive of the legal framework in its functions and applications. States need to prioritize five tasks to deal with the said challenges. In addition to prioritizing regional approaches to security issues, states should also focus on creating or enhancing professional cybersecurity forces, fostering capable and responsible civilian authorities and civil societies, and giving precedence to the rule of law and protecting human rights (Ball 2006).

To mitigate cybersecurity vulnerabilities scholars and practitioners have offered variety of approaches to conceptualize cyber governance. While there is a general consensus that effective cyber threat management and cybersecurity governance are complicated by the ongoing balkanization of cyberspace and cyber sovereignty initiatives attempts by some authoritarian states (e.g. Russia), the suggested solutions fail to bridge the ideological gap (democratic vs. authoritarian visions), which underlies the initiatives

that might lead to internet fragmentation or a cyber war scenario as Jon Lindsay claims. The contended ground of Internet governance features not only authoritarian actors versus democratic ones; perhaps more significantly, actors diverge along lines of established and modern states, versus newer, less secure states (Nocetti 2015).

Drawing upon Elinor Ostrom's *polycentric governance* model (2010) Scott Shackelford suggests a new approach to modeling cybersecurity through the lens of polycentrism. Case studies on the Internet Corporation for Assigned Names and Numbers (ICANN), and the Internet Engineering Task Force (IETF) provided Shackelford a foundation for analyzing the idea of polycentric governance as a positive development for cybersecurity. In this model he considers a greater role for states in cyber governance, which, in turn, might promote cyber stability (Shackelford 2014).

Similar to Shackelford, Madeline Carr identifies the multi-stakeholder approach a barrier to global cooperation for the internet governance. The existing international power dynamics are only exacerbated by the variety of stakeholders currently involved in Internet governance. Without an intentionally broad dispersal of power, those who already hold power are preferred—typically Western, and especially U.S., governments and companies. A need for diversity in voice and approach is perhaps becoming more essential to ongoing success, as the fastest-growing demographic of Internet users are located in North and South-East Asia (Carr 2015). Contrary to a polycentric governance approach, which emphasizes on a greater role of states, Carr's model recognizes a much broader range of non-governmental actors, in particular civil societies.

Criticizing the liberal institutionalism approach to global cyber governance, Samantha Bradshaw, a researcher on the Computational Propaganda Project at Oxford

University and her colleagues argue that the greater problem of Internet governance used to be coordination; but it has shifted to be defined more and more by challenges to cooperation, foreshadowing a general increase in contention around Internet governance (Bradshaw et al 2015). Drawing on Albert Hirschman's theory of collective action the authors argue that in the face of growing dissatisfaction to the US leadership on cyberspace other nations face three options: exit, voice and loyalty (Hirschman 1970). In the most clear and recent example of an 'exit' response, Iran and Russia announced plans to develop a separate domestic Internet disconnected from the global network. Generally, Western states as well as small states fall into the response of 'loyalty' and support the status quo, while some actors such as China and Brazil signal a voice response – demanding a bolder international status, and possible participation in global cyber governance.

Jon Lindsay's typology of cyber threat narratives explores the types of cyber threats a state perceives. This typology highlights four different types of threat narratives across political, espionage, military, and institutional areas, which overlap makes policy decision making a challenging task. In his systemic typology, Lindsay provides four types of threat narratives based on technological capability and political motivation. According to his typology, a political environment is perceived as either cooperative or competitive, and cyber technology is considered either evolutionary or revolutionary. Whereas a revolutionary perception of cyber technology might result in cybersecurity norm formation under a cooperative environment, it might lead to cyberwar if connected states perceive their environment competitive (Lindsay 2015).

Prioritizing each aspect – political or technological – of cyber threat over the other might lead to deficiencies in another area, which creates some potential dilemmas for states while building their priorities for cyberspace – national security versus global openness. For example, Internet openness promotes economic growth, but authoritarian regimes prioritize political information control over the technical aspect, which might degrade their economic efficiency and also makes them vulnerable to foreign infiltrations. While more advanced countries such as the US benefit from internet openness and enjoy prosperity and economic growth, their critical infrastructures become more vulnerable to cyber-attacks. By the same token, the higher a state's dependency on advanced network systems, the more their military is vulnerable to cyber-attacks. For instance, China might favor "informatization" policy in order to develop its military capacity, even though it is more vulnerable to cyberattack.

While each of the approaches discussed above sheds light on some obstacles preventing the formation of a global cyber governance, their solutions do not address the ideological difference underlying the current tension between the US-led multistakeholder model and the 'cyber sovereignty'-based model sponsored by Russia and backed by China.

2.3 Neoclassical Realism as Theoretical Framework

Over the last decade, cybersecurity has emerged as a matter of high politics; as is clearly shown by range of international events such as the Wikileaks release of classified information, the social media-influenced uprisings in the Middle East, and Russia's disinformation campaign and its meddling in electoral process of the United States and

some European countries. In fact, the US intelligence community included cybersecurity concerns in its annual report since 2008.

Although cyberspace has increasingly influenced transnational social relations, international politics, and global economy, the discipline of international relations has been very slow in starting to deal with the issues of information revolution and its global governance. Majority of prior studies are policy-oriented reports and the application of IR theories in analyzing the information revolution and cybersecurity is underexplored (Cavelty 2007). In other words, there is a lack of research on what Jan Frederik-Kremer, Benedikt Müller, and C. Demchak termed "cyberization of IR", meaning "the ongoing penetration of all different fields of activity of international relations by different mediums of the cyberspace on the one hand, and the growing dependence of actors in IR on infrastructure, instruments, and means offered by the cyberspace on the other hand" (Kremer and Müller 2013, xi).

I take a neoclassical realist stance in this research. Like other variants of realism, Neoclassical realism (NCR) identifies the natural state of politics as a constant struggle between different states over resources for material power and security, however, by its focus on the factors of decision-making and domestic politics, diverges from its intellectual predecessors. While the parameters for a state response can be set by external threats, it is the unit-level factors that characterize the state's response and its setting; for instance, the degree of power the executive branch holds over national security policy, or the degree of power held by specific ideals over foreign policy discourse, may qualify or influence state responses.

Neoclassical realism is a framework, where Kenneth Waltz's structural realist/neorealist rigor and theoretical insight meets Hans Morgenthau's classical realist practicality about foreign policy and complex statecraft (Lobell, Ripsman and Taliaferro 2009). In other words, whereas the international system envisioned by neorealism was formed by the polarity of the Cold War Era, neoclassical realism views international system as a barometric indicator of costs and benefits for various actions; thus, each state's understanding, ideas, and ethics influence how a systemic pressure/change is perceived and processed (Kitchen 2010). While they may consider unit-level variables, both constructivism and various liberal international relations theories have failed to truly integrate those variables consistently. In comparison to constructivist theories, NCR models incorporate the insights from domestic institutions, in which actors not only develop their strategy, but also form their identity based on a desired image (Kaarbo 2003). Unlike liberal institutionalism, NCR does not assume the state as a comprised of a passive collection of institutions, which together serve as a venue for dialogue and competition. At core and in broad strokes, liberalism and realism diverge on their assumptions about whether actors' preferences are shaped by external environmental factors or are defined by the process that forms those ideals. While liberalism assumes that states generally aggregate the demands of various classes and interest groups, Neoclassical realism assumes that national interests are defined by elites and leaders, and that foreign policy is conducted based on those leaders' international perspectives and assessments of relative power and foreign intent; always subject, of course, to domestic ability (Lobell, Ripsman and Taliaferro 2009). Further, Neoclassical realism can be identified separately from other Innenpolitik approaches by its contention that the

international system is the dominant influence over foreign policy. Questions of innenpolitik, including those of domestic politics, state power and processes, leaders' perceptions and the impact of ideas are seen as necessary examination for Neoclassical realists to explain how states react to international environments; however, those variables are considered subject to systemic factors that represent more long-term limits and opportunities for states (Kitchen 2010).

Neoclassical realist theory is seen as 'new' because of its bent toward systematizing the broad insights of classical realism and integrating the explanatory richness of those insights to identify specific influential variables. Neoclassical realism's explanatory power lies in its attempt to explore why states, or the same state at different time periods, respond differently to systemic pressures/changes. Foreign policy is the primary focus of neoclassical realist theories, and as such, they analyze international events through a hybrid standpoint, combining external and internal variables and accounting for both elements of systemic level (i.e. power distribution) and domestic politics (i.e. elite perception) (Ripsman 2011). This theoretical framework has room to explain not only the broad foreign and security concerns of great powers (e.g. China and Russia), but distinctive characteristics of developing countries, divided or failed states, smaller nations, and regional powers (e.g. Iran). A state, in neoclassical realism, might be strong or weak in its relation to society, crucial institutions might operate on parochial or national interests, or the state may be motivated by defense of the regime or of the nation; regardless, the state functions as an intervening variable between the international system and foreign policy (Lobell 2009).

2.4 Cyber Threat Assessment: A Neoclassical Realist Approach

Analysts assemble and interpret information that represents potential threats to a target, a process generally referred to as threat assessment. Potential aggressors range from individuals to nations, and potential targets include nations and their interests, as well as private companies with valuable and confidential properties, major utility providers, and companies with nuclear-related capabilities. A threat assessment process considers the potential effects of an adversary's action, as well as the capability of specific adversaries to exploit vulnerabilities, and the likelihood that those adversaries will take action. These assessments provide essential reading for policymakers, who need to quickly and accurately understand threats and respond to them appropriately (Lin 2012).

Any given cyber threat's potential to reach an appropriate level of political concern is not tied to the development of an appropriate legal or political response; threat responses are so heavily dependent on political policy perceptions and the different roles of government agencies involved in the assessment of cyber threats. While it is the agencies' responsibility to adopt or create actual responses, they are concerned with how cyber threats and incidents are perceived. Cyber incidents may be perceived as predominantly human rights issues (especially regarding data privacy), or as homeland security and/or law-enforcement territory, or as a matter of national security. Legal and political responses to cyber threats must take these perceptions into consideration (Häußler 2010).

Prior Research for Understanding Cyber Threats

Different frameworks and IR-based theoretical approaches have been developed to analyze threats and security in cyberspace. In general, when looking at the scholarship on cybersecurity and threat assessment, we can distinguish three major approaches: first, studies which concentrate on different types of actors, their motivations and respective actions (Kremer and Müller 2014); second, studies which highlight dynamics of cyber governance among broad range of stakeholders (states and non-states) to mitigate cyber threats (Mueller, Schmidt, and Kuerbis 2013); third, studies which address politics and construction of threats in cyberspace (Cavelty 2007). In their contribution, Jan-Frederik Kremer and Benedikt Müller present SAM, a three-dimensional framework, which distinguishes between stakeholders, actions, and motives (SAM), and allows a classification of cyber-threats. SAM enables government to identify whether a threat poses high- or low-level risk to a state's security. In compare to previous models, SAM is a more holistic framework with a one-to-one map between actors, their motivations and respected actions. The main shortcoming of this model is its failure to address public-private partnership responding to challenges directed at the private sectors and the potential role of state (Kremer and Müller 2014).

Milton Mueller, Andreas Schmidt and Brenden Kuerbis research (2013) on networked forms of governance reveals the failure of states and international security organizations to establish themselves as the dominant governance authority. Looking at two case studies – Internet routing security and countering Conficker (a large-scale botnet) – their study shows a networked approach is more efficient for the Internet governance. In practice, private sections, in majority of countries, control information

flow and technical infrastructure of the Internet. These technical communities not only support each other, but also practice through open standards. However, to prosecute cyber perpetrators they reach out to government agencies and law enforcements. One of the reasons that states, and transnational security organizations fail to impose a hierarchical authority is that, in compare to technical/private communities, internet governance is a fraction of states and international institutions concern; thus, a governance regime that was centered around simple coordination issues shifted to a regime that demands not only more complex coordination, but also cooperation among actors. As Bradshaw and her colleagues argue the IR theories need to pay a greater attention to potential structural shifts from coordination to cooperation (Bradshaw et al 2015). Jon Lindsay also argues a major obstacle towards a robust cooperation among states is the lack of institutionalization and norm building in cyberspace (Lindsay 2015).

The last two models utilize a constructivist approach to cybersecurity. First, Myriam Dunn-Cavelty's research focuses on the politics of threat in cyberspace. She takes a hybrid two-level approach – combining international relations and public policy theories – to capture mechanisms of threat politics: securitization (Copenhagen School) and agenda setting. During the first phase, state authorities frame the threat and set it in their agenda; the second phase covers how threat frames changes over time (Cavelty 2007). Second, based on the Barry Buzan vulnerability study (Buzan 2008), Forest Hare (2009) introduces a framework, which incorporates state's military power and socio-political cohesion to understand threats that pose risks to a state's national security. The proposed model strengthens cybersecurity policy development by providing a way to assess underlying assumptions of state actors in order to inform perspectives on various

cybersecurity proposals. By providing a broader context for the assumptions and agendas of actors and stakeholders, the model may reduce or, at least, forecast potential conflicts and dilemmas. Hare argues the stronger a state's military and the stronger its socio-poetical cohesion, the less possible that state's authority securitize the threat. At the international level, collective action demands a coalition of diverse actors to both define and map the way toward the collective "good" for all. The model can assist in identifying the areas of potential agreement or consensus among diverse states, especially where there is a lack of significant alignment between them. A coalition can empower progress by ordering a "securitization alliance" among a small set of states around areas of common ground and then expand it to other actors whose views are not in complete concert with the initial members.

The problem here is that these approaches are not holistic. They do not show how world views (perceived or constructed), agendas, and responses translate into actors' cyber posture and behavior, especially, with respect to states which challenge the status quo and the US leadership in cyberspace. To overcome these deficiencies, I have developed the MCTM framework as an attempt to show how complex domestic political processes in such states (i.e. revisionist states) translate into strategic behavior in response to the emergence and evolution of cyber-threats and the on-going tension over cyber governance.

Multi-tiered Cyber Threats Model

In this section, I develop a neoclassical realist model for identification of Cyber-threats: Multi-tiered Cyber-threat Model (MCTM). Derived from models by neoclassical realist

scholars like Steven Lobell (2009), who focused on state-society relationships and domestic politics for his complex threat identification model, as well as models from Randall Schweller (2004; 2009) and Jennifer Sterling-Folker (2009), who considered more domestic-level ideational elements that influence elite decision-making, the MCTM identifies threats by shifts in both international system and subsystem (regional) as well as in domestic environment. Of course, distinctions between these tiers are rarely clear; various shifts may be the result of action on one level, but the intended target may be on another. Threat assessment requires an understanding of the nested and interrelated nature of threats and connections; a state's or actor's motives and intentions are often far more complex than a single obvious threat might indicate.

At the global level: Offensive realists are often incentivized by the international system to continually seek opportunities to gain power over rivals, or potential competitors through expansionist foreign policies and competitive tactics ranging from outright aggression to actions calculated to counter rivals' progress. However, aggressive foreign policies most often can be traced directly to the idea that expansion is the only way to increase a state's security (Lobell 2009). At the regional level: Significant shifts in power in a region can immediately shift the playing field of threats and opportunities for local states. At the domestic level: It often serves political leaders better to prioritize the ruling regime's survival over a nation-state's, given the high stakes of domestic politics. Balance of power/threat: States balance in response to the shifts in distinct elements of a state's power (i.e. cyber power), rather than shifts in aggregate power (i.e. grand strategy) (Ibid). Cyberspace provides non-state actors and smaller states as well as rising powers with two significant opportunities: low cost of entry and cross-domain retaliation.

Barriers to entry for political actors are so low that low-budget actors such as small states and non-state actors can still have significant influence (Nye 2011). Further, with a cross-domain attack, an actor directs its main power to one domain, while simultaneously finding vulnerabilities in another area (Manzo 2011).

Observers in a threat assessment situation need to be aware of more than simply one play or game. Like chess, actors may be involved in a whole network of plays or even multiple games. If an actor's choices don't seem to make sense in the context of the play, the observer's perspective is likely to be incomplete. There are two key reasons an actor and observer might disagree on why option 'A' is not optimal. In the first case, an observer may become aware of an actor in one arena initially, but the actor is really involved in several 'nested' games in multiple arenas. In a second scenario, also involving nested games, we see a problem defined more by institutional design where option 'A' is also not ideal because an actor responsively innovates to generate additional options to choose from; in effect, changing the rules of the game. Observers in this case may lose the plot, as actors are not only potentially involved in multiple games but playing by a different set of rules (Tsebelis 1990).

The emergence of revisionists powers such as China, Russia, and Iran have been a major security challenge for the United States as well as the Western-led liberal order. Using cyber operations in various ways—from disruption of critical infrastructure and theft of intellectual property to influence citizens and manipulate democratic procedures through sharp power tactics—is fast becoming the preferred path for China, Russia and Iran in their attempts to gain economic, technological, and military advantage over the U.S. and its allies (Coats 2019).

Randall Schweller (1999), a neoclassical realist political scholar whose study focuses on the rise of great and emergent powers, identifies two types of revisionist states: limited-aims revisionists and revolutionary powers; whereas the former seeks "the adjustment of differences" within the existing order, the latter aims for "global dominion and ideological supremacy" (Kissinger 2017, 2). This study presents three cases which represent a revisionist state.[3] While Russia is a limited-aims revisionist state, because it is generally dissatisfied with its cyberspace position, China and Iran can be defined as revolutionary revisionist states, since both perceive that their domestic stability depends on specific changes to the international order, which is U.S.-led and essentially opposed to their core values.

State leadership, with insight from military officials and foreign policy executives, bears ultimate responsibility for national security strategy, including cybersecurity policy, as it sits at the conjunction of state and international system. China, Russia, and Iran face cyber threats that originate from shifts either in the international system, sub-system (regional), or in the domestic politics. The categorical division of systemic, sub-systemic, and domestic power balance into multiple tiers are interconnected and vague. Political elites have an outward focus on the systemic and sub-systemic power balance between states, and an inward focus on the domestic power balance between societal blocs.[4]

---

[3] While there is less consensus within the broader IR community on to what extent China, Iran, and Russia are revisionist powers, there is less doubt on their revisionism in the cyberspace domain. In some other domains, it is possible that US could be more revisionist than China. See: Chan, Steve, Weixing Hu, and Kai He. "Discerning states' revisionist and status-quo orientations: Comparing China and the US." *European Journal of International Relations* 25.2 (2019): 613-640.

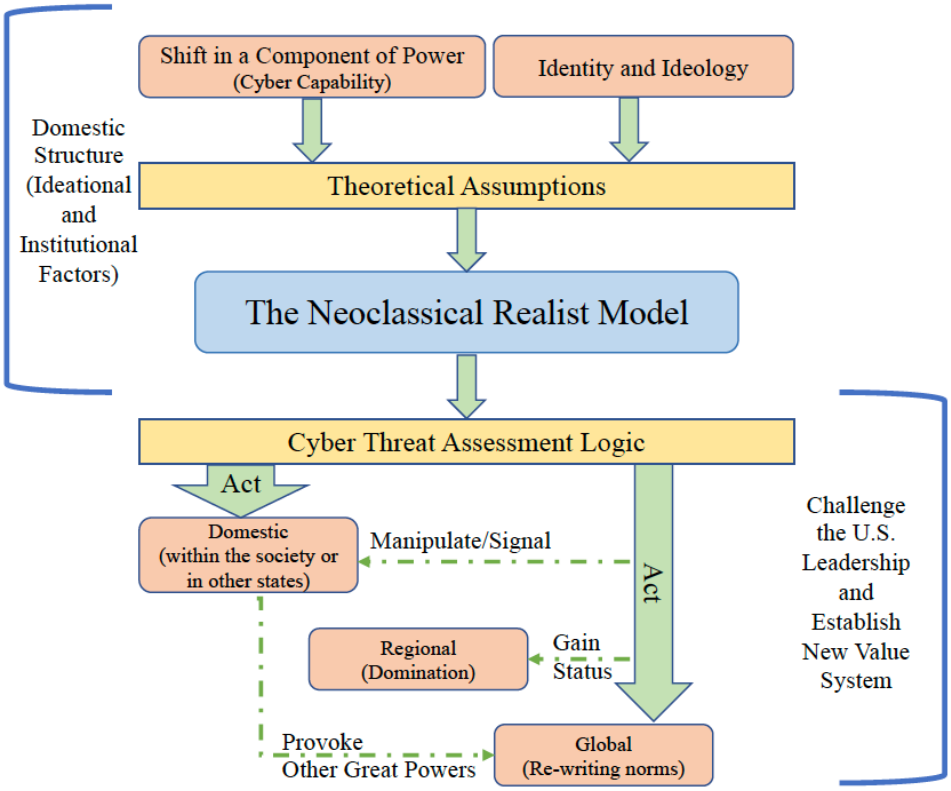
[4] For more information refer to: Lobell, Steven E. "Threat assessment, the state, and foreign policy: a neoclassical realist model." *Neoclassical realism, the state, and foreign policy* (2009): 42-74.

States respond to similar external changes/pressures in varied ways, based partially on the preferences of relevant political and societal actors, as well as on the defining characteristics of society and government. A state's willingness to balance depends on elite consensus and cohesion, and its ability to mobilize resources for this balancing task depends on the vulnerability of the regime/government and social cohesion; which together, these four components – elite consensus, elite cohesion, regime vulnerability, and social cohesion – define the degree of state coherence.

A shift in a component of power (i.e. cyber capability) → elite consensus about the nature of the cyber threat and the degree of elite cohesion → success/failure of resource mobilization as a function of regime vulnerability and social cohesion → continuity or change in cyber policy

An efficient counterbalance response depends on the degree of consensus among elites and societal forces. Any desire to change domestic power balance or the domestic politics of another country can influence the actions of state leadership in how they identify threats and create policy; as Lobell points out, executives are able to act domestically for an international interest, or internationally to achieve a domestic goal (Lobell 2009; Lim 2016).

Figure 3 – Multitiered Cyber Threat Model



Domestic Structure: Ideational and Institutional Factors

Neoclassical realism enjoys a broad ontological variation; some researchers focus specifically on the domestic-level defining ideational elements, like nationalism and regime ideology, while others focus on the domestic politics and state-society interactions – institutional elements. In a neoclassical realist framework, state's responses shaped by a complex array of factors that function as intervening variables, ranging from national identity and regime ideology to status aspirations, state interests, threat perceptions, and bargaining among elites. These intervening variables have borne distinct, if not exclusive, influence over major strategic choices (Kaarbo 2003).

Neoclassical realism approach to power departs from its predecessors; the relationship between ideas as objects with force, and elements of power, in a useful

neoclassical realist approach, would be distinct from the relationship between money and power or military hardware and power, simply by being both dependent and variable, as opposed to being intrinsic and fixed (Kitchen 2010). In ideological-driven states regime's ideology reformulates national identity, which in turn sharpens status aspirations and ultimately state interests, narrows security policy option and help resource mobilization and collective action; Defined by the prism of regime ideology, national identity defines these states' perceived status. Interests irreducibly translate into the goals of ensuring regime survival, countering hegemonic cultural onslaught (e.g. Western), preserving state dignity, ensuring national survival, and mitigating any security vulnerabilities or the U.S. regional influence. Ideational variables collectively depict these states extremely sovereign and independent, ideologically oppose to Western values, in particular with regard to the US leadership, as well as revisionist vis-à-vis the liberal international order (Kevjin 2016).

While ideas help to order the world, they also shape agendas, which in turn shape outcomes. Ideas and beliefs influence politics in different ways—perhaps most obviously through being incorporated into political debate and discourse. Institutions comprised of people drawn together by similar ideology, may also mediate influence over political action. However, influence is leveraged, the use and expression of ideas over time indicates change—whether gradual or expedient—in political rules and norms (Goldstein and Keohane 1993).

Ideational factors are particularly efficient at mobilization of resources, enhanced by authoritarianism, which doesn't face accountability hurdles of political competition and legislature. Still, leadership must identify policy choices by their ideological tags in the

interest of legitimacy (Schweller 2009). The tone of cybersecurity policy, in ideological regimes, is set by ideational factors, which are further specialized and identified by the domestic blocs competing for power, resources, and policy influence. These various factions foster political competition, but the real influence is exerted through the institutions each faction controls – institutional factors. Directions of influence between ideational and institutional elements are inter-sectional, ultimately; national identity is produced by the faction dominating the state at any given moment.

Chapter Three: China
The Emergence of a Cyber "Gardening State"

"The Internet has become the main battlefield for the public opinion struggle. Some comrades say that the Internet is the 'largest variable' that we face, and if we get it wrong, it will become 'a worry in our hearts and minds'".[1]

- Xi Jinping

3.1 Introduction

Since its inception as a military project – ARPANET – the Internet has been an American project. During the last five decades, the United States has not only led the development of the network, but has defined, shaped and internationalized its standards and norms. Yet today, China not only has turned into a rival power competing with the U.S. to lead cyberspace (Segal 2018), but it also overtakes America in regard to international image and global leadership approval (Paris 2019).

A recent study from the RAND corporation illustrates a decrease in U.S. cyber skill within the last decade. The report, which examines the U.S. and Chinese military capabilities in a cyberwar scenario, demonstrates that the U.S. cyber superiority has dropped from a "major advantage" point between 1996-2003 to a "advantage" point since 2010. At the same time, China has upgraded its military from an old-fashioned to a modern force in charge of the nation's cyber operations, and it has expanded its global access by a range of means, such as the One Belt, One Road (OBOR) and Digital Silk

[1] Xi Jinping's address at the National Propaganda and Ideology Work Conference on August 19, 2013. Cited in "Can China Conquer the Internet?", *A ChinaFile Conversation*, December 3, 2014. Available online at: http://www.chinafile.com/conversation/can-china-conquer-internet

Road initiatives, Made In China 2025 (MIC 2025), and the World Internet Conference (Heginbotham et al 2015; DoD 2018).

The collapse of the Soviet Union certainly created an unprecedented shift in international power balance. The previous bipolar system, in the wake of the power vacuum created by the fall of Soviet Union, gave way to a uniquely monolithic gap between the United States and all other great powers. The unipolar system did have some viable peer competitors such as the EU, Japan, Russia, and China; of those, only China's power was on the rise (Krauthammer 1990). China's quest for status and power after a century of humiliation, as well as its preference for a multipolar world system are established trends within foreign policy debates. Scholars have long debated China's political status and whilst they agree on China's multifaceted identity, they differ on which identity – a socialist country, a developing nation, a rising power, or a superpower – is the most significant (Pu 2017). Comparative approaches have ranged from Larry Diamond and Yan Xuetong's perspective that China is already a superpower (Diamond 2019; Xuetong 2011), to Susan Shirk and Randall Schweller's assertion that China's power is still on the rise (Shirk 2014; Schweller 1999). Other scholars view China as a returning power, rather than a rising one (Wu 2007), or as vacillating along the spectrum between a developing nation and a rising power (Pu 2019). As William Wohlforth (2009) argues, China seeks neither a global leadership, nor a dramatic change that upsets the status quo; rather China pursues recognition within the international system. The majority of China's recent initiatives, including China's attempts to establish variety of regional institutions and norms, have roots in the country's demand for standing. For instance, discussing the emergence of the Asian Infrastructure Investment Bank (AIIB), Xuetong

claims, “America did not let China play, so China established its own institutions.” (De Putter 2016).

While there is less consensus amongst academics as well as policymakers on China’s status within the international system and its ambitions for global governance, there is less doubt on its status and ambitions within cyberspace. In other words, experts on Chinese studies agree that a global powerhouse is China’s most salient identity within the cyberspace (Pu 2017). Xi Jinping has vowed (Zuo 2016) to turn China into a cyber superpower by 2050 and, declared in autumn 2017, the Chinese Communist Party’s (CCP) goal to make China a cyber superpower envisions outcomes that would improve both capabilities and influence of China in areas as diverse as domestic control, indigenous technology and global internet governance (Cook 2018b).

China often expresses resentment at what it perceives as preferential treatment of the United States. In order to balance against the US primacy and the hegemony of the Western liberal order, it’s necessary for China to undermine, rather than aggressively challenge, the legitimacy of American leadership. Prior to the Xi era, China’s strategy to undercut America’s global governance mainly remained rhetorical, with low-cost policy implications. The public statements China often makes communicate various issues of vital concern to them, although the method itself may be driven by attempts to impress domestic audiences, gain international political leverage, or both (Schweller and Pu 2011).

3.1.1 Ideational Components

Xi Jinping has surprised China analysts with his bold and effective political moves and policy choices. Five initiatives of his administration stand out in particular: the quick and skillful conclusion of the Bo Xilai trial; his remarkably tough national antigraft campaign; his restructuring of the PLA; and his moves to reform and revitalize China's economy within his vision of "Chinese dream" of a stable middle-class. The last significant initiative is Xi's reframed foreign policy which, while it is increasingly perceived by other nations as assertive or even belligerent, is increasingly seen by the Chinese public through the lens of patriotism. All of these elements reveal Xi's particular skill in identifying potential threats to the CCP, and then turning them to his own advantage (Li 2005). Since his ascension to power, Xi Jinping has advocated for a more explicit focus on the uniqueness of the Chinese system, and the dedication and effectiveness of the party that is transforming China into a modern nation; the additional message that China must not be evaluated by Western standards, but rather on its own terms has been promoted by the CCP for decades.

The current ideological narrative is that the Chinese system has been created in response to China's unique national conditions and it is addressing these with an unparalleled efficiency and excellence that has brought China into the future. Western standards, so the message goes, would not be as particularly effective as Chinese solutions. The ideology of "the West" was originally geographical, then cultural, and following the Cold War, it became a political term. With a bi-polar system established, will the concept as currently used in international relations still apply? This process of bipolarization has included internal schisms in both Western and developing countries.

As a result, political power may no longer follow Western and non-Western designations as much as ideological patterns. The political concept of "the West" will no longer serve as an international relation' objective term when Western nations do not exert unified influence over international politics (Bandurski 2018). Whereas past initiatives were issue-based and focused on promoting a Chinese alternative, the CCP's attempts have recently become more comprehensive, seeking to construct an ideological framework – the China Path – that competes with "Western" models on a grand scale. The key components of this all-inclusive ideology are the Four Confidences, the China Dream, the Community of Shared Future, the Socialist Core Value, the Four Comprehensives, and the Consultative Democracy, which represent the China Path as a canon rather than a collection of principles (see Table 1). Xi has moralized CCP's ideological core and turned it into what Delia Lin and Susan Trevaskes labeled a "virtuous Leviathan"; thus, by their claim of unmitigated central power and supreme moral authority, which requires complete citizen submission to the party, the CCP as led by Xi Jinping is clearly bent on rejecting the principles of Western liberal democracy in order to implement a new governance model (Delia 2019).

Table 1 – China Path Ideological Components[2]

Component	Year Developed	Definition
Four Confidences	2012	Confidence in China's overall path of development, the Chinese system, Chinese theory, and Chinese culture
China Dream	2013	Achieving strong but balanced economic development while restoring China to a respected place in the world
Community of Shared Future	2013	China's official foreign policy propaganda slogan; the world faces many of the same problems, so it needs to work together to solve them

[2] Source: Table 1 (From Ideological Repertoire to Canon). Shi-Kupfer 2016 (MERICS).

Component	Year Developed	Definition
Socialist Core Values	2014	Set of twelve values drawn from pre-modern sources, the Chinese socialist tradition, and reinterpretations of concepts such as democracy and freedom
Four Comprehensives	2014	Policy goals in four areas: development, overall reforms, judicial reforms, and party discipline
Consultative Democracy	2014	Incorporation of different political organizations and societal forces under single-party rule

Economic and political crises in Europe and the United States provide ample opportunity for the CCP to present a framework defined by "good" values—loyalty for the regime—against the backdrop of "bad" Western values. At the center of this framework is the goal of setting out a future development vision for China (Shi-Kupfer et al 2016). Two events facilitated China's ascendance within the international order: First, the 2008 global economic climate convinced the hawks in Beijing that China's economic system could prevail in the financial crisis, and thus that China was ready to play a stronger role in the international scene. A move praised by President Xi, after he took office in 2012, as the nation's "catch up and overtake" moment (McGregor 2017). Second, the US withdrawal from the Trans-Pacific Partnership (TPP) in 2017 provided China an excellent venue to initiate its own regional trade pact and strengthen its dominance in the Asia-Pacific region (Heath 2017).

3.1.2 Institutional Components

The party and the state, in Communist government systems, are often nearly indistinguishable. Not only does the Chinese Communist Party (CCP) appoints virtually all leadership positions, but any major decisions within government bodies must follow

party-established guidelines (Heilmann and Rudolf 2016). When Mao Zedong, in October 1949, established People's Republic of China (PRC), state institutions and organizations were perceived as instruments of the CCP, however, as the state's bureaucratic machine expanded these institutions gradually gained political influence in their own right, especially after administrative consolidation and reform in the field of economy created more autonomy for government organizations (Heilmann and Shih 2016).

While the power of the CCP and the central government are not restricted by China's federal system or any checks and balances mechanism, Government influence in this centralist and unitary context is only limited by direct confrontation from regional special interests or creative challenges to its authority. The PRC political system, with its revolutionary roots, has relied less on bureaucratic policy implementation and more on its power to mobilize and campaign. Affiliation with the CCP may serve to leap bureaucratic hurdles. Political and administrative fragmentation is normal to some extent in China, but under crisis, leadership transforms from a slow-moving bureaucracy to a centralized, autocratic, and powerful mobilization system. Crisis mode can be initiated by disruptions like natural disasters, terrorist attacks, financial crises, cybersecurity concerns, or internal party causes like political unrest, leadership changes, or organizational shifts within the CCP (Heilmann 2016).

Following Schweller's assertion on the rise of great powers, I argue that the important question here is whether China is simply dissatisfied with its position within cyberspace, or if the essential values of China's power are dependent on specific changes to the

existing American leadership in cyberspace (Schweller 1999). China faces a paradoxical situation; on the one hand, the state tries to develop an open network that facilitates global e-commerce and prosper its market economy, on the other hand, it advocates for "cyber sovereignty" and native technologies to maintain the CCP as an overseeing power. As this study will explore, for Chinese elites to safeguard and promote the CCP's core principles, major changes are necessary in the existing cyber order; indeed, a complete shift from global to national-level internet governance. In addition, the study shows Xi's administration is apparently willing and able to balance Western-style governance and the US leadership in cyberspace. President Xi, in compare to his predecessors, has even been able to bring more elite consensus, and to assert CCP's security as an authority over China. Xi also tries to bring more societal cohesion and mitigate the vulnerability of the CCP's rule through a variety of cybersecurity measures as well as initiatives such as Digital Silk Road and Social Credit System.[3]

With sweeping definitions, which perceives security far beyond its official borders, China's National Security Law of 2015 – which is broadest in scope in compare to the one enacted in 1993 – clearly represents China's desire to both control the political landscape and protect the party's position (Mattis 2018). Deputy Director of the Legislative Affairs Commission of the National People's Congress Standing Committee, Zheng Shuna explicitly identifies internal and external pressures, which galvanize the Law's rationale: On international level China concerns its national sovereignty, and on domestic level political security and social stability have highest priority for Beijing.

[3] For more information on the impact of domestic politics and elites' preferences and perceptions on foreign policy behavior see Randall L. Schweller. "Unanswered threats: A neoclassical realist theory of underbalancing." *International Security* 29, no. 2 (2004): 159-201.

Shuna also identified cyberspace sovereignty as a natural extension of geo-political sovereignty, pointing to the critical infrastructure role of Internet technology, as well as the need for securing it, as a rationale for national control of internet activities (Rajan 2015).

The first section will contextualize China's national cybersecurity strategy within its domestic politics and highlight its four priorities in cyberspace: the promotion of "cyber sovereignty", the creation of a harmonious Internet, the increased strength of offensive and defensive cyber capabilities, and the reduction of dependency on foreign technologies. The next three sections will map how these domestic priorities manifest themselves in Beijing's foreign policy, in particular, promoting norms and a governance model in cyberspace which impose no security challenge to China's cyber sovereignty, CCP rule, or its domestic affairs. The final section addresses challenges that China's cybersecurity behavior poses to the United States and tries to offer a few recommendations for US cybersecurity policy towards China.

3.2 China's National Cybersecurity Strategy

Understanding how China defines cyber-related terminologies and its cyber priorities are important first steps to study China's behavior in cyberspace. There is no Chinese equivalent for 'cyber' or its derivatives (i.e. cybersecurity), instead, China uses terms stemming from 'information' or 'network' (i.e. information/network security) to refer to similar concepts (Chang 2014). Envisioning China as a superlative 'information society' has been expressed by its political elites. A common substitute for the term 'information

society' in Chinese literature is 'informatization' also known as 'informationization' (Austin 2014), which Chinese authorities perceive it as follow:[4]

> Informationization is a comprehensive system of systems, where the broad use of information technology is the guide, where information resources are the core, where information networks are the foundation, where information industry is the support, where information talent is a key factor, where laws, policies, and standards are the safeguard.

Chinese authorities have promoted network security technologies through various national initiatives since late 1980s: Management Leading Small Group (1986), State Informatization Leading Group (1999, 2001), and State Network and Information Security Coordination Group (2003). Jiang Zemin, a former general secretary of the CCP, laid the foundations of China's vision of becoming a world-class information society in several major speeches in Beijing in 2000. From the strong support of a vast communication infrastructure, he envisioned broad economic and societal applications to both support and exploit information processing and advanced technologies. Chinese leadership clearly sees informatization as the primary driver of China's overall economic and social development. According to Sha Zukang, the head of the Chinese delegation at the first meeting of the Intergovernmental Preparatory Committee of the World Summit on the Information Society, while information infrastructure is key to future economic progress, each nation deals with the transition to information society uniquely, based on their worldview, social systems and traditions (Austin 2014). Prioritizing security of

[4] State Council Information Office, Tenth Five Year Plan for National Economic and Social Development, Informationization Key Point Special Plans (October 18, 2002), http://www.cia.org.cn/information/information_01_xxhgh_3.htm. Cited in Dean Cheng. *Cyber Dragon: Inside China's Information Warfare and Cyber Operations* (Praeger Security International) (p. 1). ABC-CLIO. Kindle Edition. 2016.

information networks, Sha asked states consider "strengthening control of network security and protection of communications networks through application of laws and regulations" and emphasized on the leading role of states rather than private sector and civil society in the development and management of the information society.[5]

Under Hu Jintao, the CCP leadership expressed greater concern over integration of national security and economic security and the authorities fostered an approach to IT development with a series of rapid infrastructure leaps (Chang 2014). Like his predecessors, President Xi Jinping has expressed his vision to turn China into a first-class information society, but under his leadership, China indicates even stronger commitment to a strategy of comprehensive informatization, seeing the waterfall effect of a strong global information society to China. In 2014, Xi elevated the priority of cyberspace and stressed its implications for China's success in economic, social, political, and military areas (Austin 2014; Chang 2014). The various facets (economic, political and social) of informatization have prompted Chinese analysts and policy decision-makers to identify national security threats as additional victims of informationization (Cheng 2016).

A series of events (systemic imperatives) – the United States' establishment of its Cyber Command (CYBERCOM) unit in 2009, the Stuxnet attack at Iran's Nuclear facility, the Arab Spring, the Snowden intelligence leaks (May 2013), and the U.S. Department of Justice indictment of five PLA officers involved in cyber espionage (May 2014) – triggered Beijing's efforts to take strong measures to centralize operations within the PLA and prioritize cybersecurity laws that increase restrictions on foreign entities and

[5] Statement by Ambassador Sha Zukang, Head of the Chinese Delegation at the First Meeting of the Intergovernmental Preparatory Committee of the World Summit on the Information Society, Geneva, 01 July 2002. Available at: www.china-un.ch/eng/gjhyfy/hy2002/t85538.htm

businesses active in China's domestic economy (Laskai 2017). China's combined efforts to reorganize domestic policy-making institutions and shape the international agenda for cyberspace behavior resulted in a level of cyberspace advancement that Adam Segal labeled it China's cyber-'Great Leap Forward' (Segal 2014b).

In response to the U.S. declaration of cyberspace as a new domain of warfare (2009), China Defense Daily published an editorial in December of 2011, listing objectives essential to an effective command system for cyber-war mobilization in China. These objectives included the development of a central command structure integrating the military, state, organizations, and individuals; the implementation of network warfare training programs for both military and civilian personnel, as well as the formation of PLA units dedicated to network warfare; and the dedication of greater research and development resources to understanding indigenous technologies and developing new offensive weapons (Chang 2014).

Chinese cyber militias as a modern manifestation of Mao's "People's War" doctrine represent one of the strong aspects of recent civil-military development and integration program, which provide logistics support and security for active duty units. Nigel Inkster estimates China's cyber militia manpower at a collective of more than 10 million participants (Blasko 2018).

As Beijing pursues the centralization that increasingly defines the Chinese political system's corporate state model, the CCP does acknowledge that social interest groups are the result of a pluralized society. These societal interest groups – including corporations and universities – form the CCP's main pool for militia recruitment and the CCP, as it will be discussed later (section 3.3 Positive Internet), continues to direct the

behavior of such interest groups to prevent the autonomous action that represents an inherent threat to regime stability. Even today the CCP appeals to the nationalist motivations of civil actors (see section 3.4 Cyber Nationalism and Foreign Policy) in order to draw them under a modicum of state control nationalism represented by organizations such as the Strategic Support Force; Chinese cyber policy is increasingly defined by this dichotomy of empowerment vs. control (Lyall 2018).

In February of 2014, under Xi's rule, the State Internet Information Office underwent a transformation into the more politically powerful Cyberspace Administration of China (CAC). This office, which has declared its mission to turn China into a 'cyber power', is also the key organizer of the World Internet Conference (aka Wuzhen Summit), which is the state's driving force to advocate for China's internet governance model. China's more recent technology measures focus on security, control, and reducing dependence on foreign technology (Segal 2016: 1-4). Xi also undertook the leadership of the Central Internet Security and Informatization Leading Group (aka, the Central Leading Group for Cyberspace Affairs). From the group's inception, Xi presented them with the goal of not just controlling internal infrastructure, but with truly becoming a cyber power, built on a foundation of domestic technology development and infrastructure, high-value culture around cyber technology, strong technological talent pools, and international cooperation (Kshetri 2016). A more direct path to formulating policy is open to Xi through the close links between the CAC and the Central Internet Security and Informatization Leading Group (Economy 2018).

Xi Jinping sees no distinction between the real and virtual worlds when it comes to political values, ideals, and standards, and for this vision to be accomplished means

reshaping the state's relationships with both internal and external society. Both at home and abroad, Xi tries to promote his vision of a 'Chinanet' into a global internet governance model. Domestically, Xi's dialogue toward the Western societal focus on freedom of information is one of values and culture conflict. Internationally, he aligns China with Russia and other nations in a conversation focused on protecting his country from harmful content and retaining the government's right to define what that means (Economy 2018: 57-59).

President Xi's emphasis on Internet security and socio-cultural informatization has impacted not only national security and development, but the daily life and work of the population, as information resources increasingly become a necessity in various fundamental areas of life and, indeed, affect a nation's competitive power in addition to soft power capacity. President Xi stated that "no Internet safety means no national security. No informatization means no modernization" (China Radio International's English Service 022714). Addressing the Small Leading Group (SLG) on Cybersecurity and Information Technology, President Xi listed six indicators of a cyber power: infrastructure, international strategy, indigenous technology, defensive capacity, and controlling the "commanding heights" of cyberspace. Chinese cybersecurity experts argue that these power indicators should be internalized in four levels: cooperation at the international level, providing legal framework and infrastructure at the national level, creation of a competitive market at the societal level, and guiding online culture at the individual level (Segal 2014a).

Nested within its national security strategy, in particular Articles 2, 3, and 25, Xi Jinping and other Chinese elites are pursuing a cybersecurity strategy with the goals of

increasing Chinese cyber power, guarding national sovereignty, and keeping order and security in open cyberspace. The CCP's approach to national security is maximalist and expands its definition far beyond China's borders:

> Article 2: National security refers to the relative absence of international or domestic threats to the state's power to govern, sovereignty, unity and territorial integrity, the welfare of the people, sustainable economic and social development, and other major national interests, and the ability to ensure a continued state of security.
>
> Article 3: National security efforts shall adhere to a comprehensive understanding of national security, make the security of the People their goal, political security their basis and economic security their foundation; make military, cultural and social security their safeguard and advance international security to protect national security in all areas, build a national security system and follow a path of national security with Chinese characteristics.

Two distinct features of this definition are that it identifies security by an absence of threat, not the power to overcome it, a stance that explains the CCP's pre-emptive security measures toward the emergence of any potential threat. The second key feature is that security concerns include the domain of ideas. Placing this second feature in context with the first puts the CCP's drive to alter the world of influence, ideas, and public perception in a new light (Mattis 2018).

> Article 25: The State establishes a national network and information security safeguard system, raising the capacity to protect network and information security; increasing innovative research, development and use of network and information technologies; to bring about security core techniques and key infrastructure for networks and information, information systems in important fields, as well as data; increasing network management, preventing, stopping and lawfully punishing unlawful and criminal activity on networks such as network attacks, network intrusion, cyber theft, and dissemination of unlawful and harmful information; maintaining cyberspace sovereignty, security and development interests.

According to China's first national cybersecurity strategy, released by the Cyberspace Administration of China in 2016, cybersecurity is "the nation's new territory for sovereignty"[6] and its embodiment and extension in cyberspace. The document characterizes China's cybersecurity strategy as follows:

> Cyberspace security (hereafter named cybersecurity) concerns the common interest of humankind, concerns global peace and development, and concerns the national security of all countries. Safeguarding our country's cybersecurity is an important measure to move forward the strategic arrangement of comprehensively constructing a moderately prosperous society, comprehensively deepening reform, comprehensively governing the country according to the law, and comprehensively and strictly governing the Party forward in a coordinated manner, and is an important guarantee to realize … the Chinese Dream of the great rejuvenation of the Chinese nation.

The strategy aims to accomplish the following major tasks, which together address China's major national security concerns:

1. Defend cyberspace sovereignty
2. Protect national security
3. Protect critical information infrastructure
4. Build a healthy online culture
5. Fight cyber-crime, espionage, and terrorism
6. Improve cyber governance
7. Enhance baseline cybersecurity
8. Elevate cyberspace defense capabilities
9. Strengthen International Cooperation

Xi's quest for China's cyber superiority, similar to his national security strategy, is rooted in his conception of 'Chinese Dream,'[7] a brand for his policies, which he defines as synonymous with a renewal and restoration of China to its ancient place of prominence

---

[6] "China Publishes First National Cybersecurity Strategy", *United States Information Technology Office*. Available online at: http://www.usito.org/news/china-publishes-first-national-cybersecurity-strategy

[7] Since its establishment in 1949 by Mao Zedong, the People's Republic of China has experienced three major revolutions: The Cultural Revolution (1966-1976), the Reform Era (initiated by Deng Xiaoping in 1978), and the Chinese Dream (adopted as a slogan by Xi in 2013). For more information see: Economy, Elizabeth C. *The Third Revolution: Xi Jinping and the New Chinese State*. Oxford University Press, 2018.

and glory. The main point is that this new thinking does something that hasn't been done in China since Mao ruled; it identifies a creed with the leader's name as sacred. With power recentralized under Xi Jinping, the supremacy of the party has been re-established. In other words, without leadership from the CCP, the 'Chinese Dream' is meaningless.

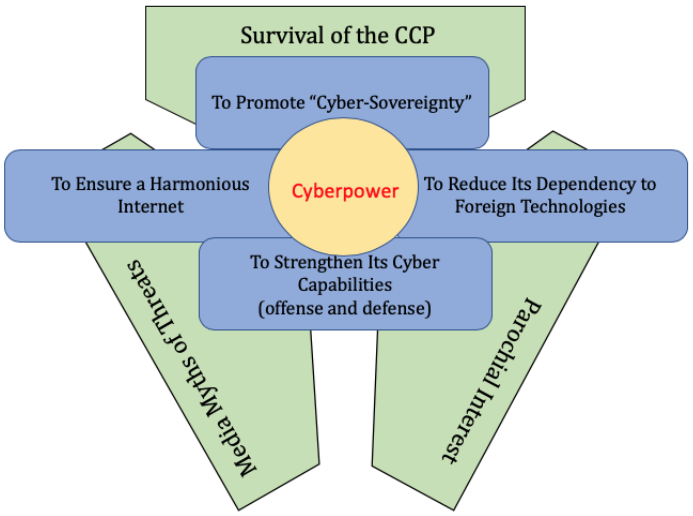
The 'Chinese Dream' of a China revived, powerful, economically prosperous, and socially stable, with a high quality of life for citizens and international prestige for the government provides the north star for all the policy development and direction of the Chinese leadership. China's security strategy, too, is led by this vision. In addition to dealing with threats and reducing risks, the security strategy aims to support revitalization within its fields of influence by clearing potential roadblocks so that the international security environment may be as amenable as possible to the institutional change that will accompany rising Chinese power. In sum, as cyberspace grows as a field of human activity, so national sovereignty grows in order to safeguard, seek governance, and continue to retain boundaries within the international community (Heath, Gunness and Cooper 2016).

3.2.1 Domestic Imperatives of China's Cyber Posture

A growing body of research explores the impact of China's domestic political environment on its foreign policy decision-making process and international status. Primarily domestic priorities do sometimes guide foreign policy, as when China promotes the adoption of only those international norms and rules that do not challenge its domestic agenda, in particular, sovereignty in cyber-space and autonomy in domestic affairs (Chang 2014). Susan Shirk, an expert on Chinese politics and a former Deputy

Assistant Secretary of State, argues that insecure leadership whose security is rooted in the stability of the Chinese Communist Party rule, media myths of threats, as well as parochial bureaucratic interests, rather than military and economic strengths as claimed by some realists (Mearsheimer 2014), are major drivers of China's foreign policy behavior and international identity (Shirk 2014). As this study shows, China's cybersecurity strategy is guided by the same features that power its foreign policy (Figure 4).

Figure 4 - China's Quest for Cyber Superiority and Its Domestic Political Environment[8]



Segal classifies China's major cybersecurity goals into four categories – promotion of cyber sovereignty, creation of a harmonious Internet, increased strength of offensive and defensive cyber capabilities, and reduction of the nation's dependency on foreign technologies – and argues that China's quest for cyber superiority is at the core of these

[8] Source: Source: Adapted from Segal, Adam. "When China Rules the Web: Technology in Service of the State." *Foreign Affairs.* 97 (2018): 10-18; Shirk, Susan. "The Domestic Context of Chinese Foreign Security Policies." *The Oxford Handbook of the International Relations of Asia,* Oxford University Press, 2014.

four national priorities. I will discuss these major cyber concerns in the next three sections.

China's vision of superiority in cyberspace has outlined in full in an article in Qiushi, Organ of the CCP's Central Committee; the plan is to protect CCP rule by increasing domestic internet control, while building up the indigenous high-tech to ensure economic growth and national security. With both of these elements in place, the way will be clear to expand information control internationally (Cook 2018a).

The Internet's potential to facilitate mobilization of dissidents and to challenge the ruling Party's authority explain the Chinese government's grip on strict cybersecurity policies and censorship. The ultimate goal of China's cyber measures is to maintain its control at home and project its power abroad. However, as it will be discussed in the following sections, China's national cybersecurity strategy, at best, serves as a double-edged sword, which might benefit the Party at the domestic level but damage its image internationally.

Guiding online public opinion to create a harmonious cyberspace has a high national priority and it is also part of the CCP's campaign for "self-reform". The Party declares its campaign's fundamental task is "to conduct in depth studies on and implement Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era, forge the political character of loyalty, integrity and a keen sense of responsibility, and unite the Chinese people of all ethnic groups and lead them to strive together for the realization of the Chinese dream." (English Edition of Xinhua 060319) In addition, the Party identifies both "online positive publicity" and social control as essential tandem

forces that guarantee the CCP's ideology remain pre-eminent in cyberspace (Creemers, Triolo and Webster 2018).

Another priority for Beijing is to strengthen its cyber capabilities. China has both defensive efforts – to prevent major informational vulnerabilities – and offensive motives - to define and influence perceptions - in its approach to internal and external security threats, which require a huge expenditure of human and financial capital in its quest for the information dominance. Manipulating netizens' online behavior to mitigate any potential threat to the CCP is one of China's defensive motives to reduce internal threats (Kshetri 2016). For instance, in 2009, the Chinese government issued a mandate requiring the installation of the Green Dam, a filtering software, on all PCs. The main goal of the software was not simply a parental control or security tool, but rather a Great Firewall-based application – The Great Firewall being China's sophisticated national-level filtering system – for censoring political and religious content (Faris, Roberts and Wang 2009). The CCP fights a war on two fronts; they must not only counter foreign opponents, but also strategic unrest generated by internal opponents. The free flow of information—particularly with social media platforms, which increase the potential of cooperation between internal and external oppositions—becomes a strategic threat that makes controlling information of paramount concern (Cheng 2016).

Chinese elites have also engaged in internal security threats through offensive measures. For instance, according to the Berkeley China Internet Project, the authorities filter websites containing words or phrases such as 'freedom', 'democracy', 'China-liberal', and 'Falun' (Foushee 2006: 8-9). With respect to foreign policy, China perceives itself as a victim of cybercrime, which resulted in its defensive motive to help more than

40 countries investigate cybercrimes between 2004 and 2010 (Dai 2011). Following the Stuxnet incident and the Snowden affair, Beijing has shifted its cybersecurity approach toward more offensive strategies (Kshetri 2016).

China's third priority is independence from foreign technologies. Narrowing the gap between China and other developed nations in artificial intelligence, cloud computing, 5G mobile networks, and other areas is a high priority, to be achieved through accelerating domestic innovations, supporting the digital economy, and increasing the global influence of local internet providers (Sacks 2018).

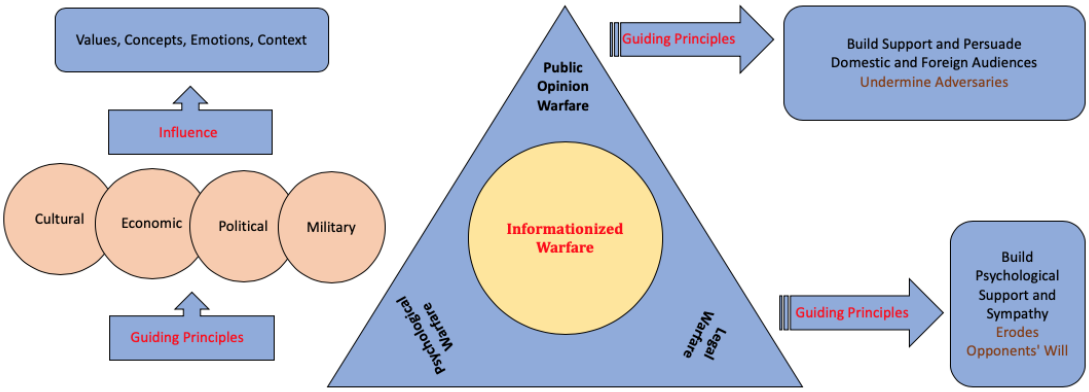
China's ambition to re-write the rules of internet governance marks its fourth national priority in cyber domain. Driven by priorities of economic growth, political stability, and military strength, China seeks to promote the state-led model of internet governance internationally. While it continues to subvert networks for its own uses, including for intellectual property theft, and economic and commerce development, China simultaneously continues to police any online behavior that potentially threatens political or social order (Clapper 2014).

3.2.2 China's Political Warfare

According to PLA writings social, economic, and technological trends are the main indicators of the nature of war and impact the choice of weaponry; thus, an 'information society' demands an 'informationized warfare', which aims at absolute control of information and information flow at any time and place. The actor who retains information dominance then has the ability to force an opponent into a less-influential, possibly reactive mode by their ownership of initiative and the power of information. The

PLA's 'informationized warfare' is echoed in China's political warfare, also known as the Three-Warfare approach (Figure 5) (Cheng 2016). The Three Warfare's initiative targets three specific audiences; the first is China's own domestic public, the second is global civilian populations, and the third is rival agencies geographically centered around the South China Sea. Each audience is specifically targeted to garner support for the Party's narratives, especially the image of China's success, as well as to consolidate power and Party loyalty in each area (Jackson 2015).

Figure 5 – China's Concept of Political Warfare: A Three-Warfare Approach[9]



3.2.3 Multi-Tier Cyber-Threat Model – Beijing's View

China exploits its complex three-warfare approach to respond to any real and/or perceived threat – that originate from shifts either in the international system, sub-system (regional), or in the domestic politics – endangers its national cybersecurity priorities. The MTCT model indicates that it is possible Beijing's external actions (e.g. promoting China Path and socialism with Chinese characteristics as a viable alternative to Western

[9] Source: Adapted from Cheng, Dean. *Cyber Dragon: Inside China's Information Warfare and Cyber Operations.* ABC-CLIO, 2016.

liberal measures) can be doubly motivated by domestic manipulation of political and economic forces (see section 3.3 – Positive Internet). Focusing attention on foreign policy (e.g. anti-American rhetoric) and interstate conflicts (e.g. Taiwan, South China Sea) may instigate the state-positive effects of strong nationalism—strengthening public feeling against opposition (see section 3.4 – Cyber Nationalism and Foreign Policy) and increasing the potential support for expensive strategies (see section 3.3). Additionally, manipulating actors and interest groups located in other states can be part of the motivation for foreign policy implemented by elites (see section 3.5 – Shaping Internet Governance and Norms). Local actions taken by China may also be undertaken with the explicit intent of galvanizing other global actors toward involvement (see section 3.4 & 3.5). The last thing that the MTCT model identifies, is that Beijing's global actions might exert key influence over second-tier states seeking to raise their regional status among competitors (see section 3.5).

I argue that in compare with his predecessor, Xi Jinping, through a series of domestic and international cyber-related initiatives (which will be discussed in the following sections), has successfully created a better consensus and cohesion amongst the CCP elites; thus, China has the "willingness" to balance against the U.S. leadership in cyberspace. The CCP elites, on one hand, have consensus over the nature and extent of cybersecurity threats, and on the other, the CCP's legitimacy, has been restored not only over the PLA, but also over the whole society; hence, an 'ideocratic' configuration, as evidenced by an official account (below), has been 'coerced'. Xi has also successfully created a stronger social cohesion, through introducing a more comprehensive ideology to counter Western values, and has been able to mitigate the CCP and regime

vulnerability through more robust channels such as rally-around-the-flag sentiments and praise for traditional values; thus, China has the "ability" to balance against the U.S. leadership in cyberspace.

> In the past five years, under the guidance of Secretary General Xi's strategic thinking on building China into a cyber superpower, cybersecurity and informatization work has been carried forward steadily, and the top-level design and the overall structure have been basically established. Online positive energy is more powerful, the main theme is more exalted, cyberspace is getting clearer by the day, and national cybersecurity shielding is being further consolidated, while the role of informationization-driven and -led economic and social development is highlighted, and the masses of people have more of a sense of sharing in the results of Internet development.[10]

3.3 "Positive" Internet: CCP's Cyber Strategy for Mass Organization

There is a growing scholarship on the role social media plays in civic activism and political participation.[11] Over the past decade, online communication has fundamentally transformed our societies from 'networked communications'[12] to 'platformed sociality' – where social media platforms are interconnected – and from a 'participatory culture' to a 'culture of connectivity' – "making connections and staying connected online"; thus, social networking has evolved into a new form of social capital, and user-generated content has turned into a profitable enterprise (Van Dijck 2013).

---

[10] Elsa Kania, Samm Sacks, Paul Triolo, and Graham Webster, 2017.

[11] For more information on social media, civil society and politics refer to Bennett, W. Lance, and Alexandra Segerberg. *The logic of connective action: Digital media and the personalization of contentious politics*. Cambridge University Press, 2013; Van Dijck, José. *The culture of connectivity: A critical history of social media*. Oxford University Press, 2013; Dahlgren, Peter. "The political web: Media, participation and alternative democracy." (2013).

[12] Networked communication is defined as "communication that links different media in the search for information and in the exchange of that information with other members in our social networks". Cardoso, Gustavo. "From mass communication to networked communication: Thoughts 2.0." *Lisbon Internet and Networks Institute* (2008), p. 17.

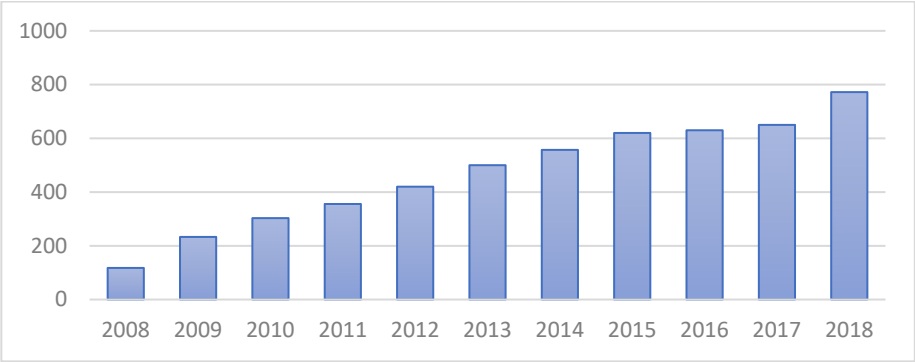
Social media platforms empower ordinary people with more participatory opportunities and challenge political and media establishments. The global access of the internet now been provided with an outlet in the form of mobile and cloud computing, into which outlet are now plugged both personal devices, and critical infrastructure. In 2012, the US Intelligence Community in its threat assessment report stated that "innovation in functionality is outpacing innovation in security" (Clapper 2012, 7).

The relative inexpensiveness of collecting information and ideas through the internet has allowed individual and small group exchanges to flourish, allowing more outsider groups to successfully evade censorship, coordinate political actions, publish information, and even to reach decision-makers with published information (Yang 2016). Internet access has provided new opportunities for Chinese citizens to participate in the political process and challenge the authorities. Empowered via online forums and mobile applications, Chinese 'netizens' may express their opinions on a wide range of topics, from air pollution to China's foreign policy.

According to a recent report published by the China Internet Network Information Center, more than 770 million people have access to the internet; almost 56% of the country's population are online—more than the global average (52%), and much higher compared to Asia's average rate (47%).[13] In 2013, when President Xi assumed office, internet penetration was at 42 percent, compared to 6 percent in 2003, when Hu Jintao became the president (see Fig 6).[14]

[13] https://technode.com/2018/01/31/chinese-internet-users-772-million/
[14] https://www.statista.com/statistics/265140/number-of-internet-users-in-china/

Figure 6 – Internet Access in China (2008 – 2018)



The evolution of the Internet has provided a public sphere where Chinese civil society and the Communist party engage in dynamic contention-participation interactions through grassroots activism and control mechanism (Jiang 2016). It is in online debates where different perspectives can be most clearly expressed on many topics; These social media debates influence the relationships and balances between the state, the economy, and society (Shi-Kupfer et al 2017).

The increase of the Internet's social power in China has allowed greater amounts of interaction between the state and society. The state's manipulation of this new form of interaction is characterized by both fear of population-driven power and need for control—defining characteristics that are also common to other areas of society-state interaction (Breslin and Shen 2010). Chinese leadership invested deeply in their concept of "social stability" after 1989. This banner term was used to spread the word to all citizens that order and prosperity in China depended on the Communist Party's rule (Shirk 2007). In China, the power of social media and mass online participation surfaced during the Wenchuan earthquake in 2008. This new form of connectivity not only facilitates civic awareness and helps in organizing citizens' socio-political mobilization

across the net, but also provides people with ways to engage in online debates according to each person's capacity and personal interest. Chinese netizens' participation in online discussions, in particular via Weibo and WeChat, is issue-based. Chinese netizens' interactions through their personal ties, emotions, and abilities create a variety of 'imagined micro communities'[15], where online users – at home and abroad – show their solidarity and lend their support for particular socio-political issues (Shi 2016).

The early days of the Arab Spring inspired some in China to call for a "Jasmine Revolution" in China. Though the CCP was on high alert for calls to protest and demonstration, no major events occurred. However, CCP identified some valuable insight on how to maintain power from the Arab Spring events. First, regimes that most effectively weathered the disruption of the Arab Spring were those whose messaging stayed ahead of the events on the ground. Secondly, governments who had the ability to shut down social media sites altogether significantly interrupted the unrest. Thirdly, some of the regimes found great advantage in using existing social divisions to keep the populace from significantly unifying. China's predominant Han ethnicity is yet highly divided by region, and the CCP already exploits these cleavages. Similarly, generating a sense of unity among the elite class has also proven to be a commonality among the resilient regimes; this may represent a significant area of weakness for the CCP, which has seen a serious decline in loyalty over the years. With these lessons in mind, the CCP effectively oppressed and contained the 2011 pro-democracy protests that spread across a dozen Chinese cities (Keck 2011).

---

[15] For more information see Anderson, Benedict. *Imagined communities: Reflections on the origin and spread of nationalism*. Verso books, 2006.

To China's leadership, cyberspace is essential ground for maintaining stability, security, and the rule of the CCP (Segal 2017). Chinese authorities' main goal is a "harmonious" and "positive" Internet, which really means one where public opinion, governance, and economic growth are guided and overseen to prevent any undermining of the regime through the spread of any dissenting information (Segal 2018, 10). In 2000, Jiang Zemin, in an international computer conference, while enthusiastically embraced the power of information technology and its development in China, stated, "we advocate establishing an international Internet pact strengthening the safe management of information to give free rein to the positive uses of the Internet" (Wired 082100).

China's political elites emphasize the significant role of media in supporting the CCP's ideology and social control and identify "correct guidance" of public opinions as journalists' highest priority. In 2008, addressing Chinese media outlet, then president Hu Jintao stressed, "the Party's work and the country's long-term stability depend on journalists doing good 'news propaganda work,'' and highlighted the role of media in "consolidating a common ideological foundation for the whole Party and the people of every ethnic group in the whole country to unite in struggle [against the West and propagate socialism core values]" (Congressional-Executive Committee on China 081608). Like his predecessor, Xi Jinping highlights the important role of internet-based media outlets and service providers to disseminate positive information as well as to guide public opinion in the "correct political direction". Internet-literate youth are at the center of the state's propaganda machine to purify the internet: the 50-cents party – online commentators, who are paid the equivalent of fifty Chinese cents for each

comment they post on social media platforms.[16] The goal of this campaign is to shift public opinion through spinning information. The fifty-cents campaigners "trawl the web for negative news and opinion and then refute it with positive information" (Rawnsley 2013).

While the Chinese Communist Party has remained committed to internet filtering and censorship, according to the Freedom House report, online restrictions were much intensified and more targeted after Xi Jinping became the new head of the state. In addition, Xi has urged the Party to not only improve the state's cyber governance capacity, but also to develop a governing network (Xinhua Headlines 042118); thus, the Party successfully institutionalized a pluralistic array for content control, and new actors and content producers have been mobilized. By mobilizing non-party actors such as public relations companies and political content producers, the CCP has found new power under Xi Jinping's administration. The fresh voices and talent have integrated and expanded on the party's messaging, effectively reaching a wider audience, particularly among the younger generations. The change with regard to building ideological strength under Xi Jinping is a greater degree of decisiveness and control; where the previous administration only aimed to prevent dissent on major issues, the CCP currently seeks not just the absence of dissent, but active support and enthusiasm for its vision. The "China Path" vision has driven the most significant change in ideology production since 2013, the unprecedented expansion of research institutions to back the vision in academic terms (Shi-Kupfer et al 2016).[17]

---

[16] "Fifty Cent Party", China Digital Space. Available online at: https://chinadigitaltimes.net/space/Fifty_Cent_Party

[17] Shi-Kupfer 2016 (MERICS).

From the perspective of Chinese leadership, political stability is absolutely dependent on information dominance, and the concerns of *Westernization* or *ideological rifts among elites* are not merely cultural concerns, but indeed threats to national security and power balance. The Chinese government perceives the United States' and European countries' calls for China to pursue greater democratization as part of the West's informationized warfare. Thus, monitoring and controlling the flow of information is one essential aspect of information warfare for the Chinese leadership, a control that forms the foundation for information dominance (Cheng 2016).

All three facets of political warfare—psychological, legal, and public opinion—are decidedly impacted by a state's level of information dominance, but it is especially significant to political warfare. The CCP central committee and the Central Military Commission both guide the political war effort. The most direct route to building persuasive support from any audience is through public opinion warfare, by defending the cause and undermining opposition; thus, seeking to shape perceptions and opinions in favor of the CCP. Public opinion warfare has certainly grown in importance as the reach of media has expanded globally. Not only news media, but literature and the arts, entertainment media, and the rise of user-generated content on the internet can have broad global effects on public opinion, generating psychological beliefs in support or critique of a cause or person – in China's case the party-state (Cheng 2016; Jackson 2015).

After the 2009 mass protest in Western region of Xinjiang Chinese authorities banned the U.S.-based social media platforms such as Facebook and Twitter and removed any references to the protest not approved by the government (Luckerson 2014).

However, the continuing popular demand for online communities, balanced with the Party's desire for control over media, message, and users makes developing Chinese versions of social media sites and apps the best solution for the government (Rawnsley 2015). China-based social media platforms such as Weibo (a microblogging application similar to Twitter) and Weixin (a Chinese WeChat social media app) launched soon after Beijing banned Facebook and Twitter. When it is allowed to flourish without restriction, social media displays the full range of reactions and opinions on the state, good and bad. In democratic states (and with a limited scope in China), there is a tacit recognition by elected politicians that any negative press in the eyes of social media is not a threat to power, unless it gains momentum toward a potential collective action that may generate a source of influence commensurate with that of the state. With respect to the type of speech that generates negative press, "the Chinese people are individually free but collectively in chains" (King, Pan and Roberts 2013, 339).

November of 2013 saw the official Communist Party of China announcement that public opinions on the Internet must be subject to management by the government; President Xi's comments emphasized the necessity of increased "opinion guidance" for new media, especially singling out internet applications Sina Weibo and Weixin, as providers of negative powers of social mobilization through the fast distribution of information (Stockmann and Luo 2017) – in particular, "online rumors" and "harmful contents". Last January (2018), Chinese government ordered Weibo to shut down several of its portals as the authorities believed the Chinese social media giant "violated the country's laws and regulations, led online public opinions to (the) wrong direction and left a very bad influence" and announced "the measures were aimed at maintaining

'social stability'" (Deutsche Welle 012818). With the goal of shaping the perceptions and opinions of both a larger public and that of major decision-makers in a given situation, successful public opinion warfare must be nuanced and targeted toward three audiences; one, the general civilian population, the constituency of the adversary, and neutral parties or organizations, including third-party constituents (Cheng 2016).

The younger generations find it a natural form of socialization to connect with people online, as well as to construct and express social and political identities through social media communities; a reality that made the youth population the first demographic target for Xi's ideological campaign. In 2013, just a few months in his presidency, addressing the party leadership, Xi warned about 'seven political perils' in an official statement. Soon after, the Party circulated a list of seven taboo topics including "citizens' rights" and "press freedom" among academia and media outlets (Schenkkan and Repucci 2019). Ideological concepts including constitutional democracy, civil society, and Western journalism were mentioned in the document identifying ideas which undermine the regime. The document, published in April of 2013 and titled *Communique on the Current State of the Ideological Sphere* (aka Document No. 9), closed with the argument that these concepts should be given no opportunity to flourish in discussion. The document instructed the Party officials to counter the spread and promotion of these seven destabilizing currents in the society[18]:

1. Western constitutional democracy
2. Universal values
3. Civil society
4. Neoliberalism

[18] "How Much Is a Hardline Party Directive Shaping China's Current Political Climate?", *Document 9: A ChinaFile Translation,* November 8, 2013. Available online at: http://www.chinafile.com/document-9-chinafile-translation

5. Western style journalism
6. Nihilism
7. Criticizing reforms associated with ‘Socialism with Chinese Characteristics’

Ideological education was at the core of Xi’s campaign to both battle the threat of Westernization and to re-establish the authority of the Party within the society at large. University campuses and the Chinese Academy of Sciences (CASS) were among his first targets. Xi instructed the Communist Party branches across campuses for a more robust involvement in students’ education and promotion of socialism (Economy 2018, 38). In 2014, Zhang Yingwei, a member of the leading Party members’ group of CASS, during an official visit, blasted some of his colleagues for ‘using the internet to promote theories that played into the hands of foreign powers’ and complain about some of his colleagues’ ‘collusion’ with their Western counterparts (Wan 2015). A few months later, *Liaoning Daily*, a Party-affiliated newspaper, criticized instructors for spreading negative sentiments about Chinese authorities within academia and warned about three ideological-based issues in crisis in China’s classrooms: underestimation of Chinese Communist Party’s theoretical and ideological innovations; praise for Western political system such as its ‘separation of power’, rather than embracing China’s political system; and the lack of emotional fervor for political and social concepts with ‘Chinese characteristics’ (Bandurski 2014).

Since its inception in 2014, the Cyber Administration of China (CAC) in partnership with the Ministry of Education has held the annual Cybersecurity Week to raise awareness about threats and policies related to the cybersecurity. The theme for the 2016 program was ‘Cybersecurity for the People, Cybersecurity Depending on the People’, which aimed at promoting a ‘healthy’ society-centered cyber culture as

mandated by the country's first National Cybersecurity Strategy published in 2016. In his opening remark, Liu Yunshan, the Propaganda Secretary, emphasized the need for developing a more 'positive' online culture (Bandurski 2017):

> The masses of internet users must abide by the law in going online, acting in a civilized manner online, being positive practitioners of our nation's cybersecurity. We must strengthen construction of online content, foster a positive and healthy online culture, and develop and expand online positive energy, further cleaning up the online space.

The integration of mobile and cloud computing in Chinese netizens' daily activities, in particular the ability to attach audio and video files in instant messaging, generated a new type of activism, the main characteristics of which are 'political jamming' and 'crowd-enabled connective action'. Some Chinese activists use the immediacy of social media to protest and document injustice in real-time. That same direct access also allows activists to construct their choices, protests, and challenges in a very personalized voice and experience (DeLisle, Goldstein and Yang 2016).

For instance, Chen Guangcheng's revelation of brutal forced abortion and sterilizations, conducted under China's one-child policy, earned him a five-year prison sentence, as well as ongoing house-arrest following his completion of that sentence, after he was convicted on a charge of "blocking traffic". Supporters of Chen's actions used political jamming – viral visual techniques – to draw attention to the case, distributing decals featuring Chen's image modeled after the Kentucky Fried Chicken logo, a popular U.S. chain in China. His supporters also created websites populated with thousands of their faces posed in a Chen-style dark glass. According to well-known blogger and social media expert Wen Yunchao, when protest campaigns succeed in going viral, the risks of showing support for a controversial person or subject are mitigated for the average

participant, as well as being more effective at evading censorship. He believes that if the major Chinese social network, Weibo, continues to develop, we will see much more of this grassroots-style change being driven by newer media (Moore 2012).

Weibo/WeChat celebrities also play an important role in the evolution of China's online culture. These social media celebrities form a growing community of microblog account influencers defined by the term 'Big V' for 'verified account'. These influencers are tantamount to celebrity bloggers, with their work being read, discussed, and shared by fans (and/or critics). As much of the content is at best, critique, or at worst, ridicule of government or policies, the Communist party spends some significant energy suppressing these voices since President Xi took office. While government officials justify censorship on the basis that many of the accounts are 'toxic lies,' activists protest that both honest and dishonest criticism are suppressed with no discernment as to which is which (Buckley 2013).

A key underlying logic behind the Party's brutal measures against social media celebrities is that the latter group has been entered in the former's zone of authority. The concept of "shared content" is one that the Chinese Communist Party seeks to control, and "Big V" verified influencers, who have the power to decide what symbols and discourses may become widespread cultural conversations, may become targets. Dialogues on Weibo, though, seem to have taught something different to government authorities, who have increased attempts to suppress celebrity users, an action that has also unintentionally silenced many users who could provide the organic, measured commentary that might be valuable to the Party officials (Schneider 2017). Such actions show compliance with strategic objectives outlined in the state's cybersecurity strategy –

protect national security and build a healthy online culture – as well as its conformity with Document No. 9 directives.

3.3.1 China's Social Credit System

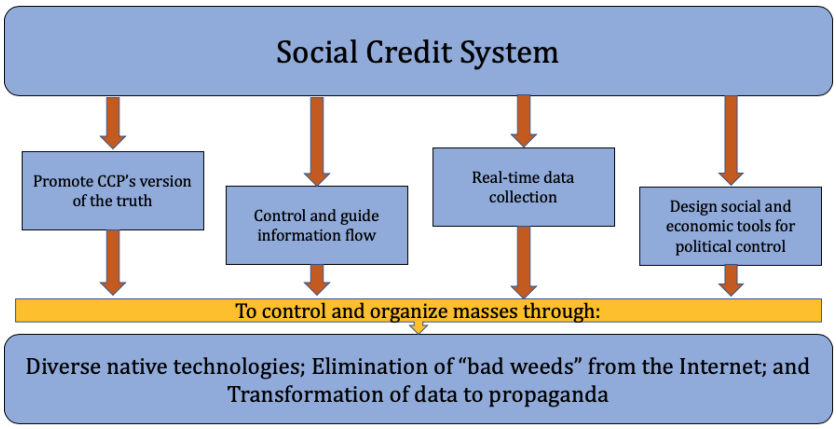
Another mechanism for social control in China is the social credit system (SCS), which scores citizens and organizations on tracked behaviors, resulting in real-world consequences and shaped behavior. First emerged in 1990s as a financial credit system – similar to the credit system in the United States – this system, since 2014, has turned into a complex state governance apparatus advancing China's national security priorities. In particular, the system helps Beijing in creating its imagined "harmonious" society in both real world as well as in cyberspace, and it also helps China to reduce its dependency on foreign high-tech products (see Shaping Internet Governance and Norms).

The SCS is the posterchild for what the Chinese government sees as a process of informatization in governance, with its use of information technology to transform the methods used by Chinese government authorities to manage both state and society. China's Credit System is framed as a set of mechanisms that reward or punish actors for legal or moral infractions, covering economic, social and political conduct. Its logic and functional design reflect China's political tradition; firstly, in the hierarchy of order, where the most important are shown first, and the idea that social morality is a State responsibility in addition to legality. Additionally, the positivist view of social reality based on systems theory is on display, which indicates that society can be understood and engineered through a holistic, scientific approach, blurring the boundaries between state and society, public and private spheres (Creemers 2018).

The political uses for the regulations implemented via social credit system might seem to be a separate concern than the ideal use of credit scores to develop trust and encourage moral behavior, but in China that is not true. Trust and morality encompass dual meanings; where one side focuses on the reliability of an individual or entity, the other is focused on securing CCP's authority and control; the purpose of both terms is rooted in the party's definition, and met when they result in increasing the capacity for the CCP to reliably govern (Hoffmann 2018).

This system will begin expanding to track citizens globally, as well as tracking the behavior of international companies with interests in China, with the results of shaping the behavior of not only their own citizens, but that of international companies and employees; corporations may be fined, face increased interest rates, or even have product blacklisted in consequence of a low social credit score (Grothaus 2018). China's Social Credit System increases the power of state to the extent that resembles a modern utopian state in search of its perfect society as described by both Zygmunt Bauman and Michel Foucault; the CCP's focus on elimination of "bad weeds" from the internet assimilates Bauman's "gardening state" and its organized control over not only the Chinese population but "a global mass" likens Foucault's "biopolitics" (Figure 7).

Figure 7 - China's Social Engineering and Biopower Projection[19]



The social credit system, aided and abetted by technological advancement in data collection, help the Chinese state with controlling discourse and defining truth—at least, the party leadership's version of it. Real-time data collection allows for integrating information from various market, government, and social/civilian sources, increasing the state's capacity for awareness, anticipation, and resolution of problems or threats. With the online ability to transcend geographical borders, decision-makers have greater awareness of the impact of social and economic solutions, and a greater ability to enhance political control as an aspect of every solution.

Improvement of both soft power ability and international influence, as well as establishment of an international credit rating system were stated goals of the Planning Outline for the Construction of a Social Credit System (2014-2020) documentation. While other international systems such as Standard & Poor's, prioritize excellent credit ratings, state security was still first in priority for the CCP's planned SCS. Beyond just protecting domestic and foreign security interests, however, this system is predicated on

[19] Source: Adapted from Hoffman, Samantha. "Social Credit: Technology-Enhanced Authoritarian Control with Global Consequences", *Australian Strategic Policy Institute*, Policy Brief No. 6, 2018.

protecting the ideological space inside and outside the CCP, both domestically and internationally (Hoffmann 2018).

The Social Credit System is still developing, but prior abuses in Xinjiang might portend negative practices; data collection creates a "trustworthiness" rating on citizen behavior, both online and offline. Activists who have been blacklisted for any kind of government criticism already report significant restrictions on their freedom of movement, leaving the door open for the System to exert punitive or repressive measures (Schenkkan and Repucci 2019).

3.4 Cyber Nationalism and Foreign Policy

From the turmoil of the Cultural Revolution, Deng Xiaoping's leadership opened a new path to economic reform and international relations. Much of the change and reform was brought about by focusing on what were called the 'Four Modernizations' – agriculture, industry, national defense, and science and technology. The secondary effect of the success of this modernization was the subsequent revolutionary transformation of the whole economic and political system (Economy 2018: 1-6). Deng's "24-character strategy" has guided China's foreign policy since 1990. His doctrine, which emerged in response to both international reaction to the 1989 Tiananmen Square crackdown and the collapse of the Warsaw Pact, provided necessary measures on how China should safeguard its national interest and project its international image. Deng advised Chinese elites to "observe calmly; secure our position; cope with affairs calmly; hide our

capacities and bide our time; be good at maintaining a low profile; and never claim leadership".[20]

During his tenure, Deng initiated a pragmatic phase in China's foreign policy and the centralization of the Mao government under an elite small group of leaders succeeded by a more dispersed model (Yang 2016). One of the key characteristics of post-Deng politics is the rise of new actors in China's foreign policy. Widespread corruption, ideological disillusionment, declining power of the Communist Party on one hand, and Deng's economic reforms, limited political openness, and collective leadership approach on the other hand, paved the way for gradual shift in China's foreign policy (Kurlantzick 2011). With a greater number of state departments involved in government, and a system of government-led academic and civil society established, the vision of a more democratic, institutionalized, and scientific Chinese foreign policy decision making has been realized (Yang 2016).

The Reform Era broadened a range of social forces that presented obstacles to the CCP's ability to easily control information. The increase in individuation and global connection has equally increased the complexity of levels of control, as it has dramatically changed not just broader culture, but individual life and personhood in contemporary China (Rudolph 2018). In addition, Deng's successors' lack of military experience and a wide-ranging authority, as well as the weakening of the Communist Party elites, resulted in an increase in military's political intervention. As China's

[20] https://www.globalsecurity.org/military/world/china/24-character.htm

military strength has improved in recent years, the PLA's top officers have become less willing to show deference to the Communist Party's civilian leaders (Kurlantzick 2011).

Socialism's decrease in ideological popularity prompted the party to turn to the ideological power of re-emerging Chinese Nationalism narratives as a method of gaining public support. Nationalism's natural need for an ideological opponent saw an increase in focusing on the West as a constraint on Chinese success in educational materials and propaganda. As the Party's ideology shifted to this new seat of power in a nationalist narrative, seeking to fill the ideological vacuum in the wake of Communism's broad collapse in the 1980s, a subtle repositioning was needed to present the party itself as the legitimate and stable political force responsible for rebuilding a strong and prosperous China. This narrative has dominated Chinese nationalism since the early 1990s (Stratfor 100412).

In post-Tiananmen protest, the three propaganda pillars revolve around economic development, strengthening the legitimacy of the CCP, and uniting citizens around national identity. Official propaganda uses historical themes of victimhood and a deep desire for status and superiority to influence (Rawnsley 2013). The current Nationalistic rhetoric in China is shaped by a nostalgia for the lost fame of its past glorious civilization, paralleled by a sense of victimization from a century of humiliation at the hands of the West and Japan, and that narrative is part of the Chinese core of identity (Bajoria 2008).

Terms such as 'invigoration', 'rejuvenation' and 'national rebirth' have often been used by Chinese leaders to remind the people of their glorious past and the strong ties between ancient and modern China, thus helping them embrace new changes

(Economy 2018). Chinese officials preferred term for nationalism is *aiguozhuyi*, literary "love the State-ism". A popular nationalism took place in the wake of the publication of an ultra-nationalist book written by off-duty policy-makers, titled 'The China That Can Say No.' A collection of essays comprised of denunciations of the Western disdain for China as well as the importance of China's continued global presence, the book remains highly influential in Chinese foreign policy thinking (Tiezzi 2014).

However, Xi and his administration's approach to foreign policy and nationalism diverges from that of preceding governments. With regard to China's international status the current administration signals a departure from Deng's "low-profile" motto. Addressing the Party in October 2017, President Xi announced, "it is time for us to take center stage in the world and to make a greater contribution to humankind," he emphasized that the nation has been "standing tall in the East", but also that its economic model, centered on socialism with Chinese characteristics, is a "new choice" for developing countries (Clover 2017). With regard to nationalism, Xi's predecessors' rhetoric were pragmatic and domestic-oriented; Jiang's plan focused on domestic development, increased foreign participation in China's market economy, and a sort of low-profile foreign policy very similar to the principles Deng advocated. Similarly, Xi's "the great revival of the Chinese nation" was a socialist-leaning agenda to promote a modern society with a moderate economic development as a goal by the mid-century (Chubb 2012).

One factor that many outsiders don't realize is a major contributor to the Communist Party's power is the support of the middle class, which has also influenced the more aggressive foreign policy. Middle class support for the CCP, even today, is

earned more by co-option than control (Kurlantzick 2011). Some elements of the rise of Internet technology over the last twenty years have outpaced the party's control, allowing nationalists certain outlets for venting dissent and sharing information. The freer flow of information permissible by the internet has also allowed more contact between Chinese citizens and the huge population of expatriates (Bajoria 2008).

As an ideology, however, nationalism's powerful capabilities to mobilize action and form strong community around the ideal nation can easily turn into fanaticism that may threaten the very leadership that sparked its flames, should they be seen as weak (Shi-Kupfer et al 2016). The influence of online technology combined with a grassroots nationalism have generated cyber nationalism as an important drive for Chinese policy processes. Online Chinese nationalism has created a new identity across Chinese society that perceives China very "different", one might call it "Chinese Exceptionalism" (Breslin and Shen 2010). Foreign affair information, in particular, is circulated in China through social media. The passion of nationalist sensation is such that the individuals who track and share information often exert political pressure on the government to respond publicly (Yang 2016).

Nationalism in China's cybersphere diverges along two major ideologies—a state-sponsored patriotism, and the unsanctioned, non-governmental, reactionary grass-roots nationalism that has populated China's online network since 1994 (Wu 2007). While the CCP brand of patriotism continues to seek ideological leadership, various ideological clusters of community form over elements of patriotism and debate the merits of a uniquely Chinese nationalism and global power trajectory. Some of these clusters

have named identities; The Party Warriors, China Advocates, Traditionalists, Industrialists, and Flag Wavers (see Table 2).

Table 2 – Major Online Nationalist Groups and Their Ideological Proximity with the CCP

Group	Description	Support for CCP
Party Warriors	Diehard supporter of the party	Complete support
China Advocates	Modernist	On China's Path
Traditionalists	Confucius-base	On traditional values
Industrialists	High-Tech equates global leadership	On technological innovation and industrial projects
Flag Wavers	Hyper nationalist	On strong assertiveness on the international stage

A spectrum of ideological representation runs from the group called Party Warriors, who represent a close affiliation with state and party ideology and CCP policy, to the Flag Wavers, a group which critiques party policy in dealing with ethnic minority unrest and for being too accommodating in international foreign policy. The groups arranged between these two extremes often separate on particular issues and approaches; both China Advocates and the Traditionalist groups approach supporting the CCP's rule in different ways. While the Chinese Advocates seek a modern approach to legitimize the CCP's rule, Traditionalists draw from Confucius' teachings as a foundation for the same goal. CCP policy, to industrialists, is defensible when it prioritizes industrial and technological advancement (Shi-Kupfer et al 2016).

Much as the CCP might seek expressive sanitization, the Chinese people find ever-new political forums where they can creatively dodge censorship. A recent designation is *xiao fenhong*, meaning "little pink," a negative term for young nationalists using the internet to whip up extreme patriotism. These "little pinks" represent an especially sinister trend for those who see parallels between Xi Jinping's leadership and that of Mao Zedong. The rage and violence which fueled the Red Guards at the inception

of the Cultural Revolution see disturbing echoes in the ugly trends of the increasingly uncivil discourse of this patriotic faction (The Economist 2016).

Nationalistic fervor among citizens can spark strong responses to any geographical region, but Taiwan, Japan, and the United States are the top targets of online nationalism in China. China claims sovereignty over the country of Taiwan, which rejects the claim. The Sino-Japanese war led to passionate anti-Japanese sentiments for many citizens, and anti-Americanism is seen as almost necessary to socialist revival and continued socialist success. There is a somewhat-parallel relationship between how nations ally themselves with the U.S.-led universal liberal norms, and how those same nations are perceived or depicted in Chinese communities. A certain resentment is often reflected toward the easy entitlement of U.S./Western ideals, interests, and values in online communities. The underlying acknowledgement of inequity reflects anger toward an international system that, at the expense of emerging or developing states, favors Western states' interests. China's perception of its own work in international relations is unique from the Western perspective, a difference that can be seen in China's dealings with Latin America, where China sees itself as a partner with a similar history of subordination to Western powers, versus its interaction with African and Southeast Asian nations, where China clearly indicates a sense of superiority and dominance (Breslin and Shen 2010).

Cyber-nationalism as a reaction to Western action can be tied to the 1999 U.S. bombing of the Chinese embassy in Belgrade. While the military action was identified as a mistaken target by the U.S., three Chinese citizens were killed, and several others were injured. The incident resulted in several cyberspace reactions, including attacks on the

White House website, and the U.S. embassy in Beijing's website, where the homepage was hacked to read 'Down with Barbarians!' More nationalist cyberactivity occurred in 2001, when a U.S. surveillance plane collided with a Chinese jet fighter and following various controversial Western media outlet stories or business decisions (Wu 2007; Yaling 2010).

More modern reasons for cyber-nationalism include the US-China trade war, which has predicated a surge in Chinese nationalism in response to 'American bullying' through tariffs and stalled trade talks. President Trump and American trade demands are being panned by the official media, while Beijing has tightly controlled the news coverage in order to prevent any backlash in public opinion. No independently-generated material is to be published by either traditional or online media, only official-channel content is allowed, according to industry insiders (Hernandez 2019).

> Urgent Notice from the Ministry of Public Security and the Cyberspace Administration of China: Local public security bureaus and internet management departments, upon receiving this directive, immediately organize personnel to control and delete rumors related to increased American tariffs on China. Violators will be dealt with seriously (Rudolph 2019).

Xi Jinping's effort to establish and enforce a national discourse and a unifying ideology is unparalleled amongst post-Deng Chinese leaders. Terms such as "China's Path" and "The China Dream" ideologically represented the strength of a globally-adept, Chinese-led alternative to capitalism and Western liberal democracy (Shi-Kupfer et al 2016). Lu Yunshan, as propaganda chief, to re-enforce Xi's Chinese Dream moto suggested the creation of a "spiritual civilization" (Rawnsley 2015). In February 2014, President Xi ordered the establishment of the Chinese National Security Commission (CNSC). Broad goals for the commission included power consolidation and the long-term maintenance of

peace and stability under the banner of "Community of Shared Future"; goals which soon became defining ideological points in Chinese foreign policy (Yang 2016).

3.5 Shaping Internet Governance and Norms

The current liberal world order is a complex system of alliances, institutions, and norms. Since 1945, a coalition of state powers, legal norms, and public-private partnerships have been at work to expand both the order's and the United States' geopolitical influence. Less than a hundred years after the United States helped to usher it in, the order faces internal fracture from populist, nationalist, and authoritarian forces, as well as increasing external challenges from revisionist powers like China (Lind and Wohlforth 2019). International norms led by Western liberalism are giving way to a stage where international norms are unworthy of respect, and overall the international system is shifting away from a Western-centered model to one where redistributed power fuels an international system that is not quite ready to accept a non-hegemonic form of leadership (Kynge 2018).

Many Chinese sources, both official and non-official, argue that U.S. dominance over cyberspace and Internet-based technologies and infrastructure is unfair to the global balance of cyber-power and identify American leadership as "a source of instability and potential danger," a defense perhaps prompted by China's ongoing dual concerns over domestic instability and securing the CCP in power (Swaine 2013, 5). China, in order to survive, has had to adapt and be smart about acting on its dissatisfaction with the order. At home, China has insulated its population from external influences through information

manipulation, media control, and securely monitoring its citizens (Lind and Wohlforth 2019).

China has also taken some recent strategic steps to bring standards and practices previously kept private into the international public view publishing details of their vision in presidential speeches and in party policy journals. The boundary between domestic and international normalization processes is quite porous; entrepreneurship in various ways can function to transfer international norms to domestic acceptance, and vice versa. A norm reaches a tipping point once entrepreneurs have driven adoption to a critical mass of participants. Prior to this tipping point, normative change is slow, unless there is support from a domestic movement. Once the threshold is reached, adoption of the norms accelerates naturally (Finnemore and Sikkink 1998).

Xi Jinping's plan to make China a cyber superpower was presented in 2017 at the CCP Congress, outlining a suggestion that other countries who prioritize independence and yet wish to speed up development might benefit from policy modeled on China's internet governance (Shahbaz 2018). China has step up its efforts to legitimize and develop the rules of the game for cyberspace through a range of international/regional institutions, events, diplomacy, and initiatives; thus, China has "innovatively" engaged in a "nested game of institutional design" to increase the number of competing alternative models (Tsebelis 1990, 8). Some global initiatives have been raised through the UN, but mainly through series of on-going state-led programs and initiatives – Wuzhen Conference, Made In China 2025, One Belt One Road/Digital Silk Road, and Social Credit System – Beijing tries to accomplish three agendas: First, mobilize enough state participants to normalize its own Internet governance model; thus, advocate not only for

competing norms and standards, but also its own world image. Second, to establish China's superiority in Southeast Asia and expand its global influence as a preeminent powerhouse in cyberspace as well as high tech industries.[21] Third, all of these initiatives are in line with China's cybersecurity priorities.

According to the Wu Ying deputy director of the Shanghai Foreign Studies University's international public opinion center, just three steps can create a better opportunity for China's right to speak internationally: First, that Beijing should be more aggressive in setting international discourse. Secondly that, Western Media's interpretation of Orientalism and "responsible power" need to be interrupted or broken down in order to free up space in the international discourse for China. And thirdly, researching Western media and watching for feedback on China's shaping of public opinion should also be a strong priority for the state (Mattis 2012).

The United Nations: Since 2015, Chinese diplomats doubled down on their negotiations to prevent UN Internet Governance Forum (IGF) to include "freedom of expression" and "free flow of information" in its final draft report. While the U.S. prefers a multi-stakeholder approach to governance, China's preference for a multilateral approach represents a fundamental difference between the two nations. In short, a multi-stakeholder model values consensus from civilian, corporate, academic, technical and governmental societies on governance, while a multilateral model values a more top-down approach where state leadership provides guidance for other stakeholders to follow (Levin 2015). In the case of a multilateral UN approach, China would see two immediate

[21] Office of the Secretary of Defense. "Military and Security Developments Involving the People's Republic of China 2019", Annual Report to Congress, 02 May 2019.

benefits; first, state interests would be prioritized over those of individual technology companies and civil groups. Secondly, China would have access to mobilizing the influence of developing countries who are also interested in controlling free information flow through the Internet (Segal 2018).

Wuzhen Summit: Following the Global Conference on Cyberspace (GCCS) in London, UK, in 2011 and similar events in Hungary (2012), and South Korea (2013), China hosted its own conference on cyberspace governance in Wuzhen in 2014. According to Wang Yukai, an academic and a member of the National Informatization Expert Advisory Committee, for China to turn into a powerful player in cyberspace realm, it is necessary to develop a "clear international strategy that lays out priorities and defends China's right to have a voice on cyber issues" (Segal 2014c).

In December 2015, President Xi Jinping addressed the second World Internet Conference held in Wuzhen. Expressing his concerns over the current cyber governance model, Xi advocated for his concept of "cyber sovereignty" (BBC 121615).[22] He argued, "the existing cyberspace governance rules make it difficult to reflect the will and interests of most countries," and urged the participant countries to respect each other's internet governance approaches.[23] China hopes to turn Wuzhen into the Davos of cyberspace forum (Segal 2015) and Xi's remarks on China's historical mission and "the positive transformation of the Internet global governance" echoed Beijing's international standing and vision. At the concluding session, China proposed the Wuzhen Initiative, in which

[22] Available online at: https://www.bbc.com/news/world-asia-china-35109453
[23] For more information on "Promoting the Reform of the Internet Global Governance System is China's Mission" see the corresponding blog entry posted on Cyber Administration of China's site. Available online at: http://www.cac.gov.cn/2015-12/16/c_1117481790.htm

the organizing committee demanded that all countries support Internet development, promote cultural diversity in cyberspace, share the fruits of Internet development, safeguard peace and security in cyberspace, and advance global Internet governance.[24]

Internet governance is currently a joint effort between commercial, academic, and civil sectors, in conjunction with the government. Some momentum is gathering behind an effort to cede full Internet governance to a model led by national governments, a movement which would potentially affect freedom of expression, the free flow of online information, and the open market of infotech products and services. A state-managed model could potentially regulate online content, restrict information exchange between nations, slow down innovation, and provide incentive for increased surveillance of internet activity by foreign intelligence communities.[25] Emphasizing the socio-historical differences between China and the West, Wang Yukai defended China's approach to information security addressing a panel at the World Internet Conference in 2015:

> Since Western standards are based more on market competition, the development of Internet-related standards is largely considered to be dominated by technologists, commercial companies, and civil institutions, and the government should not intervene too much. However, in developing countries, due to national interests and security considerations, as well as the government's dominant position in standard setting work, Internet-related technical standards have also become the focus of government public policy.

China also continues to curate a collection of sympathetic media elites and government officials, who may assist through offering local trainings and seminars to evangelize Chinese new technology, as well as potentially following China's lead on international

---

[24] "Infographic: Interpretation of Wuzhen Initiative", *China Daily*, December 21, 2015. Available online at: http://www.chinadaily.com.cn/business/tech/2015-12/21/content_22761127.htm

[25] Worldwide Threat Assessment of the US Intelligence Community, 2013.

internet policy. Some of the training efforts China exerts in evangelizing its technology and media to other nations focuses on specific countries. Conferences have been held in China for media groups, government officials, and prominent journalists from many different nations. These conferences create opportunities for visitors to learn about, new media, technology and governance models, "the Chinese Dream," and "the important role played by new media in domestic and international affairs" (Shahbaz 2018).

Made in China (MIC) 2025: The 2015 effort by Prime Minister Li Keqiang to launch the "Made in China" initiative set out to modernize and increase China's industrial capacity. The initiative is a 10-year comprehensive strategy to increase intelligent manufacturing in strategic sectors in the ultimate goal of making China a global high-tech industry powerhouse, as well as reducing Chinese dependence on any foreign technology. In fact, these key sectors represent a fourth industrial revolution, the name given to the process of integrating of big data, cloud computing, and emerging technologies into global manufacture and supply chains (McBride and Chatzky 2019).

Much of China's attempts to control information is directed toward American technology companies. Though many American companies actively seek out the Chinese government, their services may be restricted or blocked altogether. American companies who agree to the restrictions in order to reach the Chinese market help to legitimize China's methods and goals for internet governance. It's possible that American participation in the Chinese market could be assisting China's drive for military technological superiority. At the world internet conference, widely attended by American CEOs from companies such as Google, Apple, and Cisco, a Chinese expert on

antiterrorism advocated for increased pressure—even punitive measures—on internet content companies to control any negative content regarding the party, leadership, or the nation (Diamond and Schell 2019).

By echoing the language of Chinese officials on internet governance at such occasions, the U.S. tech giants have shown a tacit willingness to concede to some of China's rules in order to gain exposure in China. Attending the World Internet Conference in 2017, while Tim Cook of Apple avidly defends free speech and individual privacy concerns in the US, in a statement he focused more on the mutual goals of China and Apple with his description of "developing a digital economy for openness and shared benefits" (Segal 2018).

Both Facebook's Mark Zuckerberg and Google's Sundar Pichai showed initial willingness to submit to Beijing's rules in order to gain access to the Chinese market, creating an ethical problem. Facebook has been blocked in China since 2009, but Zuckerberg is keen to publicize interest in the Chinese market, notably sharing copies of Xi Jinping's 'The Governance of China' with colleagues. Neither the public, in China and the world, nor the Chinese authorities, were flattered by Zuckerberg's PR tactics. Many criticized that Facebook was turning into a CCP propaganda platform to impress Beijing, prompting some media outlets to dub him "Chairman Zuck". The Chinese Minister of Information also said that the value of the Chinese market would not be given away to American companies, if Chinese national interests were the price (Timmons 2014).

Google also committed to a customized search engine that would be compatible with Chinese censorship. In 2018, the existence of the Dragonfly prototype, an internet

search engine compatible with Chinese state censorship restrictions, was made public. Following the news, about 1,400 Google employees signed an executive petition demanding transparency on the project, and employee input on future Google projects, and political entities weighed in, as well (Campbell 2018). The Chairman of the Joint Chiefs of Staff found it inexplicable that an American corporation would seek business in such a restricted environment as China, and Senator Mark Warner identified Google's project Dragonfly as evidence of Western companies being courted by Chinese information control efforts (Durden 2018).

Companies who do business with or invest in China often face terms that require sharing intellectual property and industry-specific insight. These "joint venture" rules have been used, as explained by a CFR Senior Fellow, to acquire many advanced technologies. In addition, Chinese companies invest in foreign companies in order to gain early access to advanced industrial knowledge, such as semiconductor technology. While some investment comes from private companies, much of this activity is backed by the Chinese government. State-backed firms still account for a third of China's GDP, despite the economic reforms of the 1990s, which reduced their economic power. Even privately-run tech leaders like Huawei and ZTE are supported by the government (McBride and Chatzky 2019). In addition, the party-building efforts of the CCP among the private sector has been explored by both scholars and journalists. A variety of tactics have been employed by the government in order to find positions of influence in China's private economy, from establishing new institutions to coordinate private-sector affairs and focusing on better service for the private sector, to designating party-building

instructional designers, to rewarding business elites with party appointments (Yan and Huang 2017).

One Belt, One Road: Another key area where China seeks to set technical standards for the future is through infrastructure. Infrastructure competition is shaping Asia's technological future, with ambitious plans for roads, railways, pipelines, and more. All of this offers a glimpse at Asia's fast-changing future, yet China's vision is still unparalleled in its scope and ambition.[26] The Belt and Road Initiative (BRI) is an unprecedented development strategy to enhance Chinese trade and influence through infrastructure projects (Shahbaz 2018). The OBOR initiative includes a plan for a fiber-optic network called "digital Silk Road". This piece of the project is directed at making the future of the global internet into China's ideal image of a nationally regulated and censored internet (Patrick 2018). This network would also lend itself well to greater monitoring and controls by Chinese intelligence as well as host country intelligence. As China's influence over the world's critical telecommunications infrastructure grows, even global user data may become more accessible to Chinese intelligence community (Shahbaz 2018). Intercontinental underwater optical cables and improved satellite information networks are among the proposals Beijing wants to add to current infrastructure and energy projects (Wu 2019).

Social Credit System: The trust and morality supposedly generated in Chinese society by social credit is directly connected to discourse power; the Chinese state's use of the terms assumes support for and adherence to the CCP as core part of the definition (Hoffmann

[26] "Competing Visions", *Reconnecting Asia Project*, Center for Strategic and International Studies.

2018). Extending ‘discourse power’ to the international sphere has more recently been a priority, as the party has displayed a keen intention to move beyond domestic messaging and consolidating national power by shaping international values and generating positive perceptions outside of China. Exercising influence over the outside world in this context is not just a standard historical activity, but an imperative of national security (Mattis 2018). Part of the strengthening of the CCP’s discourse power that results from social credit happens because of the data collection and integration that allows the party to continually assess how it is perceived. Lu Wei described this effect in 2010, defining the party’s view that ‘discourse power’ includes the idea of effective speech, in addition to the right of speech. In the same discussion, Lu Wei emphasized that effective discourse power relies on collection of information, as well as communication of it; in fact, the correlation goes deeper, in that the power of communication is increased by the knowledge gained by timely collection of information. China’s data collection practices require global, real-time monitoring through big data management, in order to implement and inform the social credit system (Hoffmann 2018).

Possibly, emerging technologies in big data and AI may allow less technically literate nations to speed up their comparative development rates, as future economic competition may depend more on data size and speed than on only financial and economic scale. The pace of China’s data collection has increased as fast as internet and mobile internet develops; the data collected has the potential to facilitate fast AI development (Qiang and Chao 2018).

3.6 US-China Cyber Relations: Challenges and Responses

Over the last decade, China-based cyber actors have imposed various security breaches all around the globe, targeting diverse organizations and industries from Aerospace and Public Administration to Financial Services, Health Care and Education. The majority of these cyber-attacks, in particular, cyber espionage and intelligence gathering, have been directed by Advanced Persistent Threat (APT)[27] groups sponsored by the Chinese government. There are more than 20 APT groups based in China with diverse missions. For instance, APT1, also known as PLA Unit 61398, has systematically stolen terabytes of data from a range of organizations and industries across English-language countries, while APT 3 (AKA UPS Team) generally targets Aerospace and defense industries, and yet, APT40 typically targets countries strategically important to China's One Belt, One Road Initiative. Although the activity of many APT groups declined after Obama-Xi agreement in 2015, a majority of them resumed their activity in 2017.[28]

China's assertive behavior and growing ambition, while legitimate has consequences; in particular, when public activity within the domain of public diplomacy becomes more than influence and turn into interference. The United States deal with two extremely different political systems and values with respect to China. "As long as we could presume that China was reforming it was possible to believe that we were becoming more convergent in the sort of common pool of governance and ethics, if not political system" argues Oliver Schell, Director of the Center on U.S.-China Relations,

[27] APT groups unlike other attackers pursue their objectives over time and have support of states as well as access to states' resources.
[28] "Advanced Persistent Threat Groups: Who's Who of Cyber Threat Actors". *FireEye*. Available online at: https://www.fireeye.com/current-threats/apt-groups.html#apt1

Asia Society, “but when China began to slow the reform process … that sort of undermined the whole idea of engagement” (Schell 2019).

The greatest danger to the United States when it comes to China, as Susan Shirk contends, is not its economic or military power, but its internal fragility and fear-fractured leadership (Shirk 2007). The China run by Xi Jinping consists of expansive global ambitions resting on the pillars of limited domestic opposition, a significant military, an aggressive diplomatic plan, and an economic strategy focused on coercion and inducement to participate. Both the CCP and Xi Jinping himself have contributed to the synchronicity of security and economic goals, pushing toward a strong alignment with a growing number of partners, which is an essential factor in China’s effectiveness as a growing global power with strong and integrated levers of national power (Grace 2019).

China’s constant technological innovation and improvement to cyber-attack capabilities and information control methods online makes the country a persistent military and espionage cyber-threat to the United States’ core military and critical infrastructures. Of additional concern is the potential use of Chinese intelligence and security services to rely on Chinese information technology firms’ platforms to create regular espionage strongholds (e.g. Huawei affairs; OBOR initiative) (Coats 2019). Decision-makers in both Beijing and Washington are facing certain challenges, from developing behavioral standards and collaborative infrastructure to support those standards, to changing overall perceptions about cyber security (Yi 2011).

Strain between Western governments and China has increased to the degree that the west sees a threat in Chinese expansion and dominance. The technological

advancement initiatives put forward by the Chinese government meet with perceived direct or indirect hostility from leading economies like the EU, Germany, and the US. Often the initiatives function to simultaneously give China an edge as a value-added competitor, and to shut out international competition from the important Chinese market.[29]

The Obama administration's stance on cyber security saw mixed results. While some successful offensive operations were launched, including the Stuxnet attack, the extensive loss of defense technology and personnel data to Chinese hackers represented a significant failure (Farley 2018). During his second term, President Obama declared two cyber-related national emergencies in April 2015 and December 2016 and issued an Executive Order – "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" –to deal with any foreign cyber-enabled activity threatening the U.S. national security, foreign policy, or economy (Obama 2015).

Five members of the Chinese People's Liberation Army were charged with hacking American infrastructure networks such as Westinghouse Electric and the United States Steel Corporation, in the Obama Administration's most significant confrontation with China. With the disruption to international dialogues caused by the Snowden Affair, which exposed the United States espionage efforts in China, the Obama administration was possibly attempting to turn attention away from espionage by bringing those charges, and back to a stronger footing by focusing on intellectual property theft (Schmidt and Sanger 2014).

---

[29] "Made in China 2015". *Institute for Security & Development Policy*. June 2018.

A Cyber Agreement between the U.S. and China did result from a state visit in September 2015. The agreement reached by President Barack Obama and President Xi Jinping addressed some broad concerns around timely responses to information requests and prompt assistance addressing malicious online activity, not participating knowingly in intellectual property theft, continuing dialogue to identify and promote international cyberspace norms, and collaborating to fight cybercrime domestically and internationally (Rollins 2016). In addition, as Gen. Michael Hayden, former CIA and NSA director, emphasized in an interview, the highlight of the agreement was China's acceptance of the US's definition of what constitutes "legitimate state espionage"; meaning, states' sponsored cyber espionage shall make its citizens safe and free rather than rich (Ravich and May 2016).

For nearly ten years, the primary actor in China's cybertheft campaign was the People's Liberation Army; but five PLA soldiers were publicly outed in 2014, and the PLA bore the brunt of national blame over how that discovery weakened negotiations with the U.S. In addition to other concerns, this led to a significant reorganization and anticorruption initiatives that have reduced the PLA's political power and led to the discovery and punitive measures for numerous government officials. The possible new rise in Chinese hacking may be due in part to resulting vacuum left by the PLA, although the Chinese Ministry of State Security, a sort of amalgamation agency for national security, espionage, and investigation, has in many ways replaced the PLA's place as a central office for cybertheft (Graff 2018).

China and High-Tech Industries: Warnings from American military leadership, led by Secretary of State Pompeo, have been directed to allies that Chinese technology should not be used to build critical infrastructure for 5G networks. Tech companies worldwide are racing to implement 5G, which promises faster cellular service and better overall internet connection (Kang and Sanger 2019). China's ambition to control entire supply chains and even whole industries is of deep concern for policymakers, who fear the growing power of Beijing's state-led model. A White House report released in June of 2018 called out a threat of China's economic strategy concerns to not only the U.S. economy, but to innovation and industry on a global level. In particular, critics argue that Xi's policies, which priorities political considerations over economic incentives will distort the global market (McBride and Chatzky 2019).

Fighting the increasing Chinese Internet control means that the US and its partners need to exert more pressure on China to open their market to foreign companies. In order to participate, those foreign players will need assurance that their intellectual property is secure, and that China will relax their protocol of preferential treatment for Chinese firms (Segal 2018). Further, foreign companies "complain of an asymmetry in which China is free to invest in foreign countries, but foreign companies selling to and operating in China are highly constrained by investment requirements and other regulations" (McBride and Chatzky 2019).

One Belt, One Road/Digital Silk Road: Comparing China's One Belt, One Road initiative (2015) with Britain's Telegraph project (1840s), Jonathan Hillman argues that both of these infrastructure projects serve as illustration that commercial and strategic interests

are closely related. The telegraph infrastructure, in the end, represented a mixed strategic success for Britain. Initially it solidified colonial control, but it also functioned to carry news, international communication, and ideas of dissent and change. Britain's censorship could not ultimately control the information sources. India, in particular, saw the broad use of new technology and tools to fuel nationalist and independence movements. The same can be true for the case of China (Hillman 2019).

The Belt and Road initiative has garnered significant concerns from those who see it as an advance guard to allow Chinese practices—and potentially, their tools of repression—to establish solid ground in other nations and cultures, be it internet sovereignty, domestic surveillance, or explicit 5G standards (Kynge et al 2017). There is an inherent duality in the facilities that China is establishing in foreign ports, which are ostensibly commercial but quickly upgradeable to carry out essential military missions (Hillman 2019). Unlike the U.S., China has established more economic partners and less military bases. Why is it that access is much more significant in Chinese military strategy than bases are? Access is significantly less complicated, less controversial, and less threatening to one's neighbors than is establishing a force on another nation's soil (Kynge et al 2017).

Both U.S. and Japanese experts have suggested that the U.S. increase investment in Asia, as Asia's digital economy growth is happening in parallel with increasing Chinese presence in the region. Robert Atkinson, president of the Information Technology and Innovation Foundation went so far as to say the U.S. should respond strongly to China's digital development ambitions by fighting for "every scrap of the global market share" for advanced technology (Wu 2019). In order to cooperate on

security, the United States, India, and Australia started an initiative ten years ago which has been recently revived to coordinate alternative financing to what is being offered by China for regional infrastructure advancement (The Japan Times 021918).

America's approach to China's rising global influence, Susan Shirk recommended (Shirk 2007), must consider which Foreign Policy face it is reinforcing; the emotional, reactive one, or the responsible global power one. As this study shows China's cyber posture is emotional and assertive and Beijing's quest for cyber superiority is in sharp clash with the U.S. interests in cyberspace. Even on economic cyber espionage issue that US and China arrived at a consensus, the US has been somewhat successful in identifying and limiting Chinese cyber-attacks, because Chinese leadership – so focused on regime survival – sees espionage as essential to national political and military defense (Segal 2017). But if the latter face prevails, China might be a potential partner in addressing cybercrimes and offering a solution for cyber governance – maybe a hybrid model that combines positive features of US' and China's Internet governance models. To keep China from succeeding in rewriting core international or customary laws through subtle alterations in the nature of key institutions and laws that pertain to global affairs, Western powers must be constant in their awareness of China's efforts at influencing global perceptions, and clear in their statements and responses to such actions (Jackson 2015).

3.7 Concluding Remarks

Chinese foreign policy apparently presents two different faces to the world, the first an image of a responsible world power entity with moderate, reasonable goals and a meaningful global economic contribution; the second, a portrait of unpredictable and

defensive decision-making in response to perceived threats to national pride or sovereignty. Both of these faces seem to stem from China's somewhat fragile internal state (Shirk 2007). The new direction of the Chinese government wants reform, but not openness. The institutional reform happening now actually reverses, in many cases, the past 30 years of liberalization and reform, and foreign policy initiative has shifted to a bolder stance compared to what it was under Deng Xiaoping (Economy 2018).

To achieve its strategic goals in addressing its national cybersecurity dilemmas (discussed in chapter two), China's preferences according to some experts are self-defeating or contradictory at best, no matter how much Chinese political elites and the CCP strive for economic growth and reform, reflected in the various choices they make:

- One such balancing point where China has to choose between major priorities is when it comes to stimulating the economy or improving national security. Both elements are essential to China's overall security, and must be kept in some form of balance; free exchange of information and data are critical to the digital economy, and at the same time Xi Jinping is attempting to foster a dynamic digital marketplace, he is also trying to muffle social and political activities online. This shutdown of freedom of expression may point to a longer-term risk, despite the apparent success of his current economic reforms (Meltzer 2019).
- Balancing infrastructure modernization against critical infrastructure protection represents another watershed point for China. Both domestic and foreign companies have been forced to navigate the strict cybersecurity review and the restrictions China places on products and services in order to prioritize security (Sacks et al 2019). In general, authorities advocate for indigenous technologies

(MIC 2025), which providers have to comply with China's rule and in case of national security emergency the government can shut down those services.

- When it comes to private sector/public sector balance, China does not face the same challenges of a democratic nation in managing public-private partnerships; the CCP maintains a high level of control over both foreign and domestic companies, especially for strategically significant sectors. Because of this, safeguarding the public interest is the responsibility of the state; there are no significant incentives for private companies to invest in security initiatives (Heilmann 2017).
- A free flow of information and data on a global level empowers much of the digital marketplace; however, it also allows a degree of information-sharing that threatens the CCP's preference for information control and data protection. China legally requires personal data and important data collected by any operators to be stored domestically; this type of Balkanization, if it continues to be adopted, is a potential threat to the global economy and digital marketplace (Meltzer 2019; Paulson 2015).
- China was identified again in 2018 as the greatest threat to internet freedom; the CCP hosted media officials from all over the world for extended seminars on navigating its system of censorship and surveillance, and China continues to promote digital authoritarianism and its capacity for citizen control as a major advantage of internet and digital technology (Shahbaz 2018). While authoritarian internet policy effectively restricts opposition's ability to organize, it can also impact network functionality. The internet policy of China has survived periods of

> crisis and violence with at least a façade of ideological apparatus. China has demonstrated clear willingness to follow through on threats to activists, in a concerted effort to disrupt the digital structure of dissent, with consequences ranging from blackmail to imprisonment and/or death.

As discussed in this chapter, China faces cyber threats that originate from shifts either in the international system, sub-system (regional), or in the domestic politics. The categorical division of systemic, sub-systemic, and domestic power balance into multiple tiers are interconnected and vague. Chinese elites have an outward focus on the systemic and sub-systemic power balance between states, and an inward focus on the domestic power balance between societal blocs.

Beijing's challenges to the world order will remain somewhat subtle, according to Dean Cheng, and is more likely to favor gradual increase in competitive capability over direct conflict.[30] One key area where Beijing and Washington may eventually reach an impasse, however, is in the international legal field, where enforcement is difficult (Artusy 2018). Since the rise of Xi Jinping, China has developed variety of regional and global initiatives, which in turn, have influenced power and statecraft structures, and these successes have been occasionally weaponized as examples of interdependence; China retains a privilege of power from these structures, over network hubs and the domestic institutions that empower them (Farrell and Newman 2019).

---

[30] A note on earlier notion (in Chapter 2) on the revolutionary revisionism status of China: According to Schweller (1999), "The goal of revolutionary states is not the adjustment of differences within a given system which will be at issue, but the system itself. It is a quest for global domination and ideological supremacy." China, especially in Cyberspace, does not seek adjustment, but to establish its own model of internet governance and measures (as evidenced by variety of academic research and policy papers as well as its global and regional programs and initiatives). Because China does not favor conflict, it does not mean that its nature or ambition is not revolutionary.

Chapter Four: Russia
The Emergence of a Cyber "Infektion"[1] State

"Many issues have been accumulated on what route the Internet will take — whether it will develop as a common information space, which unites people, or disintegrate into various national or regional segments due to lack of response towards many threats related to the Internet development".[2]

Igor Shchegolev, Aide to the President of the Russian Federation
Wuzhen Summit 2014

4.1 Introduction

The early post-Cold War period was a strong influence over Russia's approach to order. Current leaders are wary of seeking further integration with Western order, as the Russian narrative argues that previous attempts to integrate failed due to a Western lack of recognition for Russian interests. Boris Yeltsin's desire for peace-oriented post-Soviet Russia to join leading democratic nations and major powers required critical Western support, which President Clinton and other NATO leaders tried to provide. However, Russia's democratization process ultimately did not succeed in a new post-Soviet state, and perhaps Yeltsin is largely the cause. We cannot know for sure, but Russian politics may have developed differently without U.S. military intervention in Kosovo (1998). The new war in Chechnya (1999) and Putin's emergence to power (1999) also symptomized deeper problems (Talbot 2019; Gessen 2018). As integration became less of a viable opportunity to Russian leadership, they began to seek and develop regional alternative

[1] Infektion Operation was the infamous Soviet's disinformation campaign to imply that the United States developed the AIDS virus in its Army Medical Center at Fort Detrick and spread it among the public.
[2] "Russia praises China's initiative to host first global Internet conference", *Russian News Agency*, 19 November 2014. Available online at: https://tass.com/world/760667

institutions, and eventually to actively oppose Western leadership (Radin and Reach 2017).

The impasse is formed by the generally commonly held view within Russian foreign policy leaders of the current U.S.-led hegemonic international order as a prime threat to Russian interests. Russia, seeking to protect the influence and security of its regime, as well as its local and global influence, sees U.S. leadership and democratic expansion as certain menace to its own objectives. While some elements of current global order do garner cooperation and collaboration from Russian leadership, it is largely only those that build up a Russian position of power, such as the U.N. system. U.S.-led order, in contrast, typically presents as a threat of some kind to Russia, either by undermining its geopolitical influence or its national policies, leading to active opposition of EU and NATO expansion (Ibid). Although Russia does show signs of seeking NATO relationships that strengthen the general security of Euro-Atlantic areas, a successful Russia-NATO relationship, however, hangs upon NATO's recognition of Russia as an equal partner, and whether or not plans to extend NATO's global reach beyond current norms of international law may be acceptable by Russia.[3]

The three main points of contention that shape both foreign policy and cyber-policy discussions between Russia and the West are Russia's influence over former soviet territories, Western promotion of democracy, and issues of sovereignty and intervention (Radin and Reach 2017). Russia has honed a range of tools in order to challenge the increase of post-Soviet Western influence, from hard diplomacy, economic levers, energy

[3] National Security Strategy of the Russian Federation. Available online at: http://thailand.mid.ru/en/national-security-strategy-of-the-russian-federation

supply control, trade wars, military force, and propaganda. Some of these tools have translated to cyberspace versions, such as cyber-sovereignty, disinformation campaigns, and cyber diplomacy.

The Russian democratic and economic reforms that began in 1991 collapsed quickly in tandem with Putin's rise to power in 1999. In his 2005 "State of the Union" address, Putin called the collapse and dissolution of the Soviet Union in 1991 as "the greatest geopolitical catastrophe of the century"[4] – an event whose undoing represents a key element in Putin's political motivation. In the midst of democratization wave across former Soviet republics, Putin's regime reversed the democratization course in Russia, centralized Kremlin authority, and reinstated many elements of Soviet geopolitics and active measures, including the Iron Fist, disinformation campaign, use of foreign Russophile parties and front organizations, necessary border expansion, and subversion of Western ideals (Talbot 2019). Most of Putin's political decisions can be traced back to sheer motivation for survival—both of his regime and himself. Putin controls broadcast media, the parliament and judicial systems, and security services, which have practically returned to Soviet-era functions under his power. Similar to the Soviet's active measures, which aim was to "weaken the USSR's opponents—first and foremost the "main enemy" (*glavny protivnik*), the United States—and to create a favorable environment for advancing Moscow's views and international objectives worldwide" (Boghardt 2009, 1), Russia's disinformation campaign aims to challenge the Western democratic world

[4] "Putin calls collapse of Soviet Union 'catastrophe'". *The Washington Times*. 26 April 2005.

order—first and foremost the U.S. leadership—and Moscow and its network of pro-Kremlin groups advocate for Russia's world view.

4.1.1 Ideational Components

In contrast to China and Iran, Russia lacks a coherent ideological doctrine.[5] Even Boris Yeltsin observation underlies lack of a distinct ideology in Russia's path to democracy. Western prescriptions for an ideal society, under Yeltsin's presidency, not only didn't work, but they intensified Russian cultural perception of defeat and humiliation. An important key to understanding Putin's presidency is that he began rebuilding the state on a familiar, not foreign, ideology and experience, and he even seemed to rediscover the unique exceptionality of the Russian political model (Tsonchev 2017).

At first, Putin's administration denied any need for state ideology (first term: 2000-2004), but only a little later, a national ideology was a concern significant enough to merit a discussion of creating a council of major intellectual and cultural figures to define it. Putin's return to office in 2012 crystallized a more conservative posture in official records. The vague presidential narrative of conservatism was yet explicit in its anti-Western, anti-liberal promotion of 'traditional' moral values. As it is more defined by opposition than by doctrine, it appeals to a broader base, offering space to ideological entrepreneurs who maintain their own communication networks (Laruelle 2017). Putin expresses admiration for Peter the Great, and his ideological values are similar to the Russian emperor's motto of "orthodoxy, autocracy, and nationality." This is atypical of

[5] By ideological doctrine, I mean regime's ideology like Marxism-Leninism under the Soviet; China's Maoism; and Iran's Islamist Ideology. Today's Russia lacks such a regime ideology. It has a loose value system centered on conservatism.

the Marxist-Leninist system under which Putin grew up (Glasser 2019, 10). Putin's logic centered on Russia as a unique civilization that was not served by foreign models. The failure of secular and political ideologies left Orthodox Christianity as the most convenient and useful source of national and political identity for Russian citizens; Putin's Kremlin and its Shibboleths drew on civilizational discourse, religion, and Russian imperial conservatism to craft a new post-soviet identity (Laruelle 2017), which core ideological tenets are Eurasianism and the 'Russian World' (Russkiy Mir) and the Kremlin has successfully integrated them into its interpretation of information security and cyberspace. More than elites or state structures, the Russian World project targets broader society with soft-power techniques. The Eurasian projects, in contrast, are directed toward the development patterns of member states, and does not overlap geographically with the former.

Russian World: Challenging the international order as it stands is a central tenet of the Russian World concept's definition of the Russian voice and global identity. Russia cannot challenge the world order alone, however; and though the Kremlin hesitates to define how this alliance will play out, the most obvious candidate in this negotiation is China, with its rising power trajectory. A replacement new world order isn't defined by any coherent Russian doctrine, although it is an essential part of the Russian World ideal. And while Russia and China both seek to challenge U.S. dominance, their approaches are distinctly unique; Russia's focus on confrontation speaks to a greater concern for

immediate change, as China seeks more of a gradual shift in power balance that favors Beijing's capital concerns (Laruelle 2015). [6]

The post-Soviet interpretation of the term Russian World (*Russkiy Mir*) has variety intellectual origins. Some accounts describes it as "a peaceful reestablishment of Russia's identity and its reconnection with its past and its diaspora",[7] some experts contend "being Russian is not about blood, being Russian is about a shared identity", and yet some accounts perceive the term as "attracting Russians from all over the world to participate in a new global meta-project";[8] thus, associate Russian World as a new post-Soviet brand for Russia's domestic and foreign objectives. While the Russian World concept is based on a dedication to defining Russia's global voice, it has focused mainly on Russian ethnic minorities and Russian-language speakers than on broad population segments in the post-Soviet era. The survival of Russian World concept is threatened primarily by Russia's ability to structure a successful voice that reaches beyond geographical Russian boundaries and nationalist specifics and has the potential to be accepted in the context of a global narrative (Laruelle 2015).

The Russkiy Mir concept gained cultural power during the annexation of Crimea, when the term "New Russia" (*Novorossiya*) was quickly popularized by the kremlin. Although it is essentially impossible to establish a "New Russia" within the Eastern

---

[6] For more information on China and Russia strategic partnership see Krickovic, Andrej. "The symbiotic China-Russia partnership: Cautious riser and desperate challenger." *The Chinese Journal of International Politics* 10.3 (2017): 299-329.

[7] Efim Ostrovskii, Petr Shchedrovitskii, "Orel raspravliaet kryl'ia. 1111 znakov za 1111 dnei do Novogo Tysyacheletiya.Manifest novogo pokoleniya," Russkii Arkhipelag, December 1997, http://www.archipelag.ru/ru_mir/history/history95-97/ shedrovicky-1111zn/. Cited in Laruelle 2015.

[8] Efim Ostrovskii, Petr Shchedrovitskii, "Rossiia: strana, kotoroi ne bylo. Sozdat' 'imidzh' Rossii segodnia oznachaet postroit' novoiu sistemu sviazei mezhdu russkimi," *Russkii Arkhipelag*, 1999, http://www.archipelag.ru/ru_mir/history/history99-00/ shedrovicky-possia-no/. Cited in Laruelle 2015.

Ukraine, the idea took root and its associated terminology has continued to inform the ideology and communications of the administration. The annexation of Crimea itself was justified by President Putin for two main reasons; first, for the need to protect the 'broad Russian civilization' from external forces, and secondly, in the name of a restorative unification of historic Russia, all of his language carefully pointing toward the "aspiration of the Russian World" (Laruelle 2015, 14).

Eurasianism: Originally formulated in exile by Russian elites and nobles who fled the Bolshevik revolution during 1920s, Eurasianism is rooted in nineteenth-century Russian nationalism, which envisions Russia as a sovereign civilization and promotes the solidarity of the imperial state – whether it is the Tsarist Empire or the Soviet Union. This geographical space between Europe and Asia embraces cultural and ethnic pluralism yet it is distinct from the West (Bassin and Pozo 2017). In words of Eurasianist Nikolai Trubetzkoy, a Russian linguist and historian, Eurasia "is historically destined to comprise a single state entity", which personality is "symphonic." This type of civilization, Trubetzkoy argued, is superior compared to European states, which are culturally divided, with a political identity that is interconnected through a pan-European chauvinism and a mission to civilize the world (Trubetzkoy 1991, 165). The "superiority" component of Eurasianism as a civilization plays a major role in its political significance, as proponents assume a Russian-led Eurasia in an endemic clash with the West (Bassin and Pozo 2017).

The evolution of Neo-Eurasianism bears striking similarity to the milestone markers of the revolutionary period, where the state was confronted with territorial

fragmentation in the late 1980's, a development resisted by conservative Russian nationalists, who sought to ideologically reinforce geopolitical coherence (Ibid). The neo-Eurasianism we see now was developed by nationalist leaders who sought to salvage the remnants of Soviet imperial identity, including its hostility to the West (Kello 2017). Aleksandre Dugin, Russian philosopher and political analyst, believes that Western forces on both sides of the Atlantic aim to synthesize and homogenize Eurasian culture, ethnicity and tradition; a "severe ethnic, biological and spiritual crisis" for a region that embraces diversity. It is Russia's responsibility, he emphasizes, to rescue Eurasia and its traditional values (Shekhovtsov 2009, 697). The popularity of Dugin's ideas has risen almost in conjunction with Putin's journey toward authoritarianism; the turn of Russian leadership toward conservatism has served Dugin well and increased his appeal, allowing him to contextualize Putin's policies, which serves Putin's goals well in return (Barbashin and Thoburn 2014).

4.1.2 Institutional Components

'Competitive authoritarianism' is a common term descriptive of Russia's political structure, in which formal democratic institutions are perceived as the main seat of political authority. However, the rules are so often violated by those in power that the final result cannot meet the minimal standard of democracy (Levitsky and Way 2010). Some studies counter this definition, instead designating the system a 'Pluralist One-Party State' similar to the German Democratic Republic where, incidentally, Putin lived as a KGB agent for six years (Van Herpen 2015).

Since 2001, United Russia[9] has been a key supporter of Putin's presidency. The new party introduced in 2006, 'A Just Russia,' was largely an artificial second party contrived by United Russia to create an illusion of choice that would ultimately empower the Putin's administration status quo. Two other parties—one communist and one liberal—are not active opponents and neither has the power of any significant popular support. This is not the only Kremlin-engineered fake party effort that exists, despite the risk of creating a fake multi-party system that could accidentally foster a real opposition (as happened with Mikhail Prokhorov and the Right Cause party) (Barry and Kramer 2011). Putin's formation of the "All-Russia People's Front" (ARPF or ONF [its initial in Russian]) makes it possible for United Russia to interact with other parties and organizations in order to counter potential oppositions. Presented in 2011 at a United Russia Conference, the ONF is a 'catch-all' party (Van Herpen 2015).

The inception of the ONF followed Moscow's recognition of tighter domestic and international constraints, under which elites needed to find new ways of generating support for their policies from a greater variety of social actors. The Front, it is hoped, will foster common interests between the leadership and citizens of Russia and keep the impression of top-down orders from forming a secure hold. The ONF has served to create consensus since early in Putin's third presidential term, though he does not hold any official position in the party. Putin praises Front members and action, and serves as an inspirational leader, but the organization is feared by local authorities and respected by society. Originally, their ethos is rooted in patriotism, but nationalist sentiments have

[9] The largest political party in Russia that holds 335 of the 450 seats in the parliament.

gradually become more prominent as the country has grown more internationally isolated, and they are especially active in promoting legal actions and norms on security (Malle 2016).

One party invited to participate in this Front was a successor of Rodina, a party rooted in ultranationalist and xenophobic ideals. The former leader of this group, Dimitry Rogozin, had been designated the permanent Russian NATO representative, but was called back to help organize the relaunch of the party, now renamed Rodina Congress of Russian Communities (Van Herpen 2015). Dimitry Rogozin is a key influencer in Russian politics, and is a major player, if not the main instigator, of the aggressive moves toward Ukraine, in addition to founding the Rodina party. There is plenty of less formal political influence exerted by Rogozin, as well; notably, the 'Izborsk club' and its distinct role in drawing together key Russian Nationalists, such as Alexander Dugin. Cultural institutions like this club are more than just advocacy 'think tanks,' they bear significantly more influence on government decisions. Rogozin is also supported by the Russian Military-Historical Community, where he is the chairman of the board of trustees, and the Cossack Affairs Council, where he serves as deputy chairman (Laurinavičius 2014).

Russian activity in global affairs has been on the rise since the early 2000s, positioning itself as the center of gravity of post-soviet geo-political power, and making a multipolar reality more definite with its separate sphere of influence. Russia's rebranded identity, carefully centered on the triad of conservative values, Eurasian identity, and Russian

identity, can be strategically promoted through multiple cyberspace channels, including culture and language identity, norm building, and economic networks.

Putin's third term was defined by four strategic foreign policy events, each of which represent powerful Eurasianist and Russian World trends, from reorienting the Russia-China relationship, officially launching the Eurasia Economic Union, the Ukrainian conflict and the annexation of Crimea, following up with a series of disinformation campaigns in Europe and the United States. None of these events, however, are straightforward in establishing the exact role of these ideological components (Bassin and Pozo 2017). Compared to his predecessors as well as his first two terms as president, Putin since 2012 has been able to bring more elite consensus and has mitigated the vulnerabilities of his regime through a variety of cybersecurity measures in conjunction with regional and international initiatives such as the annual International Information Security conference in Munich, Germany and the International Code of Conduct for Information Security at the UN General Assembly in 2011.

The first section will contextualize Russia's national cybersecurity strategy within its domestic politics and highlight its four priorities in cyberspace: the promotion of "cyber sovereignty", the creation of an autonomous Russian Internet, information security, and the reduction of dependency on foreign technologies. The next three sections will map how these domestic priorities manifest themselves in Moscow's foreign policy, in particular, promoting norms and a governance model in cyberspace which mitigate security challenges to Russia's cyber sovereignty, the survival of Putin's regime, and domestic stability. The final section will summarize the key arguments made in the

chapter and highlights Russia's preferences in addressing its national cybersecurity dilemmas (discussed in chapter two).

4.2 Russia's National Cybersecurity Strategy

The current international order, as defined by Russia, is rooted in new centers of economic growth and political influence, which are harbingers of an unfolding geopolitical narrative. This narrative shows an increased preference to seek resolutions for geopolitical problems and crises at the regional level, without relying on the interference or influence of non-regional states. However, the current global and regional architecture remains oriented toward NATO, and international security continues to be compromised by this and by the imperfect nature of legal instruments and mechanisms in governing compliance. National Security priorities for Russia begin with creating a strong cultural defense, guaranteeing social stability, and ethnic and denominational harmony, which in turn more readily guarantees a national defense and a strong state and social security. Following that, the first priority is to transform the Russian Federation into a leading world power.[10]

Five indispensable interests guide Russian foreign policy, beginning with essential defense of the nation and the regime's power. Secondary to that is influence of the former Soviet states and geographical neighbors, followed by supporting a vision of Russia as a great power. Noninterference in domestic affairs is a fourth principle, and lastly, political and economic cooperation in a context of equity to other powers (Radin

[10] National Security Strategy of the Russian Federation. Available online at: http://thailand.mid.ru/en/national-security-strategy-of-the-russian-federation

and Reach 2017). Cyber tools and their potential misuse for political, military, and even criminal purposes have been a high-priority concern for Russia for at least two decades. A review of Russian diplomatic engagement history around Information and Communications Technology (ICT) and its impact on international stability reveals that two major concerns drove Moscow's initiatives: the prevention of conflicts, and the prevention of a cyber arms race (Chernenko 2018).

Any study of Russia's behavior in cyber-space requires an understanding of specifically Russian definitions of terminology and priorities. Russians generally don't use the terms cyber (*kiber*) or cyberwarfare (*kibervoyna*); like the Chinese, they more commonly use the word "informationization," indicating an integration of cyber-operations in the broader world of information warfare (*informatsionnaya voyna*) (Connell and Vogler 2017). As such, Russia does not have an official cybersecurity doctrine, rather an information security doctrine. The 'Information Security Doctrine of the Russian Federation' was released shortly after Vladimir Putin's regime came to power (2000). The document set out to define any information security threats to the Russian Federation, and lay out the methods of securing national interests, and truly became the first instance of connecting the concept of sovereignty to information space.

Just as China faces the challenge of chasing the more-developed nations like America and Britain, Russia faces developmental transformation to an information-based society. Putin laid the foundation of Russia's transformation to an information society by affirming the "Development Outline on Establishing Russia's Information Society for 2011-2020," in which the Russian government allocated an annual fund of 2 billion USD to establish and promote the Information Society Project (Ragulina, Lobova, and

Alekseev 2018). The Russian Federation elevates the importance of legal norms foundational to the information field, with its basis in the "Information and Informatization Legislation Development Conception of Russian Federation" document. Article 149 of federal law, adopted and issued by the State Duma in July 2006, defines the foundational Russian standard of legislative Information Security policy with "Law on Information, Information Technology, and Information Protection". Russia has fostered international cooperation in the informatization field by establishing bilateral cooperation agreements, information exchanges, and cooperation under the multilateral frameworks of the United Nations, APEC, and the Shanghai Cooperation Organization, as well as dialogue mechanisms with various countries, including China (Hai-Li 2014).

The Ministry of Communications and Mass Media along with the Ministry of Economic Development developed the Information Society for 2011-2020 program[11] which includes six sub-programs:

1- Improving the quality of life and the conditions for doing business
2- E-government and effective state governance
3- Development of the Russian market for information and communication technology, and measures to go over to a digital economy
4- Bridging the digital gap and building the basic infrastructure of the information society
5- Security in the information society
6- Development of digital content and preservation of Russia's cultural heritage

The above programs are defined by certain objectives: the development of digital government services and access infrastructure; development of innovative high-tech services; development of spatial data infrastructure in Russia; essential development of

[11] "State Programme: Information Society, 2011-2020". Official Website of The Government of The Russian Federation. 20 October 2012.

information society infrastructure; fostering increased awareness of information society opportunities among public and business communities; and supporting Russia's national interests in preserving multi-ethnic cultural heritage and identity.

A series of events (systemic imperatives) – the United States' establishment of its Cyber Command (CYBERCOM) unit in 2009, the Stuxnet attack at Iran's Nuclear facility, the Arab Spring, the Snowden intelligence leaks (May 2013), and US and EU sanctions on Russia after annexation of Crimea (2014) – triggered Moscow's efforts to take strong measures to securitize the internet and centralize intelligence gathering.

As a relative latecomer to cyber-activity, the Russian military builds on what was formerly the domain of the state's security services, where it was previously limited only to elements that overlapped with electronic warfare. Following the Georgian conflict in 2008, this has changed (Connell and Vogler 2017). In response to the U.S. declaration of cyberspace as a new domain of warfare (2009), a Russian cyber-command was first publicly mentioned by Russian Vice Prime Minister Dimitri Rogozin suggesting the need for a division that paralleled the United States Cyber Command; however, an official announcement of Russia's "information troops" was not made until February 2017. The work between those dates consisted of recruiting "scientific troops" from the field of young ICT professionals to serve either as soldiers or as civil staff in Ministry of Defense-affiliated research centers (Giles 2011). In addition to its international efforts, the Russian state plans to mobilize information combat against pro-democracy activists, as announced by the deputy head of the troops of the National Guard of Russia in May 2017. Similar to China, it is within universities that major Russia cyber militia members are situated. Russia still enforces a mandatory 12-month draft conscription, and as of

2013, the military has been encouraging top graduates from civil universities to serve that term within the 'research companies,' where they conduct applied research relating to various information security fields. These conscripts have the opportunity to continue military service as contractors after the 12-month term (Lysenko 2018).

Nested within its national security strategy, in particular Articles 21and 80, Putin and other Russian elites are pursuing an information security strategy with the goals of increasing Russian cyber power, guarding national sovereignty and Moscow's geopolitical interests.[12] The main directions of the national security policy of the Russian Federation are:

> Article 21: The national interests of the Russian Federation in the long term consist of the following: developing democracy and civil society, and the enhancement of the competitiveness of the national economy; ensuring the solidity of the constitutional system, territorial integrity, and sovereignty of the Russian Federation; transforming the Russian Federation into a world power, whose activity is directed at supporting the strategic stability and mutually beneficial partner relationships within the multipolar world.
>
> Article 80: The main threats to national security in the cultural sphere are the dominance of production of mass culture oriented towards the spiritual needs of marginalized groups, and likewise unlawful infringements against cultural objects.

Almost a decade ago, Timothy Thomas, a Russia expert at the U.S. Foreign Military Studies Office at Fort Leavenworth warned that "perhaps more than any other country, Russia is alarmed over the cognitive aspects of cyber issues as much as their technical aspects" (Thomas 2009, 476). Thomas' studies highlights a major point of difference

[12] The differing views on sovereignty and foreign intervention held by Russia and the United States are politically definitive; where Russia insists on a norm of non-interference, it demands exclusive intervention authority within the Eurasian region. In contrast, the U.S. emphasizes that sovereignty is always conditional on the prevention of mass atrocity or gross human rights violations.

between Russia and the West in their approach to cyber issues. Russia's approach to information security, outlined in official documents like Information Security Doctrine (2000, 2016, 2017), is more holistic than the West's concern over technical/net-centric aspects of cybersecurity. The Doctrine locates information security at the core of Russia's national interest and defines the term as "the state of the protection of its national interests in the information sphere, as determined by the overall balanced interests at the level of the individual, society and the state."[13] Further, the Doctrine emphasizes the significance of information security to spiritual wellbeing of Russian citizens, society and the state and internalizes the concept to its strategic, domestic and foreign policy objectives.

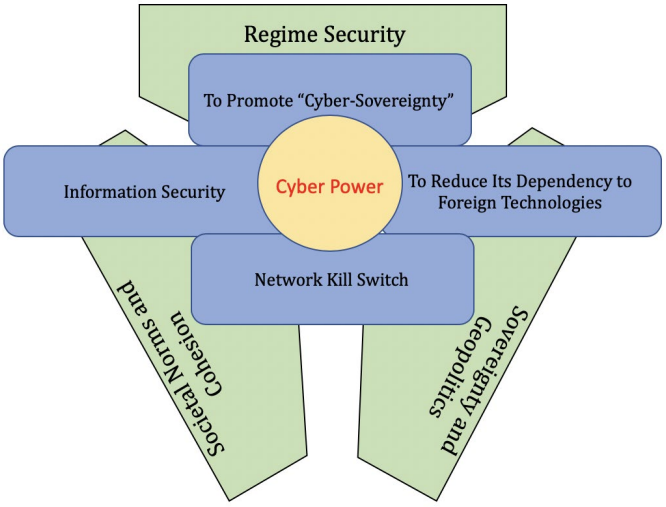
4.2.1 Domestic Imperatives of Russia's Cyber Posture

A growing body of research explores the impact of Russia's domestic political environment on its foreign policy decision-making process and international status. Primarily domestic priorities do sometimes guide foreign policy, as when Russia shows willingness to cooperate and collaborate with elements of current global order that build up a Russian position of power, such as the U.N. system, or Moscow promotes the adoption of only those international norms and rules that do not challenge its domestic agenda, in particular, sovereignty in cyberspace and autonomy in domestic affairs. The scholarship on Russian Studies demonstrates that stability of the regime; sovereignty, geopolitics, and zone of influence; as well as public safety, societal norms and cohesion are major drivers of Russia's foreign policy behavior and international identity (Radin

[13] www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf

and Reach 2017). As this study shows, Russia's cybersecurity strategy is guided by the same features that power its foreign policy (Figure 8).

Figure 8 - Russia's Quest for Cyber Power and Its Domestic Political Environment[14]



Russia's major cybersecurity goals can be summarized into four categories: promotion of cyber sovereignty, information security and territorialization of information flow, an autonomous Russian internet, and reduction of the nation's dependency on foreign technologies. Russia's quest for cyber power is at the core of these national priorities, which will be discussed in more details in the following sections.

The desire to centralize communications control has intensified following social media's emergence as a political mobilization platform during the Arab Spring, but also the anti-regime protests of 2011-13, which lent weight to the fear of Russia's political and military leadership of imminent 'color revolutions' taking place in Russia, as well as the suspicion of outside influence through the Internet. The Internet Research Agency, a

[14] Source: Pigman, Lincoln. "Russia's Vision of Cyberspace: A Danger to Regime Security, Public Safety, and Societal Norms and Cohesion." *Journal of Cyber Policy* 4, no. 1 (2019): 22-34; Stadnik, Ilona. "Sovereign RuNet: What Does it Mean?". *Internet Governance Project*. Georgia Institute of Technology. 2019.

known ‘troll factory’, was founded in the wake of Russian anti-regime protests over 2011-2013 (Kurowska and Reshetnikov 2018). Addressing his advisory Security Council on combatting extremism, Putin emphasized that:

> In the modern world extremism is being used as a geopolitical instrument and for remaking spheres of influence. We see what tragic consequences the wave of so-called color revolutions led to. For us this is a lesson and a warning. We should do everything necessary so that nothing similar ever happens in Russia (Korsunskaya 2014).

The current story in Russian doctrine is that of a “democratic transformation,” as it was called in the Journal of the Academy of Military Sciences, that represents a subversive, Western-led attack on Russian information and psychology, seeking to turn the moral, social, and public consciousness of citizens away from Russian values and toward a ‘Western liberal’ democracy (Pomerantsev 2015a). One of the most influential Kremlin aides, Vladislav Surkov, explained to Western journalists that the Kremlin term “sovereign democracy,” is practically similar to Western democratic practices. The term is a Kremlin brand that conveys two messages: “first, that Russia’s regime is democratic and, second, that this claim must be accepted, period. Any attempt at verification will be regarded as unfriendly and as meddling in Russia's domestic affairs” (Lipman 2006).

To the Russian military theorists of today, the twenty-first century seems to be an alarming cacophony of progressing democracy, ‘color’ revolutions, national chaos, and psychological influence caused by the flow of international information. In order to challenge these perceived threats, Russia has drafted new laws to limit freedom of speech, expanded state-led news channel Russia Today, and continues to refine Internet and telecommunications surveillance through the SORM program (System for Operative Investigative Activities) (Thomas 2015). In tandem with its “sovereign democracy” and

stemming from its Information Security Doctrine, Russia formulates one of its major national priorities – "cyber sovereignty". To advocate for its state-centric cyber policy Russia has sponsored variety of information security initiatives at UN General Assembly over the past two decades. According to International Information Security (IIS) bill drafted by Russia in 2000, states or non-state actors might deliberately use information to undermine another state's "economic and social systems and psychological manipulation of a population for the purpose of destabilizing society".[15] The bill expands state's sovereignty over information sphere and cyberspace to the extent that legitimizes state surveillance and censorship; thus, violating UN Charter on Human Rights (Freiberg 2014).

Another priority for Moscow is territorialization of information flow. Russia's territorializing tactics, while not quite the Chinese Golden Shield, include a mix of external content filtering, data localization laws, and geo-blocking, and was developed by a more gradual process of geographically tagging data and information, and extending legal regulations to deal with content and search engine filtering (Stadnik 2019). The distinctly localized territorial perspective of national information space has continued legislatively ever since, and the latest updates to the Information Security Doctrine call to further strengthen and centralize information security forces and systems (Kovaleva 2018). The 2016 Information Security Doctrine signed by Putin to replace the previous 2000 document outlined three pivotal objectives: countering external threats, overcoming international Russian media "discrimination", and eliminating barriers to Russian

[15] "Information Security Doctrine of The Russian Federation". 9 September 2000.

information technology equivalence. The primary objective is to secure full state control in the domestic information space, and the secondary objective is to justify Kremlin propaganda and Moscow's aggressive actions to the world audience. The final objective is to further Russia's progress in the global domain of IT and cyber-security (Sukhankin 2016).

Russia's third priority is independence from foreign technologies. "Import substitution" has been an important concept for the Russian government since the anti-Russian sanctions that followed the Ukraine and Crimea events of 2014, which inspired great caution about the nation and government becoming too dependent on foreign software and hardware (Ibid). The 2016 version of the information security doctrine positions "IT bonds" as an ancestral development of the infamous Russian 'spiritual bonds' derived from Russian culture, language, history, and sacred texts by Kremlin propaganda to protect Russian citizens from harmful information.

Dividing global domain name and IP address spaces along national lines gives nation-states greater freedom for territorial-based governance of cyberspace. The development of RuNet is a good example of legislation developing in tandem with critical Internet infrastructure, with a view toward creating an independently controlled network – a Kill Switch. The Russian authorities initiated the "Kill Switch" program in 2014, in response to both Snowden revelation as well as sanctions imposed on Russia after the annexation of Crimea, to protect Russia's internet and information infrastructure against possible internet shutdowns by aggressive governments (Stadnik 2019; Mueller 2017).

4.2.2 Russia's Information Warfare

Among Russian scholars, political analysts, and commentators, the idea of subversive operation and information (net-centric) war waged by the West to undermine the Kremlin is extremely popular. Whether it is called Hybrid Warfare, Controlled Chaos, or Color Revolutions the idea gets broadly discussed and even promoted by the political and academic elite of Russia. Beyond mere political speeches from Kremlin leadership these narratives have worked their way into Russian doctrine and documentation; one example being the *Russian National Security Strategy amendment* released in 2015. The narrative of Western information war being waged on Russia is less likely to be a carefully staged plot of the Putin administration than it is to be an amalgamation of academic, political, and public interest colliding and influencing one another: "Academics want to promote their ideas, politicians want to enforce their power, and the general public wants to regain a sense of national pride" (Fridman 2017, 81).

The Armed Forces of the Russian Federation perceives information war as *permanent* and *peaceful*, and its doctrine defines the term as:

> conflict between two or more states in the information space for damaging the information systems, processes and resources, which are of critical importance, and other structures, to undermining the political, economic and social system, and massive brainwashing of the population for destabilizing the society and the state, and also forcing the state to make decisions in the interests of the confronting party.[16]

The same document emphasizes that the Russian Federation defensive potential is dependent on the ability of the Armed Forces to be efficient and build capacity in the

[16] https://carnegieendowment.org/files/RUSSIAN-DRAFT-CONVENTION-ON-INTERNATIONAL-INFORMATION-SECURITY.pdf

containment, prevention, and resolution of conflicts in the information space – "a collection of databases and data banks, the technologies for their maintenance and use, and information and telecommunication systems and networks, operating on the basis of common principles and general rules that guarantee the information interactions of organizations and citizens, as well as the satisfaction of their information needs" (Kovaleva 2018, 137).

Since the late 2000s, Russia initiated a concerted effort – a mix of conventional and non-conventional warfare – to destabilize some of the former soviet states. Rather than an open confrontation of NATO, the EU, or the United States, which would too openly reveal Russia's weaker economic and military strength, Putin has opted instead for a "weaponized" information program of campaigns aimed at a soft-power influence. Russia uses information technology to spread doubt, division, discord, and to promote their own narratives to lower opposition to Russia among citizens (MacFarquhar 2016). Moscow's destabilizing campaigns pursued a host of objectives: to regain its zone of influence over those states, to stop the West's – in particular, NATO's – expansion into its back yard, and to defend Russia's interests as well as to protect Russian ethnic minorities. Based on lessons from its involvement in Estonia (2007) and Georgia (2008) conflicts, Russia developed a new operational mode, which employed more non-military means such as proxy war and cyber-attacks. Gen. Valery Gerasimov, the Chief of the General Staff of the Russian Federation Armed Forces, was the first to introduce this new modus operandi as Moscow's best approach – asymmetric and less expensive – to achieve its foreign policy goals (Giles 2016).

At the center of Gerasimov's doctrine lies information warfare, which grabbed attention of politicians and media in the West after the outbreak of the Euromaidan Revolution in Ukraine in 2014. Russia and the West have different perceptions of information warfare. While, the West regards information warfare as "limited, tactical information operations carried out during hostilities", Russia understands it as an "ongoing activity regardless of the state of relations with the opponent". Addressing the Federal Assembly in 2006, President Putin referred to Moscow's intellectual superiority as a base for Russia's future responses to other countries' military developments and stated such advancements while less expensive, they will provide Russia asymmetrical means to balance against other states' military power (Giles 2016, 2).

Russia's use of information warfare dates back to the Soviet era. Some of the modern-day actions seem to hark back to the Active Measures model, the KGB-run Soviet-era department that aimed to confuse and mislead Western interests with disinformation and psychological warfare. Some of the Active Measures included credible story forgeries fed to media outlets. Soviet-era forgeries took some care to make stories believable, but the Kremlin today does not show the same level of care with media misinformation. The greater the chaos, the better, as far as the Kremlin seems concerned, as the goal is to confuse and distract the audience into ultimate mistrust of the information space, rather than to convince them of any other reality (Pomerantsev 2015b). At the core of Russia's information war operation lies "reflexive control" – or "perception management" as it is known in the US. Stems from the Soviet's *maskirovka* (military deception) this mechanism "conveys to an opponent specifically prepared information to incline him/her to voluntarily make the predetermined decision desired by

the initiator of the action" (Mateski 2016). To win the information war an actor's aggressive toolbox includes the followings:

- Change citizens' traditional moral values and 'landmarks', create a lack of spirituality, and cultivate a negative attitude towards one's cultural legacy;
- Manipulate the consciousness of social groups by implementing so-called 'democratic transformations';
- Disorganize state administrative systems;
- Destabilize political relations among parties and coalitions to provoke conflicts and distrust; exacerbate political struggles and provoke repression against the opposition;
- Reduce the level of information support for organs of authority;
- Misinform the population about the work of state organs;
- Provoke social, political, national, and religious conflicts;
- Mobilize protests and incendiary strikes, mass disorder, and other economic protests;
- Undermine the international authority of a state; and
- Damage important interests of a state in the political, economic, Defense, and other spheres.[17]

The modern Russian approach to information warfare philosophically underscores a key truth about the Russian worldview refers back to Samuel Huntington's *clash of civilizations* concept, which presupposes a grand conceptual conflict about essential political order that exists between Russia and the West. This perceived battle for domination takes place within cultural and regional boundaries—and in between the boundary lines, states like Estonia, Georgia, and the Ukraine function as the front lines of the clash (Kello 2017). The central tenet of this worldview is the struggle for dominance between Russia and the West, specifically over information spaces. Conservative thinkers

[17] Iu. E. Kuleshov, B. B. Zhutdiev, and D. A. Fedorov, "Informatsionno-psikhologicheskoe protivoborstvo v sovremennykh usloviyakh: teoriya I praktuka" ("Information- Psychological Confrontation under Contemporary Conditions: Theory and Practice"), Vestnik Akademii Voyennykh Nauk (Journal of the Academy of Military Science), 1 (2014), pages 104–9. Cited in Thomas, Timothy L. "Psycho Viruses and Reflexive Control: Russian Theories of Information-Psychological War." Information War: From China's Three Warfares to NATO's Narratives (2015): 16-21.

in Russia overall perceive the fall of the Soviet Union as catastrophic, and that information operations were a key element in its failure. In order to correct this weakness, Dugin recommended the creation of a Eurasian-centered information network (Ibid).

The modern Russian information warfare doctrine is essentially that modern conflict centers on information domination more than geographic domination. While rooted in Bolshevik historical origin, the political implications of this modern implementation are far-reaching. To avoid the information failures of the past, Russia is taking a pre-emptive approach, seeking to disrupt foreign information spaces in any way possible, from citizen-led social media activism and advocacy, to official state actions (Kello 2017).

> Russia has become known for its high-standard, openly advertised hacker schools. In Voronezh, for example, [Federal Agency for Government Communications and Information] FAPSI … runs what is possibly the biggest and best hacker school in the world. And, in a country where any publication unacceptable to the government is harassed or closed, "Khaker: Computer Hooligan Magazine" thrives. There is no clear law against cybercrime, and it is even semiofficially encouraged -- so long as hackers do not attack the Russian state (Mshvidobadze 2011).

Russian scholars' conceptualization of 'information space' falls into five categories: territorial, technological, social, evolutionary and noöspheric (a global system consists of human, goods and nature). According to Russian scholarship, the nation's information domain is defined by a particularly territorial approach to policy development. In this type of territorial approach, information space and the media located therein is defined by physical boundaries of the state. The sphere of influence and communication, despite its physical ability to transcend them, is limited by the state's geopolitical borders. When the state controls spatial informational relations, it controls message integrity and has several

channels of power to leverage, through legislation and media outlet ownership, over domestic information. All of this makes the information space of unparalleled strategic importance to maintaining control of public life (Kovaleva 2018).

4.2.3 Multi-Tier Cyber-Threat Model – Moscow's View

Russia exploits its complex information war approach to respond to any real and/or perceived threat – that originate from shifts either in the international system, sub-system (regional), or in the domestic politics – endangers its national information security priorities. The MTCT model indicates that it is possible Moscow's external actions (e.g. promoting Russian conservative values, Eurasianism and Russkiy Mir as competing narratives to Western liberal measures for domestic audience, public policy in near abroad, and among Russian diaspora communities) can be doubly motivated by domestic manipulation of political and social forces (see section 4.3 – Cyber Authoritarianism and Domestic Politics). Focusing attention on foreign policy (e.g. anti-Western rhetoric) and interstate conflicts (e.g. Ukraine and the Baltics) may prompt the state support behind Russian World programs—strengthening public feeling against opposition (see sections 4.3 and 4.4 – Disinformation Campaign). Additionally, manipulating actors and interest groups located in other states can be part of the motivation for foreign policy implemented by elites (see sections 4.4 and 4.5 – Russia's Cyber Diplomacy and Norm Building). Local actions taken by Russia may also be undertaken with the explicit intent of galvanizing other actors to support Russia's foreign policy (see section 4.4 & 4.5). The last thing that the MTCT model identifies, is that Moscow's global actions might exert

key influence over former Soviet states seeking to re-establish its regional superiority (see sections 4.4 & 4.5).

I argue that in compare with his predecessors as well as his two first terms as president, Vladimir Putin since 2012, through a series of domestic and international information security-related initiatives, has successfully created a better consensus and cohesion amongst the Russian elites; thus, Russia has the "willingness" to balance against the U.S. leadership in cyberspace. Putin has also successfully created a stronger social cohesion, through introducing a more comprehensive ideology to counter Western values, and has been able to mitigate the regime vulnerability through more robust channels such as praise for traditional values; but due to its underdeveloped high-tech industry and its dependence to Chinese technology Russia does not have the "ability" to balance against the U.S. leadership in cyberspace.

4.3 Cyber Authoritarianism and Domestic Politics

The context in which Russian political elites began securitizing cyberspace—between the events of the Arab Spring, the social media-based protests all over Russia in the aftermath of 2011 parliamentary election, and Putin's return to office in 2012—may certainly have contributed to constructing the most significant cyber threat – regime security. Before the waves of Arab uprising, two camps had formed within the civilian and military elites debating cyber governance in Russia, the first, led by representatives from military and security services, advocating for digital rights restrictions, and second, led by Dmitry Medvedev, then president of the Russian Federation, and his administration, resisting such regulations. But the post-Arab Spring environment and the

Snowden revelation (2013) changed broader perceptions about how digital tools could influence regime change and provided Russian elites the opportunity to justify the regime security concerns about foreign interference (Pigman 2019).

The unique thing about Russian media freedom, on the spectrum between complete government control and universally free media, is the significant difference between media freedom online and offline. This disconnect has influenced the development of Putin's government coalition and his relationship with the middle class, as well as prompting early government adoption of tools like bots and trolls (Sanovich 2018). Media freedom started to be curtailed in Russia within the first months of Putin's presidency, beginning with Putin's September 2000 approval of the Information Security Doctrine of the Russian Federation. This policy move built the foundation for the official state information security policies and set up the media classification system (Barbashin et al 2014). Since Putin's first inauguration as president in 2000 to his third term in 2012, Russia's internet policy evolved from a response regime to a control regime.

In the wake of Putin's re-election in 2012, activist took the opportunity to demonstrate in a new way the internet's potential for political mobilization. This increased activity around social and political concerns have attracted the attention of the state, which has reacted by tightening regulation around internet security (Kelly, Cook, and Truong 2013). A bill President Putin signed into law in December of 2013 was used to block much access to majority of the independent media who were reporting on the Ukraine conflict. The bill grants the Prosecutor General authority to federally blacklist sites containing extremist content or encouraging the public to participate in unsanctioned action (Kelly et al 2015). In February 2014 the state added the "Lugovoi Law" to existing

"blacklisting" policy, which gave the state security apparatus the ability, without court order, to block access to sites that call for mass riots or publish "extremist" content. The ambiguous wording allows the Kremlin a broad interpretation of "extremist" language; almost anything contrary to official Kremlin stance could qualify (Barbashin et al 2017). In May 2014, the government extended legal oversight and limited the ability of citizens to publish ideas and information in relative anonymity by requiring certain online social media writers or bloggers to register with telecommunications regulation. These state regulations empowered Russia's online regulator, Roscomnadzor, which holds an effective monopoly on censorship, and may block online sources at any request of the prosecutor general's office. Censorship traditionally occurs as official monitoring or legal actions, but now Denial of Service (DoS) attacks or mysterious "technical difficulties" are more commonly occurring, especially with influential articles or news items criticizing Kremlin's policies. Content producers and service providers are regularly pressured by telephone to remove critical material, and even owners or shareholders in the companies that own websites may face legal prosecution or police action. This form of censorship-by-threat pressures some providers into a kind of self-censorship (Kelly, Cook and Truong 2013).

Russian political elites, when focus strays from the threat to regime security, instead are discussing the threats cyberspace represents to society, public safety, and community exemplified by the excessive freedom of an unrestricted internet, which allows criminals and extremists the same access as regular citizens (Pigman 2019). Controlling the public narrations to "achieve and maintain public harmony and of the

spiritual renewal of Russia"[18], as underlined in the Information Security Doctrine (2000), has a high national priority for Russia in the information sphere. Media control, disinformation and propaganda are the Kremlin trademarks to manipulate its own citizens as well as other countries' citizens, where Russia's interests are at stake.

Russia's Information Security Doctrine identifies the following provisions as two of the greatest dangers in the sphere of spiritual life: "Deformation of the system of mass information owing to uncontrolled expansion of the foreign media sector in the national information space" and "the inability of contemporary Russian civil society to ensure the formation in the growing generation, and maintenance in society, of socially required moral values, patriotism and civic responsibility for the destiny of the country". Shortly after Putin's ascendancy to power, he established "Kremlin's monopoly on the truth", thus, anytime a media outlet, a public figure, or civil society challenges or interprets Moscow's domestic or foreign policies, their act is perceived as a threat to national security (Barbashin et al 2017, 202).

To mitigate threats from media outlets and civil society – that experiences a significant awakening following post-election unrest in early 2012 (Kelly, Cook, and Truong 2013) – in addition to control and censorship (discussed above), Putin's administration relies on propaganda. Comparing Putin with Joseph Stalin, Igor Yakovenko, a Russian journalism professor said, "if Stalin was 80 percent violence and 20 percent propaganda, then Putin is 80 percent propaganda and 20 percent violence" (cited in Pomerantsev 2015, 40). In contrast to a Marxist-Leninist presentation of

[18] Information Security Doctrine of The Russian Federation (Approved by President of the Russian Federation Vladimir Putin on September 9, 2000). Available online at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf

doctrine, Putin's administration has focused on shaping worldviews through a distinct control of prevalent news media, beginning with print and television, and progressing more recently to the internet. The Putin presentation of worldview is more implicit than previous doctrines—for one thing, it is more visual and sensory than doctrinal. The glamorized branding of Putin's character and effect communicates that, as well as the broadness of its appeal, defined more by marginalizing and delegitimizing opposition than by any specific doctrine (Laruelle 2017).

Since 2000, Vladislav Surkov, assistant to the president, has been cultivating a superhero image of Putin through series of disinformation campaigns and propaganda techniques. The domestic political campaigns have been as much under Surkov's control as televised media is. Surkov and his successors, not content with mere propaganda, have sought to control the entirety of civil and societal discourse. They have gone so far as to put words in the mouths of political opposition players, in order to set up a favorable contrast for Putin, by use of direct telephone line access to politicians. Other tactics actually made use of the fervor of what might be potentially dissent civil movements, such as the sponsorship of modern art festivals—and the concurrent sponsorship of nationalist youth movements which reject modern art and liberal thinking. Along with generating state-sponsored NGOs that are loyal to the Kremlin, and pacifying liberal elite groups, all these strategies allowed the Kremlin unrivaled control of the civil dialogue and how it is presented domestically and internationally (Pomerantsev 2015c). Putin administration deputies reportedly call up chief editors regularly to coordinate the Kremlin's official perspective on news and policy items distributed to mainstream media outlets (Barbashin et al 2017).

To alleviate any cyber threat that might endangers regime security, public safety or social norms and cohesion of the Russian society, Moscow has developed two major mechanisms for social control: The Russian Internet (RuNet) and data localization policy.

4.3.1 The Russian Internet – RuNet:

In general terms, the Putin administration has shown positive attitude toward the Internet's advent and progress, a move that has favored the young and energetic political image of Putin by association. The 2001 e-Russia initiative demonstrated the administration's interest in the growing influence of Internet technology within the broader economy and society. At the same time, high-profile propaganda sites proliferated, fueling concerns among the media community, which was already seeing increasing restriction of the press and television media. Early on, the public generally perceived computer networks as an extension of *Blat* – the Soviet practice of contact building through bartering goods and services, typically functioned to avoid the restrictions of a planned economy. The RuNet will likely continue to be defined by its contrast to Western infrastructure represented by its unique characteristics, including the huge geographic area it covers, the specific interpretation on intellectual property rules, and a centralized media structure (Bowles 2006). Russia's weapons of choice vary from China's, resorting to censorship and intimidation over application-level blocking, shutdowns, and infrastructure barriers. Recently, the idea of an emergency "kill switch" for the Russian Internet has gained popularity, allowing government to disconnect the internet in the possibility of unspecified crisis. The "Law on Communications" was revised by the ministry of Telecom and Mass communications in August of 2017, with

specific amendments that increased government control over infrastructure and traffic on the internet by transferring the national domain zones ".ru" and ".pф", and the entire system of traffic exchange points to the government (Kovaleva 2018).

4.3.2 Data Localization Policy:

Freedom of information and distribution is a hallmark of the Internet Age, but as security concerns have risen in response to cyber threats, governments are increasingly adopting the pre-emptive data localization regulations that limit cross-border data transfers (Wei 2018). Since Snowden's leaks and revelation about NSA global surveillance in 2013, many countries moved to draft data localization laws, requiring that certain types of data about a nation's citizens or residents initially collected, processed and stored locally within its territory before being allowed to transfer outside that country's borders. However, in the case of Russia, domestic and regional concerns such as censoring information, controlling dissents and regime stability also contributed significantly to the country's data residency laws (Newton and Summers 2018).

The final amendments to Russia's data localization bill came into effect on September 1, 2015. The law requires "the processing of personal data of Russian citizens be conducted with the use of servers located in Russia. Operators that process personal data of Russian citizens have to notify Roscomnadzor of the location of their servers where such personal data is stored". Accordingly, the *Roscomnadzor*, Russia's data protection authority, established a Register of Infringers of Rights of Personal Data Subjects, which blocks the websites of Russian or foreign data operators if they violate

the law.[19] Russia's information sovereignty policy has major security, as well as economic, implications.

The legislation of data localization represents a strategic continuation of Russian governance priorities, which in the realm of cyber operations seek to control Internet communications, a resolve that only strengthened following the Arab Spring and the Snow Revolution protests. The role of internet and social media platforms as a free-speech form and political mobilization tool put it directly in Moscow's crosshairs, even as tens of thousands of Russian citizens rallied against fraudulent parliamentary elections. In the name of counterterrorism, the increased Information Security laws of 2016 served to embolden legal campaigns against dissenting domestic voices as they cracked down on extremist behavior. Recent economic sanctions from the U.S. and the EU have impaired the already-weak Russian economy, stunting its prospects for growth in IT and data storage infrastructure. In response, Russia has moved to repatriate information, indicative of increasing defensive tendencies, which serve to reward domestic economy and reduce the market influence of big data globally (Newton and Summers 2018). President Putin signed a data localization law in July of 2014, requiring any technology company that processed any Russian data to shift to hosting the information on local servers only by September 1, 2015. Privacy advocates expressed concern that local servers could increase government surveillance opportunities on citizen data (Kelly et al 2016). Both Russian and U.S. companies have moved data to Russian centers, though some failed to comply and were blocked temporarily. Apple, Facebook, and Google all complied, but LinkedIn

[19] "Amending Certain Legislative Acts of the Russian Federation as to the Clarification of the Processing of Personal Data in Information and Telecommunications Networks". Legislation/Russia. Available online at: https://wilmap.law.stanford.edu/entries/federal-law-no-242-fz

was blacklisted, the first social media network to be so banned. Roscomnadzor even required Google and Apple to remove the LinkedIn app from their mobile stores (Newton and Summers 2018).

Data localization is increasingly becoming an excuse for restricting platforms; LinkedIn was blocked in Russia for data localization compliance failure in November 2016 (Kelly et al 2018). Even Google, at some point, must subjugate itself to Russian jurisdiction, according to a Russian MP's comments. The MP also noted that mass media and information are high priority concerns for Russian defense against foreign aggression and noted that all sensitive internet resources would be subject to observation and review by Russian specialists (Russia Today 090914).

Apple was banned on January 1, 2015, from selling iPhone and iPad devices in Russia, a ban which applied to any device relying on iCloud, as iCloud data is not stored locally. The iCloud servers are U.S.-based, and so violate the data localization requirements. It is not the devices themselves, but cloud-based, non-localized applications, a category which includes some social networking sites (Rathinavel 2014). In 2014, Russian Parliament passed a bill that even prevents members of government from using some Apple products for any confidential or classified government information, because of data security concerns (Fitsanakis 2014).

4.4 Disinformation Campaign

According to *The Kremlin Playbook* – a Center for Strategic and International Studies report – Russia's major goal is destabilizing world order and generating chaos as both a means of regional advantage and distraction from aggressive endeavors. Within this

context, Russia sees critical state institutions and bodies, in addition to the economy, as essential sectors and targets for influence, if not for outright control. Political warfare, new media (a combination of social media platforms and proliferation of mobile technology), and cyber-warfare tactics are all means of pursuing that overall goal of destabilization (Quinn 2018).

The key element in modern warfare from the Russian perspective is the mind; this battleground, so to speak, logically makes information and psychological warfare the primary focus of troop development, weapons control, and strategic internal and external communications with the goal to morally depress armed forces and population in a targeted society (Berzinš 2014). Instead of open confrontation with NATO, the EU, or the U.S., which would openly test Russia's economic and military strength, Putin weaponizes information to sow chaos and doubt. By weakening unity and strengthening discord in domestic and international politics, Russia seeks to weaken opposition through disruption and distraction. The idea of a permanent war implies a permanent enemy, and in the current world order, Western civilization's values, culture, politics and ideology clearly stand out as the predominant permanent enemy. The objective in this situation is to reduce any need for military force, instead integrating the attacker into the enemy's military and civil population and garnering powerful internal support against the enemy from its own population (MacFarquhar 2016). At the 2007 Munich Security Conference, Putin exercised heavy criticism of the United States' international actions, accusing 'the West' and allies of fomenting international instability through illegitimate use of force, and advocating for a greater global effort to share international power and leadership with

rising economies. Every Russian aggression since that time – Georgia (2008), Ukraine (2014), Syria (2015) – has reflected its antagonism with 'the West' (Facon 2017).

Political warfare, in the Russian model, is both a means to enacting foreign policy goals and a potential pretext for military action. It goes beyond a simple hybrid approach and moves into a new generation of cyber warfare. As defined by Russian theory, victory means developing a buffer between Russia and the West, including NATO, the U.S, and their allies and partners, in addition to maintaining their own sphere of influence (Quinn 2018). As with China, the role of non-physical conflicts has increased in priority over the years. The Russian deputy General chief of Staff argued in 2008, following the Georgia conflict, that in future conflicts, the first concern for military forces would be disrupting the opponent's military-political leadership, as well as population, through modern information technologies. Weaponized information, he added, provide a path to gaining military advantage, even without a formal declaration of war (Pomerantsev 2015a). Russian intelligent officer trainees are invited in the 2011 edition of the "Information-Psychological War Operations" to consider their role successful when it acts on the population like invisible radiation—its presence invisible, but its effects distinct (Pomerantsev 2015b).

The first Kremlin target of disinformation campaigning is Russian civil society and its domestic interests are to isolate Russians from true information and to generate belief and support for Putin. A secondary target is the Ukrainian audience, including the Russian-occupied areas, with the goals of destabilizing competing political systems, including undermining the popular hope of Ukraine joining the EU. And the third target is of course the West, in which Russia hopes to spin information about its military

aggressions and occupations and destabilize the unity of the EU and NATO (Ogrysko 2016).

Under the Soviet Union, a clearer demarcation was made between internal and external disinformation operations and its actors, but in the late 2000s to the present, more informal actor networks were given the job of policing any internet criticism of the Kremlin, regardless of geographic borders. As the cyber-warfare component of foreign policy grew in strategic importance, the line between domestic and international policy was blurred, as the roles of various institutional actors began to overlap. This, as well as the aggressive cyber-warfare component of the current foreign policy, has led to a stunningly effective cyber warfare strategy (Soldatov and Borogan 2018).

4.4.1 Russia's Trolling Complex

Initially, the Russian government first developed bots and trolls for use domestically; however, Moscow has extended use of bots and trolls to coerce or even force foreign social media platforms to engage selective censorship of opposing narratives. The government doesn't want to censor social media platforms outright, but they certainly want to control the conversation. Bots and trolls as propaganda tools were used under Medvedev in order to engage opposition in online discussions. Under Putin, after 2012, these tools were also used to curb oppositions (Sanovich 2018).

Internet Research Agency operations began in 2013, modeled on the production lines of a high-end marketing office. Over a thousand people were employed and trained in "influence operations" in this context, working on specific targets, from Ukrainian and Russian citizens at first, to U.S. audiences later. The results are staggering—from what

we know now, the campaigns reached 126 million Facebook users, 20 million-plus Instagram users, 1.4 million Twitter users, and over 1,000 YouTube videos. Themes for each community target were chosen in order to reinforce tribalism, first of all. Most IRA posts simply reinforced the group sense of connection and togetherness, with occasional posts which denigrated "outsiders" to that particular community. Across all the targeted communities, two major themes have emerged—first, to undermine trust in mainstream media, and second, to promote the Russian perspective on the regional conflicts and Russian intervention (DiResta et al 2019).

The strategies employed by the IRA are no innovation; modern digital marketing techniques certainly informed the campaigns, from digital advertising of propaganda and disinformation across multiple platforms, to false personas and content mimicking real content from activist groups. The power of the IRA campaigns can be partially traced to the extended reach of target audiences created by the variety of platforms and formats. The mimicry of legitimate accounts generated an additional level of trust for the false ones. Another advantage of the diversified strategy allowed the IRA efforts to continue even after detection, by redirecting traffic to a different platform if an account was suspended, and even using complaints of suspended accounts on one network to garner support on another. Analysis of the IRA dataset shows that Facebook and Instagram posts and ads were specifically and strategically targeted in two ways: first, posts that appealed to common narratives in a targeted group (e.g. Black, LGBT, or diasporic communities). And second, contents intended to provoke outrage from the same audience. The Twitter dataset reveals an extended and highly engaged run of participation from false accounts, some of which spent months establishing authentic user history in order to gain

meaningful influence over targeted audience communities. Some accounts were effectively incorporated into the national conversation up until the accounts were suspended (Howard et al 2019).

Social media platforms create a powerful computational infrastructure for propaganda use, with their unique ability to simultaneously message both large audiences and targeted individuals. The functionality that attracts advertisers to take advantage of social media also holds value to political and foreign actors (Bradshaw and Howard). Blogging and social media sites like LiveJournal and the Russian platform VKontakte were co-opted into service by the Kremlin as propaganda machines during the Ukraine-Russia crisis. Interpret Magazine reports that the Kremlin hired over 250 people to act as internet trolls, each of whom was paid almost $1,000 per month to work on 24-hour social media campaigns, comprised of creating and maintaining social media groups, commenting on mainstream media outlets, and meeting messaging objectives, including attacking the pro-Ukrainian media and Western news sources that were too openly critical of Russia in any way. By using multiple puppet accounts – fake online identities – these troll armies or 'web brigades' promoted ideological goals by spreading fake photos and videos (Al-Khateeb and Agarwal 2016).

Russia Activities in the United States (Presidential Election 2016): The U.S. social media platforms provided data on the IRA's activities to the Senate Select Committee on Intelligence, which revealed distinct and sustained manipulation of U.S. public through social media and Internet platforms. Leveraging decades of experience manipulating public opinion in Russia, the IRA targeted U.S. voters through major social media

platforms with content meant to polarize users and to undermine democratic ideals. Among intentional Russian online targets were extreme conservative communities, and populations especially sensitive to issues of race and immigration. Fake accounts created by the IRA posed as U.S. users from both right and left of political spectrum. These accounts often operated from the same computers and entered political discussion communities and activist groups of a diverse range, including black activist communities and both right and left-oriented groups, seeking to aggravate social divisions and polarize conversations (Howard et al 2019). The IRA sought to create a perception of their accounts as trusted brands—in the case of the targeted Black communities, this was achieved through connection and promotion by legitimate cultural groups. Another tactic was to pursue a lot of audience growth across many parallel accounts, so that users who followed one account were prompted to follow others, creating legitimacy through numbers and exposing the community to repetitive messaging (DiResta et al 2019).

Russia Activities in the Baltic States: Driven by anxiety about the rise of Western influence made possible in the vacuum of post-Soviet space, during which many key Russian leaders were displaced by popular elections, the Kremlin has formed many proxy groups to buttress its foreign policy. The Kremlin employ both internet trolls and NGO affiliates for disseminating narratives. These pro-Kremlin policy support groups advance key ideology concepts, such as Eurasia-centrism and Russian World, and also provides outside justification for Russian actions and policies. One unique example of this is Russian-affiliated NGOs in Latvia, where the Russian resident communities represent both the target group for disinformation, as well as the means of spreading it. The March

16 – an annual commemoration of soldiers who died in WWII, when some members of Latvian Legion veterans honor their fallen fellows at Regia's Freedom monument and pro-Kremlin media and NGOs frame it as a symbol of Nazism in Latvia – events show especially the connection between Russia's foreign policy goals and the involvement of Russian-financed and supported NGOs within Latvia (Lithuania Tribune 090415). In such situations, language is a key element of preserving specific cultural communities, in which the 'Russian World' naturally takes precedence over any other cultural association. From that strong natural connection, what emerges is a diaspora-identity, which connects community, defines politics, and requires cultural diplomacy (Pieper 2018).

4.5 Russia's Cyber Diplomacy and Norm Building

As early as 1998, Russia raised global awareness of the risks of cyber technology, even introducing the first resolution on 'Developments in the Field of Information and Telecommunications in the Context of International Security' in the United Nations' General Assembly. Shortly thereafter, Moscow introduced a similar resolution, with two additional points: one, that cyberspace had the potential to be misused for military objectives, and two, that international community should seek to mitigate the risk by agreeing on principles of governance (Chernenko 2018).

In fall 2011, Russia in partnership with China, Tajikistan, and Uzbekistan introduced an *International code of conduct for information security*. Later, the same coalition (SCO states) proposed a UN convention on *ensuring international information security*, which required member nations to oversee and restrict any information source

that motivates "Three Evils"[20] –terrorism, secessionism, and extremism – "or undermines other countries' political, economic, or social stability, or their spiritual or cultural environment."[21] The Chinese-Russian led proposal seeks to define information communication technologies that violate individual state laws as weapons, even social media channels. After multiple attempts and revisions, the Russian-backed cybercrime resolution passed at the UN in fall 2019, although the U.S. protested that the measure would impede efforts to address Internet crimes. The resolution ostensibly establishes guidelines for a cyber-crime prevention convention and accompanying committee. But some human rights groups have seen it as an effort of the Kremlin to expand state-backed internet control policy (Vavra 2019). More importantly, the resolution created an OEWG (Open-ended Working Group) on the topic of cybersecurity at the United Nations to run parallel to the already existing UN Group of Governmental Experts (GGE), effectively bifurcating the discussion of cyber norms at the United Nations. This could allow Russia to use the OEWG as a forum for the reinterpretation of previous UN GGE reports to better align with Russian preferences for internet governance (Weber 2020).

Further, participating states would agree to not use communications technologies or networks to act aggressively, threaten international peace or security, or proliferate information weapons or technologies. The proposal reveals to security professionals the Chinese and Russian perspective that the free flow of information is a direct security threat, especially in the wake of the Arab Spring demonstrators' use of social networks.

---

[20] Human Rights in China, *Counter-Terrorism and Human Rights: The Impact of the Shanghai Cooperation Organization* (New York: Human Rights in China, 2011) cited in Sarah McKune, "An Analysis of the International Code of Conduct for Information Security", *The Citizen Lab*, University of Toronto, 28 September 2015.
[21] "Freedom on the Net – Russia", *Freedom House*, 2012.

The free flow of information concept in the U.S. is, of course, considered an essential and universal right. The Obama administration document “International Strategy for Cyberspace” stated that “arbitrary restrictions on the free flow of information” are used by many governments to subdue opposition or dissent (Farnsworth 2011).

Another mechanism Russia advocate for its cyber governance model and norms is through weaponization of civil society, think tanks, and academia. For instance, One of the Russian Security Council’s channels for exercising influence outside its borders, the Information Security Institute (IISI) is clearly dedicated to advocating Russian policy points on information security internationally in various ways, including at its annual conference in Garmisch-Partenkirchen in Munich, Germany. The program and the conference resolution issued by the IISI at its fourteenth annual event in April 2017 reflected an agenda obviously focused on major Russian initiatives, including discussions on state cyber-sovereignty. In addition, the institute takes part in bilateral meetings with officials and experts across Eurasia, in which advocating for the Russian perspective on information security is the openly stated goal (Pallin and Oxenstierna 2017).

During a press conference at the Wuzhen Summit, Aide to the Russian President and former Minister of Communications and Mass Media, Igor Shchegolev, highlighted cybercrimes, cyberespionage, lack of international norms for cyberspace and hegemony of the Western-style cyber governance led by the United States as major cyber threats and challenges facing states. He explained, fate of the Internet and the future of cyber governance, as either a global common good for information flow or fragments of national and regional networks, to a great extend depends on the way the global community responds to such cyber threats. Further, he emphasized, it’s important to

ensure that the monopoly of a state is not merely traded for a monopoly of commercial enterprise; regardless of how much multilateral participation and a thriving, diverse base of organizations are discussed, there is no guarantee that participants will comply with any established rules.[22]

4.6 US-Russia Cyber Relations: Challenges and Responses

The Russian strategic challenge is underpinned by two background elements that are important to understand (for US and EU), one being 'the West' as an idealized enemy. This element has grown in popularity following President Putin's foreign policy vision presented at the 2007 Munich security conference. The second, it is the prevalence of Russia's military power.

Russian perspective differs significantly from the Western when it comes to the nature, potential, and use of cyberspace. Of particular concern to Russia is the free exchange of information, including information which might be perceived as threatening to society or state, made possible by the limited relevance of national borders in cyberspace. Deep in the Russian list of cybersecurity concerns is the perception of content as potential threat, while the West is far more concerned with hostile code, vs. hostile content. Protecting the sovereignty of the national internet takes priority for Russia; this essential ideological divergence with the West has so far, despite Russia's efforts to invite other states into their definition of norms, prevented agreement on common principles or cyberspace behavioral governance (Giles 2016).

---

[22] "Russia praises China's initiative to host first global Internet conference", *Russian News Agency*, 19 November 2014. Available online at: https://tass.com/world/760667

Further, Russia favors a secure international regime of oversight, while the U.S. sees cybersecurity first as a law-enforcement paradigm that should be governed through mutual cooperation and enforcement. And just as both nations see the economic opportunity, as well as the heightened risks represented by cyberspace, to the U.S., that risk is not political in origin, but criminal, and the Russian insistence, therefore, on broad international oversight seem highly prescriptive and restrictive. The U.S. does not want international oversight and collaboration on governance to favor repressive state policies or legitimize State censorship (Arimatsu 2012).

In fact, the term preferred by Russia in these conversations is 'information security,' vs. the more commonly used term in the U.S., 'cybersecurity,' which subtly indicates that Russia's security concerns are far more comprehensive than mere defense against attacks. Information security points to Russia's desire for state control over citizen information space. Maintaining control, not of just of secure identity information, but of the social space the internet represents, appears to be a very prominent concern in the Information Security Doctrine of the Russian Federation released by President Putin in 2000. Essentially, each nation's approach to cybersecurity is a direct reflection of each nation's ideological belief about the role of the State in a society (Ibid).

Among western nations, the "free flow of ideas, information, and expression," is regularly cited as a fundamental principle, including by UK Foreign Secretary William Hague at the London Conference; at the same event, however, Minister Shchegolev continually added significant caveats when this principle was mentioned, such as how freedom of information should yet be subject to both national policy and national security (Giles 2016). While the U.S.'s dependency on information technology overall increases

its risk when it comes to malicious cyberactivity now, it has also developed domestic professional expertise and customization, while Russia has heretofore depended largely on off-the-shelf hardware and software. The lack of deep expertise may be the greater vulnerability in the long term; perceiving itself at a relative disadvantage, Russia hopes that an international treaty may level the playing field (Arimatsu 2012).

Disinformation Campaign: Domestic trolling activity in Russia continues to obscure voice of dissent on the internet and undermine any political action against the regime, while activity beyond Russian borders supports a strategy of disrupting the international liberal order to Moscow's advantage (Kurowska and Reshetnikov 2018). The watershed moment of Moscow's acknowledged interference in U.S. election in 2016, along with its domestic political implications and those for international affairs, served to make the Western nations acutely aware of Russia's perspective and behavior. Beyond propaganda and internal security, Russia's information security strategy reveals a significant, comprehensive, integrated approach to information operations and cyber-operations (Maurer and Hinck 2018).

Volodymyr Ogrysko, Ukrainian former foreign minister (2007-2009), suggests a set of recommendations to counter Russian disinformation (Ogrysko 2016), which begins with increasing the pressure on Russian information spaces in an intentionally systemic approach, by which the most effective ways to influence the largest groups of citizens with correct information can be determined. In addition, NATO recommends legal action, nationally and internationally, to close loopholes to outside access and reduce Russian propaganda and infiltration opportunities. It will also be important to spread accurate

information about the real effects of the Kremlin's actions. The contrasting opportunities for Ukrainians and their absence for Russians, due to Kremlin's behaviors, such as the concept of a visa-free regime and why it would make sense, may be an effective talking point. The key point that the current regime is not creating positive advantages for average Russian citizens should be consistently, but sensitively, part of the West's messaging.

Cyber Governance: In 2011, Russia and other nations (some who are members of the CIS, CSTO, and SCO) draw a line at the impasse of Internet sovereignty, strongly prioritizing national control of internet resources within each state's physical borders and legislative power (Giles 2016). The draft Convention on International Information Security, in Article 5, states that "each member state is entitled to set forth sovereign norms and manage its information space according to its national laws." The governments seeking this kind of control in effect want to impose national barriers on cyberspace, an approach that would be disastrous for internet freedoms, and represents a direct opposition to the U.S. approach. As Secretary of State Hillary Clinton said in 2011, national control over the internet would allow each government not only to restrict free flow of information and potentially undermine human rights, but to affect the interoperability of international networking (Ibid).

4.7 Concluding Remarks

The policies of the West, which are increasingly perceived as inherently threatening to Russia's interests, are one of the major international factors that appear to influence Russian international actions. In consequence, the Russia that once wanted to join the

Western-dominated world order instead now prefers to work toward positioning itself as a leader a multi-polar world order. Where post-Soviet Russia showed signs of wanting to integrate in the global economy, Russia now only engages selectively, and fosters further political and business ties with emerging economies, especially China (Kanet and Sussex 2015). By allying with China, Putin has effectively made Russia a valid competitive global force. The multipolar world Putin envisioned at his first authoritative election has effectively become a reality. Although Russia does cooperate with China, there are different hurdles it faces in imitating Beijing's information control model completely. Where China's large domestic market, as well as the strength of private Chinese enterprise to provide sufficiently competitive native social media platforms, make domestic internet functional enough to satisfy its audience. Russia's technological ability and networks are not as deep, and it has struggled with implementing inspection tools and bans of specific apps like Telegram (Weber 2020).

Putin's strategy, since 2012, has been founded in political insulation and defined by 'national community building' and 'mental self-determination;' a foundation which has been defined by a practical, rhetorical, and ideological distance from the oppositional 'other' – Western influence. To achieve its strategic goals in addressing its national cybersecurity dilemmas (discussed in chapter two), Russia's preferences are as follows:

- <u>Stimulate the economy vs improve national security:</u> Economic stimulation is a high priority and digital and emerging technology depend heavily on access to global software, hardware, and process innovations. With Russia's digital trade policy focusing more heavily on restrictive security around data flow and localization, this presents barriers of time, convenience, and access (Meltzer

2019).[23] Two other factors that potentially slow e-commerce trade growth within Russia, another study shows, are the diversity of language regions, and the slow and expensive mail delivery system (Sadyki 2017).

- Infrastructure Modernization vs. Critical Infrastructure Protection: government order from 2018 shows a government proposal to ban the use of foreign information technology for critical national infrastructure, as well as potentially prohibiting key facilities from using security or support provided by foreign organizations. Some rules around foreign software use have already been introduced to ensure that no back-door security loopholes can be used by foreign intelligence; the rules require outside software, especially security products, to be reviewed by Russian engineers before import and sale within the country.[24] Ideally, striking the balance between modernization and security is made easier when indigenous technologies dominate, and so those are broadly advocated for adoption by the government, although indigenous social network platforms, search engines, and mail platforms create a functional ghetto for businesses who may want to reach a more global audience (Sadyki 2017).
- Data Protection vs. Information Sharing: Global data flow enables goods and services from both direct-to-consumer and business-to-business value chains to move effectively; however, Russia's extreme restrictions around cross-border data movement and localization requirements create a higher cost for companies who

[23] Also see "Data Flows, Online Privacy, and Trade Policy". Congressional Research Service. 11 March 2019.
[24] "Russia to ban foreign information technology companies for national infrastructure". CDE News. 11 February 2020; Schectman, Joel, Dustin Volz, and Jack Stubbs. "Under pressure, Western tech firms bow to Russian demands to share cyber secrets". Reuters. 23 June 2017.

operate on both sides of the border (Ferracane, Lee-Makiyama and Van Der Marel 2018).

- Freedom of Expression vs. Political Stability: Increasing data sovereignty was a distinct priority for Russia recently, leading to increased restrictions on VPNs to prevent users from accessing sites that do not meet localization requirements outside the country. Freedom of expression has certainly been stilted by a government averse to any open criticism; since 2014, blogs with over 3,000 monthly visitors are required to register as media outlets, and bloggers are legally liable for “accurate” content (Shahbaz 2018).

Chapter Five: Iran's Cyber Posture
Perception, Organization, and Behavior

The importance of cyberspace is as significant of an opportunity as the Islamic revolution itself.

Ayatollah Ali Khamenei
Iran's Supreme Leader

15 June 2009

Following Mahmoud Ahmadinejad's re-election, pro-reform candidate supporters of Mir Hossein Mousavi clashed with riot police in Tehran in spite of a ban on public protests. Ayatollah Ali Khamenei's statement only praised the high voter turnout and called for public calm and unified celebration. The Green Movement – supporters of Mousavi in coalition with a broad range of opposition forces – was prevented from forming a broader support network in Iran by the simple expedient of keeping its leaders under house arrest, if not detaining them outright. However, led by groups of women and students, Iran's fragile civil society grew quickly in strength, empowered and connected through social strata and geographic distance by the Internet and social networks. Opposition supporters overwhelmingly were members of the Facebook generation, and when public protests were no longer tenable, they took their dissent to cyberspace.[1]

July 2010

A powerful internet worm repeatedly targeted five industrial facilities in Iran over a 10-month period, empowered by a novel structure and several previously unaddressed Windows vulnerabilities. Many have suggested that only a "nation or state" could have been behind a virus this sophisticated.[2]

5.1 Introduction

The Green Movement in 2009 certainly served to make the regime acutely aware of social media's potential to fuel dissent and protests, despite a rapid official dismissal of

[1] "Ahmadinejad Wins Iran Presidential Election". *BBC News*. 13 June 2009; Milani, Abbas. "The Green Movement". The Iran Primer. 6 October 2010.
[2] Fildes, Jonathan. "Stuxnet worm 'targeted high-value Iranian assets'". *BBC News*. 23 September 2010; Fildes, Jonathan. "Stuxnet virus targets and spread revealed". *BBC News*. 15 February 2011.

the role social media played in the unrest. The second wakeup call to the regime was 2010's Stuxnet virus crisis in Iran. Stuxnet is supposedly created and launched by U.S. and Israeli cyber forces and is believed to be the first offensive cyber-weapon use that sabotaged a physical industrial facility—Iran's nuclear program (Eisenstadt 2016). However, Iran's cyber posture, domestically and to the great extent internationally, has mainly formed in response to its perceived cultural threats (i.e. the West's soft war against the regime) rather than a targeted cyber-attack by a foreign actor (e.g. Stuxnet). Following the Green Movement protests in 2009, Iranian authorities have recruited Chinese assistance in policing domestic internet sites, social media, and Virtual Private Networks (VPNs) in order to shut down outside influences and internal dissent. Since 2009, cyber police unit (FETA) has been dedicated to enforcing Islamic cyberspace decorum, specifically targeting both internet crimes and networks of dissent (Lim 2013).

For the Islamic Republic's hard-liner faction, including the Supreme Leader, enmity towards the United States and anti-Westernization rhetoric are fundamental pillars of the revolution and core to the regime's identity. The four main points of contention that shape both foreign policy and cyber policy discussions between the West and Iran are US influence in the Middle East; issues of sovereignty and intervention in Iran's domestic affairs, including democracy promotion; Israel's existence; and rivalry with Saudi Arabia. Since the revolution in 1979, Iran's foreign policy adventures "is framed as an effort to counter these evils and nearly every domestic agitation is attributed to American and Zionist plots" (Sadjadpour 2017, 8).

Iran among most Middle Eastern states has the potential to engage in cyber warfare; it tops some ranking lists among the top five, along with the U.S., Russia, China,

and Israel. While Iran's military cyber policy is still largely focused on defense, the distinction between offensive and defensive means is becoming difficult to define (Kevjn 2013). Cyber-operations have become one way for Iran to demonstrate how a nation with weaker military capability can yet contend with adversaries. Through cyber-attacks and retaliations against both foreign and domestic enemies as well as cyber-attacks in Israel, Saudi Arabia, and the United States, Iran has increasingly relied on cyber-operations for monitoring enemy activities, communications and controlling internet access (Nye 2010). Domestically, the Iranian government is working toward their own alternative internet search engine and seeks to ultimately implement an Iran-only internet network, intentionally slowing regular internet speeds to discourage users (Kevjn 2013).

5.1.1 Ideational Component

A strong national identity not only shapes cultural expectations, aspirations, and collective action, it frames state interests, political discourse, and practice; Iran's national identity underwent a fundamental restructuring after 1979. The concept of *Velayat-e Faghih*, originally a social principle strictly intended for society's weaker strata became, under Khomeini's influence, the 'rule of the jurist,' in anticipation of the Twelfth Imam's reappearance, effectively fusing religion and politics (Kevjn 2013). The political regime of the Islamic Republic, the remnant of the followers of Ayatollah Khomeini, has seen a deep divergence between conservative and moderate factions, each represented by a prominent figure from the early post-revolution. On the conservative side, Seyyed Ali Khamenei, the current Supreme Leader and former president, and Mousavi, 2009

presidential challenger, and former Prime Minister, on the moderate side (Esfahlani 2009).

According to the secretary of Supreme Cyberspace Council, Abolhassan Firouzabadi, Iran does not perceive cyberspace to be merely a technological tool and information superhighway which supplements society; rather, leadership sees the cyberspace as a system with the potential to bring new societal movements to life and which embodies a goal of the new civilizational establishment (Khoshnevis 2018). Tehran's civilizational interpretation of cyberspace has been echoed repeatedly in the Supreme Leader's statements. Ayatollah Ali Khamenei views cyberspace itself as significant a force as the Islamic Revolution, not only for Iranians, but for the world. Khamenei believes that cyberspace can provide Iran with a magnified cultural capacity for civilization-building and argues that the Islamic Republic's approach to cyberspace is neither passive nor offensive, but active and dynamic (Afkar News 122618*)*.

The first section will contextualize Iran's national cybersecurity strategy within its domestic politics and highlight its six priorities in cyberspace: to launch the National Information Network, to shape a second internet, to form a global coalition to challenge the American leadership/hegemony, to create a dominant discourse for an alternative governance model, to invest in indigenous high-tech industries, and to mobilize the general public in cyberspace to protect culture and traditions. The next three sections will map how these domestic priorities manifest themselves in Iran's foreign policy, in particular, creating a dominant discourse for an alternative governance model and mobilizing masses to protect Iran's culture and tradition in cyberspace which mitigate security challenges to Iran's cyber sovereignty, the survival of the regime, and domestic

stability. The final section will summarize the key arguments made in the chapter and highlights Iran's preferences in addressing its national cybersecurity dilemmas (discussed in chapter two).

5.1.2 Institutional Component

A prominent characteristic of The Islamic Republic of Iran's government is its dual structure, in which the president and parliament share an uncomfortable co-existence with a collection of unelected clerical and military institutions overseen and delegated by the Supreme Leader. Foreign policy, for example, is theoretically part of the president's purview over domestic and economic issues, but it is the Supreme Leader who determines all foreign policy strategy on a grand scale, and it is to the Supreme Leader that all security, military, and intelligence leaders owe allegiance. Elected establishment in the Islamic Republic necessarily has to work with, or in many cases, under, the Supreme Leader's unelected delegate institutions. Ayatollah Khamenei serves as "balancer-in-chief" to harness this elite-led competitive set of factions into some kind of efficient direction in the interest of governance, however, this style of government can't help but be marked with periodic vigorous and public altercations. Within established boundaries marked by an acceptance of the political status quo as well as commitment and loyalty to the principle of *Velayat-e Faghih*, incumbent political elites are free to operate competitively, pushing the interests and agendas of their respective institutions, in continual bids to re-shape boundaries (Kevjn 2013).

Supreme National Security Council (SNSC) is the highest political body, where grand strategy and regime's foreign policy on critical issues is debated. While president

has some weight over the foreign policy, SNSC and the Supreme Leader remain the major decision-making actors. The parliament, the Guardian Council, the Expediency Council, and the Islamic Revolutionary Guard Corps (IRGC) also influence Iran's foreign policy. All international agreements and treaties must be approved by the parliament, however, the Guardian Council, which members (six clerics and six jurists) are appointed by the Supreme Leader, has veto power over the parliament's decisions. At the event of any disagreement/conflict between these two governing bodies, the Expediency Council, a clerical institution under the control of the Supreme Leader, act as an arbitrator. Lastly, the Quds Force, the IRGC's branch responsible for extraterritorial operations, plays a significant role in the Islamic Republic's regional policy and the export of the revolution (Beehner 2006).

"I'm not as worried about economic and political issues as I am about cultural issues. I can't sleep at night because of cultural concerns", the Supreme Leader once said. The importance of cyberspace in the eyes of the Supreme Leader is so great that he emphasized, "If I were not the leader of the revolution today, I would definitely be the head of the country's cyberspace force". Iranian Supreme Leader Ayatollah Ali Khamenei's efforts to centralize control of internet communications under his authority is one indicator of how critical the role of digital communications is considered by Iranian leadership (Hawzah News Agency 120418*)*.

To further centralize decision-making, Khamenei implemented the Supreme Council of Cyberspace, a 27-member body, in March of 2012. Although Iran's president functions as the chair, individual members and organizational representatives are handpicked by the supreme leader, the president, or cabinet members with an approved

interest. The presidential administration's power, which leans toward a less-restrictive online policy, has been significantly hampered by this council. The formation of the Supreme Council of Cyberspace made several institutions that had previously influenced internet policy redundant, and most were merged into the council. While other organizations participate in shaping internet policy in addition to the Council, they're all more or less under Khamenei's authority (Center for Human Rights in Iran 010918).

For internet filtering decisions, oversight rests with the Working Group to Determine Instances of Criminal Content, a group that reports directly to the judiciary, under Khamenei's purview. Both the judiciary and the cyber-police retain the ability to directly shut down websites and applications, and to order content deletion and/or filtering. Although the president and administration have been relatively sidelined, officially internet policy decisions and the implementation procedures do fall under Ministry of Communications, which has allowed president (e.g. Rouhani) to occasionally intervene directly in policy decisions. In a key example, in May of 2014, Rouhani used a direct order to the Ministry of Communications to successfully reverse the block on messaging app WhatsApp that the Working Group to Determine Instances of Criminal Content had implemented (Center for Human Rights in Iran 010918*)*. Driven by the core motivation of Global Internet control, President Rouhani has championed the National Information Network's (NIN) continuous development since 2006. There is, however, a distinct divergence between Iranian users' desires and the state's, judging from the significant increase in the use of popular circumvention tools.

5.2 Iran's National Cybersecurity Strategy

Understanding how Iran defines cyber-related terminologies and its cyber priorities are important first steps to study Iran's behavior in cyberspace. There is no Farsi equivalent for 'cyber' or its derivatives (i.e. cybersecurity), instead, Iran uses "virtual space" to refer to similar concepts. Further, the Islamic Republic's elites consider cyberwar as one of the aspects of the soft war.

The Islamic Republic believes that the West, and in particular the United States, prefers not to engage in a conventional war with Iran; thus, the most effective way to attack Iran is through soft war tactics. The term covers a broad set of activities from cultural NATO to cyber war. In particular, the far-right faction of the regime argues that the disputed Presidential election in 2009 provided a good opportunity for the US to intervene in Iran's domestic affairs. Accordingly, the regime believes that college students are the main targets of this war, as the enemy wants to recruit the sharpest minds of the Iranian society. Similar to Russia, college students and university professors affiliated to the Basij are the main pool for the regime's cyber militia force – Young Officers of Soft War (YOSWA).[3] As a defensive strategic force, the state-backed militia's goal is to advocate for the Revolution's achievements, Iranian-Islamic life style, and culture of waiting for Mahdi.[4]

The Islamic Republic has identified eight areas that have highest priority for protection against the enemy's cyber-attack:[5]

---

[3] Basij is the Islamic Republic's paramilitary organization
[4] In Shia culture, the application of the term as a proper noun refers to a person who will be regarded as the savior, with Christ as his deputy, at the time of apocalypse.
[5] https://hawzah.net/fa/Magazine/View/5211/7149/871556

1. The Supreme Rule of the Jurist (*Velayat-e Faghih*): Both clerical and military elites in the Islamic Republic believe that the institution of *Velayat-e Faghih*, which is the authoritative source of the Supreme Leader, is the main ideological pillar of the state that prevents the regime from collapsing. Therefore, one of the key targets of the US soft war is to delegitimize and discredit *Velayat-e Faghih* as a whole, and the Supreme Leader in particular. Iranian elites believe color revolutions would have failed, had Ukraine and other states integrated *Velayat-e Faghih* into their political structure.
2. The Iranian-Islamic style of living: the Islamic Republic recognizes secularism as the biggest threat to its culture; stripping Iranian society from real Islamic values and replacing it with an American Islam.
3. The Media: the main battleground of the soft war is media and communications, and a country with weak media outlets and structures cannot survive in this war.
4. Students' spirit: Youth in general and students, in particular, should remain optimistic with respect to the Revolution and its achievements.
5. University campuses
6. Enemy's infiltration in the name of human rights issues
7. Enemy's infiltration in the name of ethnic and religious minorities rights
8. Public awareness: provide public education on how to identify enemies

Ayatollah Khamenei, in different occasions, states that the importance of cyberspace is as significant of an opportunity as the Islamic revolution itself. This space is like a river full of roaring water; as channels constantly add to its volume, the water becomes rougher. If a river's volume changes are planned for, with overflow channels, dams, or other controls, it will be an opportunity. If those controls are absent, the river will be a threat. Acknowledging the range of opportunities that online culture provides to states, a report published by the National Center of Cyberspace, affiliated to the Supreme Council of Cyberspace, argues that seizing this opportunity provides Tehran a historic prospect to propagate their revolutionary values. Tehran claims cyberspace gives the regime the best opportunity to provide the world access to the pure culture of Islam and Iran, while setting an example for young people. Majority of Military and religious elites also believe

cyberspace has unprecedented capacity for sharing the culture of martyrdom and sacrifice (Hawzah News Agency 120418*)*.

In a decree dated March 8, 2012, the Supreme Leader emphasized the importance of forming a decision-making institution for cyberspace (the Supreme Council of Cyberspace). The formation of this council, led to the important definition of the Supreme Leader's cyberspace goals, summarized below (Iran Hoshdar 031018):

- Active and innovative confrontation with cyberspace at the national and global levels and development to the extent of the regime's definite readiness to take advantage of opportunities and deal with threats.
- To minimize the country's reliance on other countries in the use of cyberspace and high-tech.
- To create attractive and rich local content and indigenous tech platforms to satisfy domestic demand.
- To encourage enthusiastic participation of loyal forces and grassroots organizations in a competitive environment for optimal use of cyberspace opportunities.
- To increase Iran's creative and innovative presence in cyberspace, regarding both hardware and software, in order to create a thriving online service culture.
- To regulate information exchange on/across the World Wide Web.
- Providing the necessary and optimized conditions of infrastructure to enable Iranian cyberspace to reach the highest level of security and health for individual users, the regime itself, and for all other actors in cyberspace.

Iran's cyberspace values: By 2025, the Islamic Republic's cyberspace will be governed based on wisdom, rationality, rule of law, responsible freedom, and cyber-sovereignty to protect and advocate the following ethical values (National Center for Cyberspace 0718):

1- Islamic beliefs, the values of the Islamic Revolution, morality, spirituality, righteous deeds, rejection of oppression or violation of members of society, rejection of seductive behavior and respect for the rights of all;
2- National unity, national trust and social discipline;
3- The right of the people to participate in the governance and management of cyberspace;

4- Free access to information for public awareness and the right to criticize and monitor the performance of public institutions while simultaneously respecting the rights of society and the individual;
5- The Iranian Islamic way of life and family-oriented values;
6- Health and sustainable security, citizens' private and public rights;
7- Independence in providing infrastructure and basic services needed by society, and independence from foreign domination;
8- Transparency, accessibility and accountability of authorities and civil servants;
9- Provide basic needs of citizens efficiently, effectively, sustainably, intelligently and economically;
10- Provide virtual and smart services related to the elderly, children, the disabled and the Physical and mentally disabled;
11- Protection of the environment;
12- Progress on the frontiers of science and knowledge and reliance on indigenous technologies and specialized domestic capabilities;
13- Domestic capacity-building and reliance on providing services internally;
14- Ethics, justice and systematization of services to citizens;
15- Sustainability and transparency of policies, laws and regulations.

National Information Network (NIN): Iranian internet users are able to use internal-content domestic tools to access like search engines, email services, and bank and trade transactions through the National Information Network (NIN), a state-controlled network. While global internet access is available, Iranian users must go through the NIN, which allows the state to separate international traffic from domestic. Ultimately, this allows the government the power to cut off Iranian global internet access at any point (*Center for Human Rights in Iran* 0118). The Supreme Council of Virtual Space (hereafter the Council) defines the National Information Network of as:

> the communication foundation/infrastructure of Iran's virtual space will be based on Internet protocols—including switches, routers, and data centers—in a way that denies any request from overseas to access information that is maintained in domestic data collection centers, thus providing a safe and secure environment for domestic private networks and intranets (National Center for Cyberspace 090517).

The Council identifies the followings as requirements to establish such a national network (Tasnim News 020414):

1- A network consisting of a communication infrastructure with complete domestic management.
2- An autonomous, protected and supervised network with the ability to communicate and interact securely with other networks, including the Internet.
3- A network capable of providing a variety of content and communication services to the entire nation, with a guarantee of quality and mobility.
4- A network with the capability to provide secure services, including cryptography and digital signature.
5- A network that provides secure and sustained communication channels among Iran's critical infrastructures.
6- A high-capacity broadband network and competitive tariffs, including data collection centers and domestic hosts.

The development of the NIN as an acceptable alternative to global internet access certainly included the development of additional infrastructure, tools, and services; the Iranian government's progress in these areas has been uneven.

Email Services: Three national email services were launched during the Ahmadinejad administration; *Chapar*, *Iran Post Company*, and *Iran Dot IR*; all three are still operational, but Iran Dot IR has gained precedence as the national email service, becoming integrated into the government's central information and communications portal, the "Electronic Dashboard System." National email services in Iran store information on both accounts and content on the state-controlled NIN. This includes access to the NIN storage centers, and all email content stored within. Although users could encrypt email content, very few people are familiar with content encryption processes and most average citizens would not have the technical skills to do that.

Data Centers: The NIN infrastructure is dependent in part on national data centers inside Iran's borders responsible for data storage, maintenance and processing, website hosting space storage, email communications and domestic communications between government

and non-government organizations and users. However, the Iranian companies connected with these data centers are unknown in their ownership and state affiliation, raising security concerns as the state's level of involvement is unknown. Now, in contrast to the first two decades following the Iranian revolution, Iranian citizens' communications and online activities seem to be increasingly out of the state's reach. Attempts to force foreign firms to comply with user data sharing have not been successful, and domestic alternatives to global services have not gained significant adoption locally as millions in the Iranian diaspora now live in nations where communications cannot or will not run over insecure Iranian platforms (Anderson and Sadjadpour 2018).

Search Engines: The national search engines (e.g. Parsijoo) in Iran represent one of the government's main means of information control across the NIN. Search engines determine the flow and presentation of content, so censorship and content filtering have a huge impact on access.

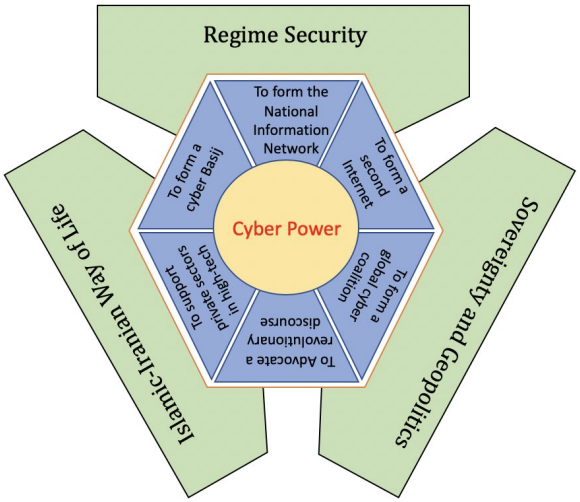
5.2.1 Domestic Imperatives of Iran's Cyber Posture

A growing body of research explores the impact of Iran's domestic political environment on its foreign policy decision-making process and international status. The scholarship on Iranian Studies demonstrates that stability of the regime; geopolitics and zone of influence; as well as the Islamic-Iranian way of life are major drivers of Iran's foreign policy behavior and international identity.[6] As this study shows, Iran's cybersecurity strategy is guided by the same features that power its foreign policy (Figure 9).

[6] For more information on regime stability and geopolitics see Radin and Reach 2017.

Reza Gholami (2019: 13-16), Head of Sadra Research Center on Islamic Humanities,[7] in *the Islamic Republic of Iran's Cyber Governance Approach – A Hexagon Model*, classifies Iran's major cybersecurity goals into six categories: to launch the National Information Network, to shape a second internet, to form a global coalition to challenge the American leadership/hegemony, to create a dominant discourse for an alternative governance model, to invest in indigenous high-tech industries, and to mobilize the general public in cyberspace to protect culture and traditions.

Figure 9 - Iran's Quest for Cyber Power and Its Domestic Political Environment[8]



First Priority: The National Information Network has three layers: infrastructure, content, and services. The Ministry of Communications and Information Technology has completed a major part of the first layer, and it will be ready to launch in two years. This

[7] Established in 2008, Sadra Research Center major goals are: to identify and address Iran's major research needs in humanities; to scientifically criticize the Western lifestyle; and to design and advocate for an alternative lifestyle based on Islamic-Iranian values.

[8] Source: Gholami, Reza. "the Islamic Republic of Iran's Cyber Governance Approach – A Hexagon Model", *National Center for Cyberspace*. Report No.6. June 2019; Hoyt, Paul. "The changing character of Iranian foreign policy." *Foreign Policy in Comparative Perspective: Domestic and International Influences on State Behavior, eds. Ryan K. Beasley, Juliet Kaarbo, Jeffrey S. Lantis, and Michael T. Snarr. Washington, DC: CQ Press* (2002).

infrastructure layer alone will provide, to a good extent, national security as well as user security, technologically, financially, and culturally. Additionally, users will enjoy higher speeds with more reasonable pricing. According to Gholami, the National Information Network protects Iran's national and religious values in cyberspace and seeks to prosper e-commerce, while also helping to purify cyberspace content, which assures family users of a degree of safety for children.

Second Priority: To curb the power of the American-Zionist alliance, Iran seeks to encourage other countries to form a second internet. China, Russia, and other nations have the necessary motivation to take on this endeavor, as well as the Islamic Republic. By pursuing its common interests with others, and of course by maintaining the NIN as foundational to the second Internet or transnational information network, the Islamic Republic is forging a significant role in creating and widening the ideological gap between the United States and other nations. Khamenei does not accept US leadership in cyberspace governance and has instructed the government to advocate for its own set of cyber rules and norms for the well-being of the world.

Third Priority: The Islamic Republic believes that cyberspace is currently governed by a functional Sheriff (the U.S.-led West), whose authority faces only limited accountability. There have been many attempts by various countries including China and Russia to raise cyberspace issues to the United Nations and its affiliated organizations, but these attempts have met with opposition and been undermined by the U.S. Therefore, Iran initiated a move towards the creation and strengthening of coalitions that seek to reduce the unlimited authority of the Americans in cyberspace. Gholami argues that a major step

to form such a coalition is to establish a Deputy Minister of Cyberspace position in the Ministry of Foreign Affairs and to train skilled and courageous officers for cyber diplomacy.

Fourth Priority: Gholami argues that a successful realization of a governance model requires creating abroad unifying metanarrative to advocate for such a model – a dominant discourse narrative broad enough to be inclusive of domestic and international actors, as well as the general public with the policies of the Islamic Republic could further facilitate norm building. Currently, the Islamic Republic lacks this metanarrative and sees competing perspectives, even discourses that counter regime policies to grow in the society. However, the document identifies the first step to creating a broader narrative is to create consensus among the elites.

Fifth Priority: The model urges the Islamic Republic to facilitate the financial foundation for startup companies in various indigenous high-tech and IT industries.

Sixth Priority: A significant element, Gholami claims, is to mobilize and educate the general public to defend national and religious values by generating value-based content and counter anti-regime/anti-value content: “We should be vigilant in supporting Islamic and revolutionary values in cyberspace and thwarting attacks on these values. However, in recent years, one of the focal points of our enemies has been psychological operations aimed at influencing public opinion” (16). The document does not limit cyber mobilization to the Iranian people and recommends the regime to extend its effort to reach like-minded people – whose most important concern is to protect the divine values – all over the world.

5.2.2 Iran's Soft Power

The Islamic Republic elites tie cyber war and the US soft power tactics to the Unipolar status of the international system after the Cold War and argue that to continue its supremacy, the US tries to extend its domination through cyberspace. Referring to the declining power of the US as discussed by US politicians and scholar such as Zbigniew Brzezinski and Noam Chomsky, the Iranian state-run daily *Siasat-e-Rooz* (close to the IRGC) concludes that cyber war is the US new strategy for maintaining its unilateral presence across the globe (Ghafouri 2013).

In 2010 the Supreme Leader and President Mahmoud Ahmadinejad emphasized a need to accelerate the Islamization of universities and educational spaces. As a result, soft-war strategy has been part of this fast re-education plan. Under the Ahmadinejad administration, the Ministry of Education organized a program with the help of 'political liaisons' to educate students, from elementary to high school, on the cyberspace technologies and soft war tactics. The Director of Education, in an interview with the IRINN mentioned that the Ministry of Education in coordination with many seminaries dispatched a thousand clergymen across the country to educate lecturers as well as students on the dangers and risks of cyber war. At the same time, Iran's Student Organization, to reinforce efforts of the Ministry of Education, started its cultural-educational program on coping with strategies of soft war under the banner of "cultural ditch" (Aftab News 102010).

An editorial in *Siasat-e Rooz* frames the danger of US soft war tactics against Iran by comparing them to the "road map of the greater Middle East" concept discussed under President George W. Bush's administration. The author argues that the unfolding soft war

is part of the US's new "road map" targeted at Iran's young generation, and a part of the greater scheme of a complex warfare against Islam. The author continues that the Middle East has been faced by a cultural camisado campaign waged across media like Hollywood movies, satellite programs, music, and internet. In particular, the author explains how the US and the UK, through English language programs, try to promote Western cultural values throughout the Middle East. The author recommends that the Ministry of Education should neutralize this aspect of the US soft war by re-structuring English language curriculums in both pre-college and higher education levels, based on scientific methods modeled after TOEFL or similar programs (Siasat-e Rooz 010812).

To emphasize the importance of the cyber war, the Islamic Republic holds a weeklong celebration to embrace and appreciate the works of the unknown soldiers of Mahdi, who counter the soft war tactics of the West. This cyber-brigade has a variety of tasks ranging from countering the cyber activities of anti-revolutionary and terrorist groups, to identifying the US drone attacks. This week generally coincides with the Mahdi's birthday (Siasat-e Rooz 062213).

Both civilian and military universities as well as seminaries stress the role of students and faculty in soft war. The representatives of the Supreme Leader at university campuses have addressed the university faculties and emphasized that university instructors are at the forefront of the battle against the imposed cyber war (Fars News 092612). They emphasized in order to counter the enemy's soft war students and faculty members should transform the mode of soft war into a 'holy' soft war, to sacralize it with the culture of martyrdom and resistance as well as through the promotion of Basij culture. They advocated that a defense of the Islamic Republic's monotheistic system and its

revolutionary values should be the pillars of Iran's youths when facing enemies in cyberspace (Fars News, 092412). The deputy commander of Imam Hossein University, a higher education institution affiliated to the IRGC, said "the enemy targeted the Islamic Republic's belief system and that to find our way we should just follow Mahdi's true representative at the time of his absence - the Supreme Leader" (Fars News 092012). Seminaries in Qom and Mashhad, two major religious cities, frame soft war as a way to counter either enemy's Shia-phobia propaganda (e.g. Saudi Arabia) or the spread of American Islam (a version of Islam that is not hostile to Israel). For instance, a Qom Seminary instructor insisted that the holy defense period – the Iran-Iraq war – must be a model to follow in battle against the enemy's cyber war. He argued that the main target of the enemy's soft war is the Muslim world, especially Shia Muslims (Fars News 092612).

The government officials also encourage other factions of the society to actively engage in the soft war. Women are equals on this cyber-front, fully expected to engage in defending the Islamic regime, and even to encourage their families and children to join them. For instance, the Director of the Organization for Women's Affairs and Family said that women should play an important role in the battle against soft war, just as they did in the Iran-Iraq war, especially as the enemy has targeted women through fashion and the Western lifestyle. An IRGC commander, Hossein Hamadani, even said that there are no limitations on female involvement in the "soft war" of cyberspace, as opposed to the "hard war" of physical space (Golkar 2015). The Director of Islamic Affairs of the Isfahan Province said the enemy's tactic today is to invade intellectual boundaries instead of attacking geographical borders. In order to continue to battle the US soft power, we

should strengthen the religious and cultural foundations of Iranian society. He also emphasized the necessity of equipping all available forces in the country to deal with the cultural invasion (Fars News 092412).

Law enforcement officials and Imams also propagate for encountering the West's soft war against the regime. The Disciplinary Force of the Islamic Republic (NAJA), a law enforcement body, announced that in order to mitigate cybercrime, they have established a cyber police unit (Fars News 100212). The commander of the IRGC in the Ardebil province indicated that Iran's resistance against soft war is now more robust than it was during the eight-year war with Iraq (Fars News 092412). Comparing the warfare styles of cyber war and the Iran-Iraq war, the preacher of the Friday Prayer in Nahaband said, while conventional war is waged with weapons, cyber war is waged with the weapons of faith and virtue (Fars News 092212). Further, authorities advocate the necessity for strengthening the relationship between clergymen and the general public as a way to counter cyber war. In particular, the report encourages clerics to enroll in educational courses on web publishing and internet use in order to broaden their base contact with the society.

Last year (2019), the social deputy of the NAJA cyberspace police (FATA) explained details of both general and specific conditions of recruitment for committed and revolutionary police forces dedicated to the production and exchange of information in cyberspace. The priority of recruiting candidates for employment begins with the families of martyrs, veterans, honorable families of armed forces employees, honorary police officers, Basij members, scientific elites, and faithful and committed youth. Other conditions of employment for this group include a practical belief and commitment to the

religion of Islam, and a belief and practical commitment to the Constitution of the Islamic Republic of Iran and the absolute authority of the jurisprudence, in addition to a readiness to sacrifice for the revolutionary cause in order to achieve its goals. Potential members are also required to be citizens of the Islamic Republic of Iran.[9]

In the aftermath of the presidential election in 2009 and the emergence of the Green Movement, the Ministry of Defence holds annual exhibitions for indigenous cyber and communications products, which the regime considers "safe", including mobile phones, in a way that enemy cannot tap their conversations (Fars News 121413). In response to Trump's administration expanded sanctions against Iran, officials of the Supreme Council of Cyberspace raised their concerns about the country's critical infrastructure and its reliance on foreign, and in particular US made technologies. In March (2020), the speaker of the Supreme Council of Cyberspace, in a news conference announced, that due to the US expanded sanctions, which covers variety of government agencies, public corporations and some segments of the private sector, Iran's critical infrastructure and web services, which major technology exported from the US, is at risk of disruption. He emphasized Iran should reduce its dependence to foreign services (National Center for Cyberspace 031020).

5.2.3 Multi-Tier Cyber-Threat Model – Tehran's View

Iran exploits its soft war approach to respond to any real and/or perceived threat – that originate from shifts either in the international system, sub-system (regional), or in the

[9] "The Terms and Conditions of Employment to the Cyber Police". Available online: https://www.cyberpolice.ir/hamyaran

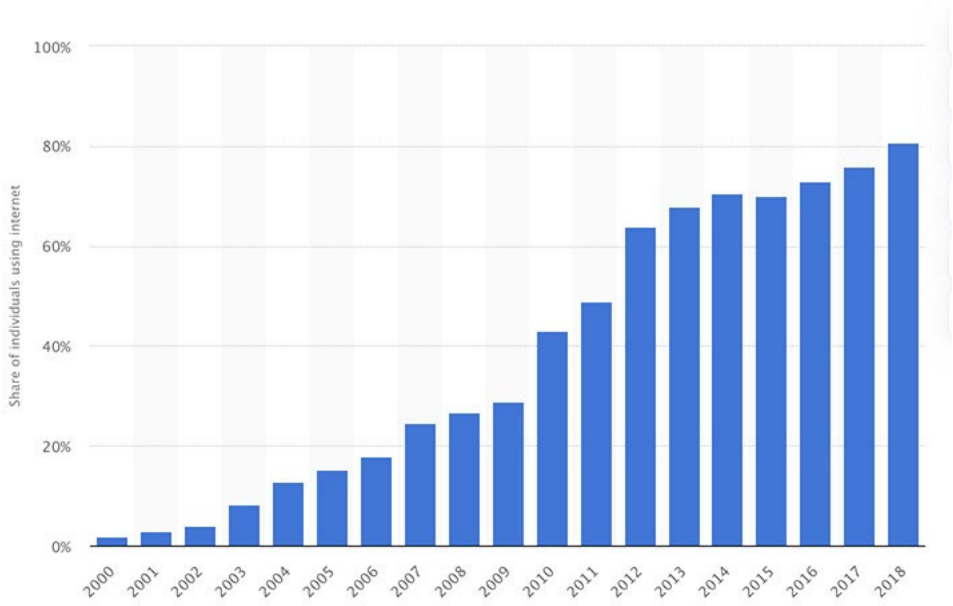
domestic politics – endangers its national security priorities. The MTCT model indicates that it is possible Tehran's external actions (e.g. promoting Islamic-Iranian values, as well as its influence operation) can be motivated by domestic manipulation of political and social forces as well as domestic signaling (see section 5.3 & 5.4). Focusing attention on foreign policy (e.g. anti-Western rhetoric) and interstate conflicts (e.g. Israel and Saudi Arabia) may prompt strengthening public feeling against opposition and seeking status in the Middle East (see section 5.3 & 5.4).

I argue that in compare with his first decade as Iran's Supreme Leader (before the presidency of Mohammad Khatami and his reformist administration), Ayatollah Khamenei since the US invasion of Iraq in 2003, through a series of domestic and regional/global initiatives (e.g. A Second Internet), has successfully created a better consensus and cohesion amongst the Iranian elites; thus, Tehran has the "willingness" to balance against the U.S. leadership in cyberspace, much more limited in extent than Russia and China. Khamenei has also successfully created a stronger social cohesion among the regime's base, through introducing a more comprehensive ideology to counter Western values especially after the 2016 presidential election in the US, but due to elevated sanctions and vast economic hardship has not been able to mitigate the regime vulnerability. Further, similar to Russia due to its underdeveloped high-tech industry and its dependence to foreign technologies especially German and Chinese technology Iran does not have the "ability" to balance against the U.S. leadership in cyberspace.

5.3 "Pure" Internet: Iran's Cyber Strategy for Social Control

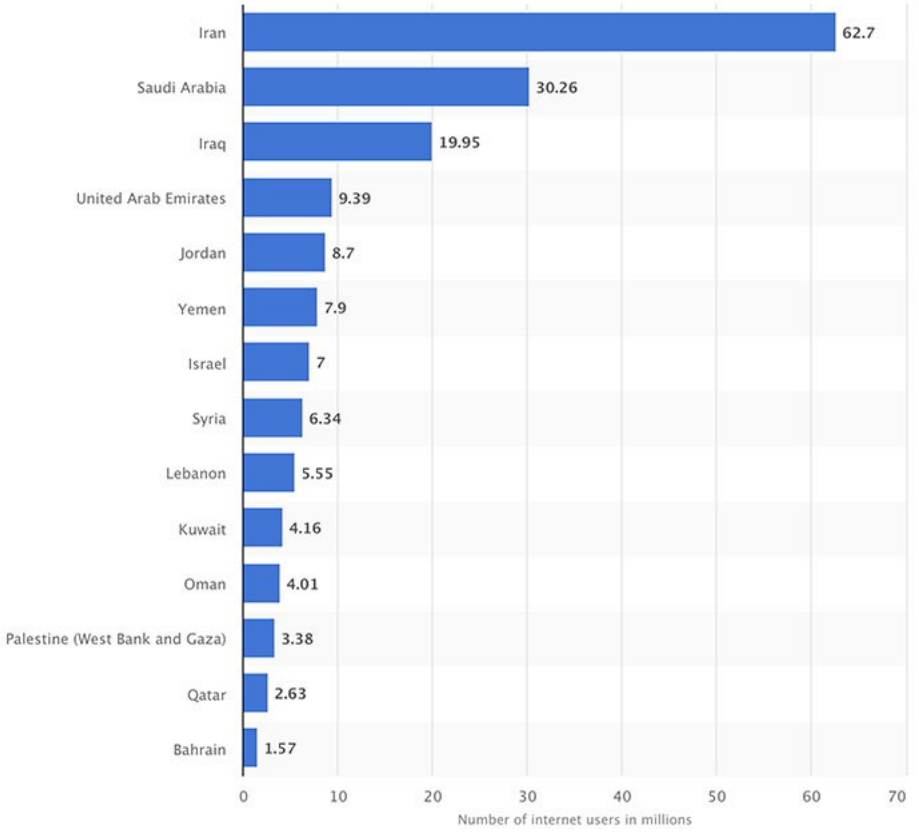
According to a recent report published by the Internet World Stats and Statista, more than 56 million Iranians have access to the internet (2018); almost 69% of the country's population is online—more than the global average (52%), and higher compared to the Middle East's average rate (64%).[10] In 2013, when President Rouhani assumed office, internet penetration was at 53 percent, compared to 11 percent in 2005, when Mahmoud Ahmadinejad became the president (see Fig 10, Fig 11).[11]

Figure 10 – Internet Access in Iran (2000 – 2019)



[10] Internet World Stats.
[11] Internet World Stats.

Figure 11 – Number of Internet Users in the Middle East (2019)



There was a major crackdown on freedom of the press near the end of Khatami's first term as president (1997-2005), in which some media outlets were shut down, and others were threatened to conform to self-censorship. Some journalists and bloggers were arrested – including Khatami's vice, Mohammad Ali Abtahi. These actions drove many journalists to internet blogging platforms that were just then emerging as a new platform for free expression (Human Rights Watch 1999).

The open dialogue with the emergent civil society through variety of newly established press, and also fostered by the blog-led conversations created an increasingly popular place to share ideas, and the number of Internet users rose precipitately. In addition, Khatami's willingness to initiate a dialogue with the West and the United States

through the ‘Dialogue of Civilizations’ initiative helped the regime to gain some credits as a cooperative international actor. The hardliner faction not happy with such initiatives found the US invasion of Iraq as an opportunity to escalate oppression and state-control mechanisms as well as the regime’s anti-American rhetoric.

It was only in January of 2009 that Facebook and Twitter were allowed access to the general population, and new users signed up in droves, making Facebook the fifteenth most-visited website in Iran within just one month. Twitter, challenged by the fact that most potential users were already invested in similar content on FriendFeed, another microblogging site, was popular to a far lesser degree. The strategy for unblocking these social platforms is unclear, but it’s possible that authorities were seeking to drive attention away from more political online sites like Balatarin – which was hacked around the same time that general access to Facebook and Twitter was allowed. Balatarin had become a central hub for Iranian dissidents and journalists as bloggers had found ways to use the link-sharing websites to seek and expose evidence of corruption in the Ahmadinejad regime. The impact of social media hit hard globally during the Iranian presidential election in June 2009, when the social media mobilized viral grassroots movements to demand governmental change. Online activism lowered the costs of political opposition and allowed a huge portion of dissidents to discuss and express a need for change without risking retribution (Yahyanejad 2010).

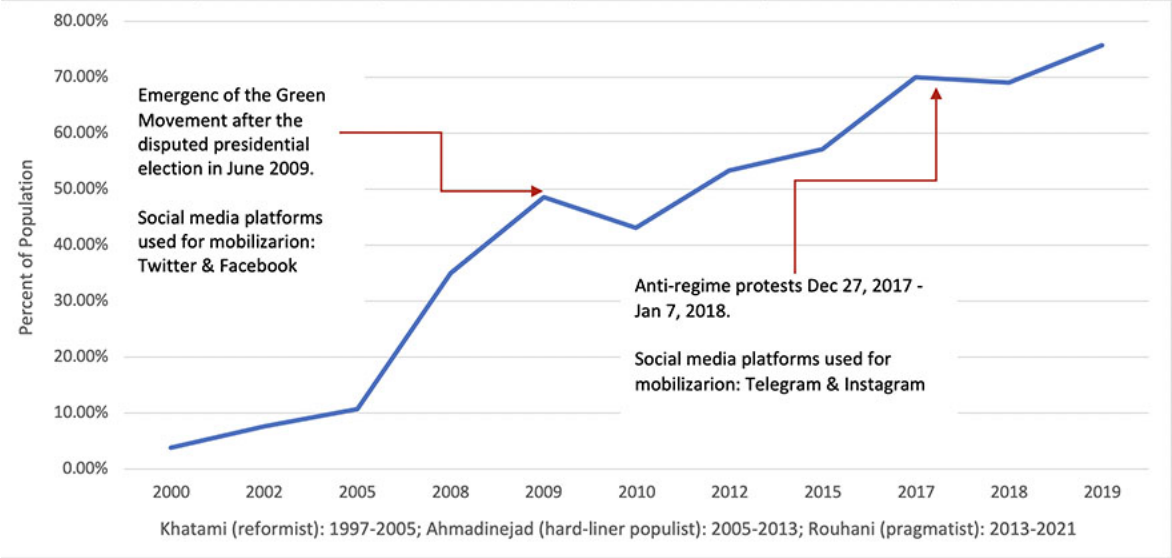
5.3.1 A Filtered Society: Social Media and Social Control

Internet activism has been key to anti-regime mobilization efforts in the past, leading Iran to implement more severe controls on internet activity, access, and user freedoms through

the development of new government agencies, including the Cyber Police Department in 2011, and Khamenei's Supreme Council of Cyberspace, implemented just one year later. It is possible for some users to evade restrictions through VPN access, but that carries risks (Majidyar 2018). The Islamic Republic clearly perceives the Internet as the central focus of a cyber war front between Iran and Western thought, with Basij activities and perspectives almost completely treated as military action. Each blog is carefully treated as a valuable source of enemy observation and intelligence, and as a real opportunity to foil the enemy's goals (Golkar 2015).

More powerful, perhaps, than any overt controls on the internet and blogging in particular, has been the regime's efforts to colonize blogs and internet content in the service of propaganda and displaying support for their goals and policies through the presence of many religious and conservative content sites. At the end of 2008, the IRGC's official press channel, *Sobh-e Sadegh*, announced a project to launch 10,000 blogs to promote revolutionary ideals. The IRGC considers Internet technology generally as a foreign government-led threat to be controlled; but also, as a powerful instrument for its own uses (Sreberny 2010). University students, through campus organizations like the University Students' Basij Organization (USBO) and the Students Basij Organization (SBO), have also been highly encouraged to engage more with online content, especially in defense of the regime, through creating propaganda-like blogs. Student members of the Basij in particular are often viewed as the first line of the Islamic Republic defense front in cyberspace (Golkar 2015).

Figure 12 – Social Media and Protest in Iran[12]



The Case of Telegram

Regardless of its greater popularity (approx. 40 million users) in comparison to other social media platforms, in April 2018, the Islamic Republic's Judiciary instructed all Internet Service Providers to block access to Telegram. Despite coordinated efforts by different political groups and organizations to encourage Iranians to rely on indigenous platforms, Telegram users utilize a variety of tools/applications to bypass internet censorship and stay connected to the messaging platform. Iranians have serious concerns about Telegram's domestic alternatives, and believe these applications facilitate government surveillance of citizens (Kargar and McManamen 2018).

In Spring 2018, the National Center for Cyberspace (NCC) initiated a series of discussions to regulate consumption patterns on social media platforms – in particular, Telegram, Facebook and Instagram. According to an ISPA (Iranian Student Polling Agency) poll conducted in March 2018, 65.3% of Iranians older than 18 years old

[12] Source: Social Media Stats. Statcounter.com (Archive)

subscribe to at least one social media platform. Telegram and Instagram together consume 80% of Iran's network bandwidth – Telegram 60% and Instagram 20%. In its report – *Telegram: A Project for Specific Countries* – participants at the discussions sponsored by NCC conclude that Telegram was developed specifically to contend against the Islamic Republic. Iran considers Telegram to be a dark social media platform and a safe haven for terrorist organizations, with a central intent to bypass legal channels and destabilize national security in countries that are defined as enemies by the United States (National Center for Cyberspace 0318). Based on Pavel Valerievich Durov's earlier project – VKontakte – and its role in organizing anti-regime protests both after the 2011 parliamentary election and in the midst of the Ukrainian crisis (2014), Tehran believes that the U.S. solicited Durov, invited him to New York City, and provides essential support for his new social media platform, specifically developed to target U.S. enemies, Russia and Iran in particular. Citing Theresa May (Hern 2018), who said Telegram has become a haven for terrorist organizations and allowed them to organize operations; Iran identifies the messaging platform as a form of hybrid warfare, versus defining other platforms like Facebook and Twitter as "soft power" tools of the Wester.

The terrorist attack on Iran's parliament in June 2017, followed by series of uprisings across the country in January of 2018, both demonstrations organized through Telegram channels, led authorities in Tehran to ban Telegram temporarily for few days. They point to Durov's message on his own page that: "Telegram has never yielded to pressure from officials who wanted us to perform political censorship. Freedom of speech

is one of the values we've been defending for the last 11 years, first in Russia, and then globally".[13]

The NCC report states that one month before the uprisings in Jan 2018, Durov's office reported relocation to Dubai. During this period, Telegram increased access to the platform for Iranians through CDN servers seven times faster than typical European users. (very similar to what Twitter did during 2009 uprising, by establishing server centers in Iran's neighborhoods to increase local access.) Referring to Telegram's plan to establish a network based on Blockchain technology, which can pass through any filter, as well as its plan to introduce a currency that allows users to conduct financial transactions over the platform, Iran argues that Telegram is preparing for war with Iran, an positioning it's Gram currency as a logical replacement to the national currency.

Since social media platforms allow information and communication exchange, Tehran believes that users will easily adopt the new currency and conduct economic transactions there. Soon, the management of society will be naturally in the hands of managers of social media platforms more than governments. So far, Telegram has been a threat to security and culture, and soon it will endanger the economic system, too. It is imperative to stop Telegram's progress while it is still possible.

The Case of Facebook and Instagram

When collective identity became a more prominent priority after the 2009 elections, Facebook functioned paradoxically to expose collective action of movement participants, while simultaneously undermining the coherence of the movement by allowing framing

[13] Pavel Durov's Tweet (October 29, 2017).

process adjustments that allowed varying forms of collective action and alternative meanings. The political quality of Facebook, consequently, might rest in its ability to resist political controls. Political institutions which seek to frame meanings and form the template for collective action and identity in Iran find in Facebook a contending platform for elevating alternative meanings and identity for Iranians seeking political change (Esfahlani 2009). In January 2009, the Committee for Determining Criminal Cases presented a list of criminal acts on the Internet. The list divided cases into five areas: Content contrary to public decency and morality, anti-sanctity content, content against public peace and security, anti-government or anti-authority content, and cybertheft or espionage-purposed content.[14]

In 2013, when Hassan Rouhani became the president, his administration tried to remove filtering from some of the social media platforms such as Facebook and Twitter. Ali Jannati, the Minister of Guidance and Islamic Culture, implicitly stated that it was possible to remove filters from some social networks, such as Facebook. However, the secretary of the Working Group on Determining Instances of Cybercrime, affiliated to reacted to this possibility of removing filters from social media sites, urging the government to strengthen domestic services instead of removing filtering from foreign social media platforms (Balatarin 120213). Not a few years after the passage of some restrictive laws on social media and internet use, the authorities of the Islamic Republic have gradually adopted a dualistic and discriminatory policy on social media use. For

[14] "The Committee for Determining Criminal Cases". Gerdab.ir

instance, the Supreme Leader and the president both have Facebook accounts, but the law penalizes the public for using such services.

The hardliners and conservatives hold the majority of seats in the current term of the parliament (Majles 11th). An unrestricted cyberspace and unfiltered social media platforms, such as Telegram and Instagram, are at the center of many parliamentarian debates and conversations. Hassan Norouzi, a member of the Legal Affairs of Majles, stated: "May the filtering of Instagram happens soon. The open space of this social media platform is a threat to our youth, and this brings instability to the regime."[15] Mohammad Hassan Asferi, another MP compared Instagram to a military organization like NATO, and warned of an imminent coup d'état by its users due to uncontrolled freedom the photo and video-sharing social media platform provides its users: "these activities [Instagram posts] that take place in cyberspace are nothing but a coup d'état and cultural NATO against our revolutionary values, the ideals of Imam Khomeini, and the will of martyrs".[16] Even Mohammad Baqer Qalibaf, Speaker of the Parliament and a veteran of the IRGC, called cyberspace "unbridled" and emphasized on its control. Interestingly, Qalibaf has an account in Twitter, which has been filtered and reflects his political views there.[17] The MPs even summoned the Minister of Communications and blamed him for the failure of his ministry in filtering Instagram and the size of bandwidth is allocated to this social media platform (Tavaana Tech 062720).

---

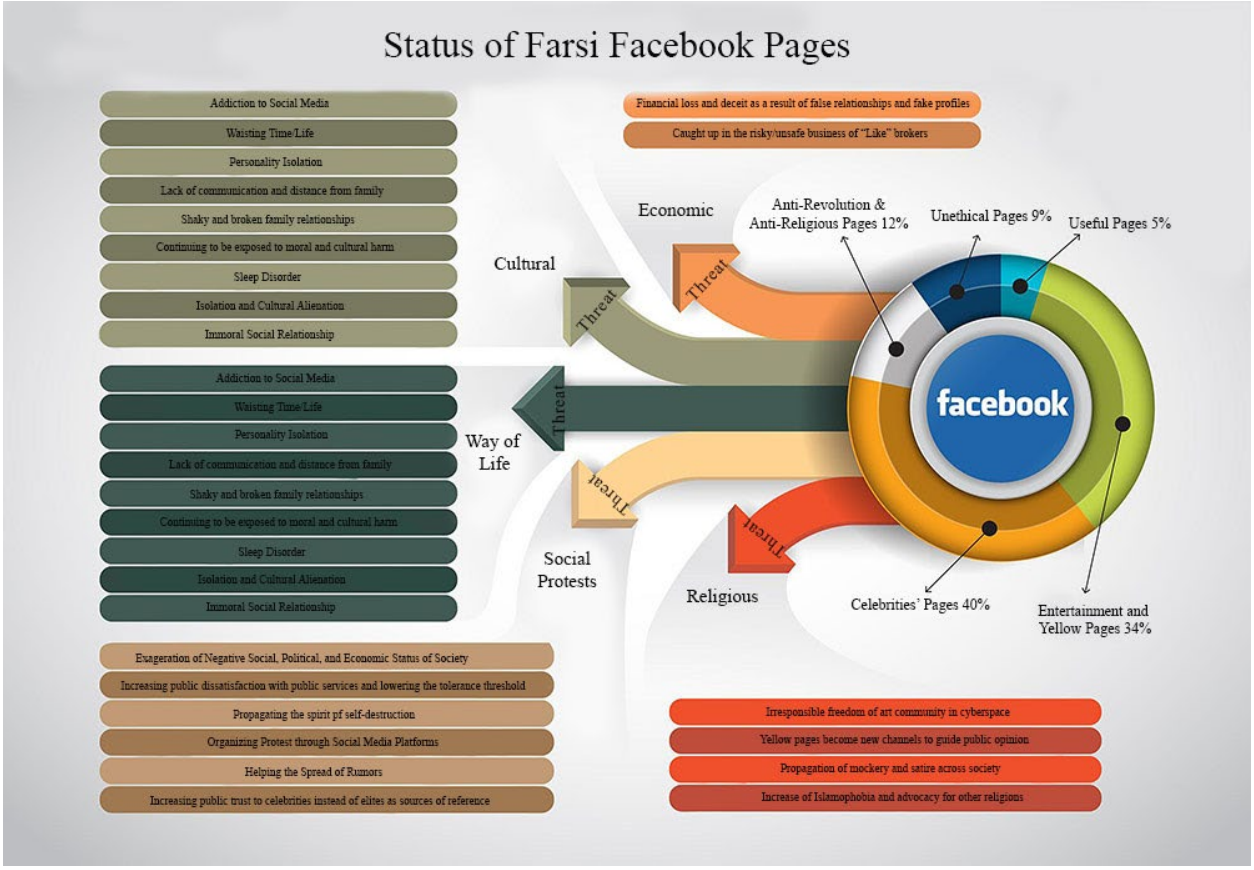
[15] "May the Filtering of Instagram Happens Soon". *Hamshahri Online*.22 June 2020. Available at: https://www.hamshahrionline.ir/news/524396/

[16] "What Takes Place on Instagram Is Nothing but a Coup d'état". *Goftareno*. 21 June 2020. Available at: https://goftareno.ir/fa/news/37423

[17] "Like Automobile, Cyberspace Needs Management". *Asr-e Iran*. 21 June 2020. Available at: https://www.asriran.com/fa/news/734248

The elites of the Islamic Revolutionary Guards Corps (IRGC) believe that cyber war is more dangerous than traditional war because it is difficult to notice its presence. In his keynote speech addressing the Basij of Universities' Faculty, the commander of IRGC, Tehran branch, mentioned that the main duty of the IRGC at this juncture is defensive and counter-technological strategies against cyber-attacks. Referring to the Iran-Iraq war legacy, he emphasized that Iran does not respond well to force, and the West learned this from that war. He also indicated that members of the IRGC and Basij are at the forefront of any cyber war, however there is a big difference between a cyber war and a conventional war. While in the latter the order is dictated from top to bottom, in the former, every individual must act based on their intuition and capacity. He empowered professors across the country to act as commanders of any soft war, encouraging a sense of responsibility in order to operationalize the Supreme Leader's demands (Etemad Newspaper 090312).

Figure 13 – Infographic of Facebook's Socio-political Harms[18]



According to Article 150 of the Islamic Republic's Constitution, the main mission and responsibility of IRGC is to protect the revolution and its achievements.[19] In 2007, the IRGC, in collaboration with the Judiciary Branch of Government, established a center for the investigation of organized crimes. The main goal of the center has been to counter and prevent international organized crimes, including abuse of the Internet and other communication channels to conduct terrorist activities, spying, money laundering;

[18] Source: https://gerdab.ir/fa/news/13570/

[19] Islamic Republic's Constitution, Article 150: "The Islamic Revolution Guards Corps, organized in the early days of the triumph of the Revolution, is to be maintained so that it may continue in its role of guarding the Revolution and its achievements. The scope of the duties of this Corps, and its areas of responsibility, in relation to the duties and areas of responsibility of the other armed forces, are to be determined by law, with emphasis on brotherly cooperation and harmony among them".

damaging the socio-cultural systems of a country and insulting religious and revolutionary values. Due to the following factors as well as emerging threats, the IRGC's center for organized crimes has expanded the scope of its mission; in Spring 2014, the IRGC established its cybersecurity command center to protect Iranian society in cyberspace:

- Growth (increase in number and scope) of mobile social media applications, and the increase in ways that enemies can utilize such applications to destroy society's cultural systems.
- Children from early ages have access to the internet, and as early as thirteen can have social media accounts. Due to a lack of age restrictions, the state is concerned about the corruption and manipulation of the youth by the enemy and opposing ideologists.
- Foreign entities try to influence change in the Iranian lifestyle through information technology.
- Cyber-diplomacy has turned into a branch of state diplomacy.
- Western intelligence communities spy on other nations by providing free internet services.
- The enemy utilizes cyberspace for attack and espionage on critical networked infrastructures.
- The enemy tries to provide Iranians with access to illegal sites through filtering services.

So far, the center has completed several projects to counter enemy influence and opposition, with code names such as Malice, Deep Intrigue, Woodpeckers, Mersa'd, Eyes of Fox, Na'seh and Spider.[20]

5.3.2 Marching Toward a "Pure" Cyberspace

For nearly a half-century, an identity of Islamic value defined all public matters and policy, including media and the internet, where users were encouraged to promote state perspectives and refrain from any distinctly anti-Islamic language. The efficiency of this

[20] https://gerdab.ir/fa/about

system as a whole has been increasingly compromised by factionalism within the Iranian state as well as by social movements, activist challenges, and journalist critiques of policies and official measures. Three key regulations introduced in 2006 exerted specific controls over the internet—the first measure, introduced in August of 2006, required official blog registration, and the other two, introduced in November the same year, clarified previous regulation and specified exact punishments for cyber-crimes. Download speeds for all ISPs across Iran's residential clients and internet cafes were restricted to 128Kbps by new regulations from the Radio Transmissions and Regulations Organization of the Ministry of Communications in October 2006, a legislative move seems aimed at limiting users' access to effective political organization, as well as to foreign cultural products like music and films. Additional modes of censorship have included:

- Closing any and all ports that have been used by savvy internet users to bypass filtering systems.
- Censoring keywords in URLs, yet another obligation that ICPs and ISPs have to meet.
- Implementing periodic crackdowns on internet cafes (Sreberny and Khiabany 2010).

In an interview with the Parliament's News Agency, *Khaneh Mellat* (the House of the Nation), vice president of international relations committee, praised the effective strategies of the Intelligence Ministry in countering cyber-attacks and called the cyber troops recruited by this ministry as *Mahdi's unknown soldiers*. He said these individuals have presence across the country to protect the Islamic Republic against any soft threat. He emphasized that the power of information within a state is its most important pillar (Mardomsalari Newspaper 070412). Since the emergence of the Green Movement in

2009, Iran's internet policy evolved from a control regime to a cordon regime. The military and civilian elites have utilized three mechanism to create a "Halal" or pure internet environment: Basij resistance forces, state-sponsored civil society groups, and decreasing the countries dependence on Western-based high-tech industry.

Basij Resistance Force: Basij members are typically encouraged by the IRI to disseminate physical propaganda as well as their preferred cyberspace ideologies. With the strategic establishment of internet cafés in Basij-populated areas, the Basij presence in cyberspace became more intentional and widespread following Khamenei's 2007 order for expansion of information technologies. Other Basij strategies for an increased presence in cyberspace led to the creation of 10,000 blog sites given to Basij members, in exchange for each blogger sharing a certain amount of government-approved content on their sites. In particular, female bloggers position much of their content to align with the official government position on women's rights. Cyber councils were also established in Basij regions, to oversee, regulate, and encourage online activities, as well as to confront "cultural threats" that came from online sources. Additionally, the Engineers' Basij Organization was delegated monitor and filter the Internet for Iranian users (Golkar 2015).

Another organization founded to focus on the "soft war" is the Artist's Basij Organization (ABO), founded in 2005. The pro-regime artists of the group organize to defend the IRI against the more subtle cultural threats and undermining ideologies. In an interview, Nasrollah Yadollahi, the Associate Director of Education and Training of the Artists Basij Organization, stated that members of ABO are cultural officers of the

ongoing soft war between Iran and the West. In addition, he said, the organization plans to form a "cultural cyber-army," tasked with the goal of establishing a variety of think tanks and advocating for the significant role of art in soft war, to the extent that confronting soft war becomes the main concern of Iranian artists. In addition, the organization plans to provide managers of art galleries and enterprises with a variety of consultancy and support opportunities. Since art deals with people's emotions and feelings, it has a key role in confronting Western attacks on our cultural values (Javan Online 060810).

IRGC commander Ali Soltani also emphasized the role of art and artists in soft war against the West, saying that poetry, theatre and cinema must serve the values of the revolution and praise the culture of sacrifice, jihad and martyrdom. Persian language and script are the cornerstones of the Iranian culture, and the regime perceives social media platforms, Telegram in particular, as a real threat to language and script. Soltani emphasized, in general, the increased use of social media platforms imposes two types of threats to Persian language and script, according to National Center for Cyberspace report; the first threat is due to increased rates of misspellings, which have become normal and even fashionable in social media message exchanges. This is seen as potentially damaging to accepted norms of writing over the long term. The second threat concerns a reduction in the number of websites that generate Persian content; social media platforms and their messaging systems gradually will be replaced by Farsi content provider sites, which in turn damages the perception and widespread use of the Persian language in online contexts (Fars News 071115).

Sacred Migration: On April 9th, 2018, in a joint parliamentarian session, members of the Committee on Economy and the Committee on Foreign Policy and National Security shared their concerns regarding Telegram with the Secretary of Communication and the Secretary General of the Supreme Council on Virtual Space. Aladdin Boroujerdi, then Chairman for the Committee on Foreign Policy and National Security, mentioned that Western-based social media is an important concern for the state, both in regard to national security concerns, and because it provides access to enemies who wish to influence the Iranian people. Another member of the Parliament stated that, due to organized rumors against indigenous social media, which cause panic and confusion within the Iranian populace, people favor Western-based social media and their mobile applications. This representative urged people to switch to native social media applications and called this act a "sacred migration" (Jamaran News 040918).

Referring to the five indigenous social media networks (Bisphone, Eitaa, Soroush, Gap, and iGap) approved by the Ministry of Communication to be replaced by Telegram in Iran, MPs also raised concerns regarding Telegram's economic threats. Because Telegram users are able to conduct transactions through virtual currencies, Iran's market may possibly be impacted. The Parliament emphasized that any economic transactions through social media should support Iran's market; and this is another important point that people must consider when switching to native applications. With the increase of web-based markets and transactions, the Parliament recommended that the government should initiate and draft policies and programs to develop and advocate for indigenous technologies, protecting both individuals as well as financial and credit institutions. Among indigenous social media, Eitaa and Soroush have more popularity. The rumor is

that native applications are under the supervision of the IRGC, and people do not feel safe exchanging messages through such media.

The Siraj Cyberspace Organization:[21] The organization has been formed to shape and support public activities in cyberspace, and accordingly, in the two layers of users and content. The founder of Sira, Mansour Amini looking at the current situation in the country in the field of cyberspace, especially regarding social networks, contends, "it has become clear that the demands of the leadership have not been implemented and even in some cases, including with domestic technology, that continued weak points have persisted for several years". In the field of social networks and messenger apps due to the lack of proper native technology innovation and support for domestic products, Western/foreign messaging platform (such as Telegram) that does not comply with the laws and regulations of the Islamic Republic attracts 40 million users in organizing sporadic uprisings against the regime. Amini argues that if the regime had a strong indigenous messaging platform, the state could have prevented the spread of lies, disinformation and rumors much more quickly.

One of the important prerequisites for public activities, Amini states, is the issue of education and training. The Siraj Organization and its national specialized centers train dozens of talented people, according to values acceptable to the norm and culture of the society. Another area, which desperately needs to be addressed, according to Amini, is the area of cyberspace literacy/awareness and user's culture, in the sense that people are educated to benefit from the opportunities cyberspace provides them while avoiding its

[21] https://www.magiran.com/article/3847781

dangers. In this field, the cyberspace literacy promotion movement, or "literacy corps," has been on the agenda since 2015, and by holding dozens of coaching courses across the country, several thousand cyberspace literacy instructors have acquired the necessary training and skills through the Siraj training camps.

In addition, for the first time in the country, the Clinic for Improving Mental Health in Cyberspace was launched by the Siraj Organization, which aims to control the use of this space and improve the conditions of those who deal with Internet-based addictive behaviors. One of the most important areas of activity. Hundreds of applications for a variety of social categories, such as women, children, lifestyle, jihad and resistance, religious education, etc., were produced. And the construction of dozens of mobile and computer games/apps by people groups were led by the Siraj Cyberspace Organization, which is committed to these areas. Providing specialized services within each field of information and providing communication technology to public groups are other measures being pursued to support the cultural front of the Islamic Revolution technically.

5.3.3 Young Officers of Soft War

It is beautiful that you write so devotedly about our savior, Mahdi. He let us announce, on the eve of his second coming, his appearance on our website. Be ready for the war, observe the enemy, recruit your members, take ablution and sit behind your computers. You will be rewarded as martyrs.[22]

The above statement is part of commander Hossein Yekta's sermon, published on the Young Officers of Soft War website. Yekta, a former commander of the Islamic

[22] http://cyber-officers.blogfa.com/

Revolutionary Guards Corps (IRGC) and a war veteran, is the founder of *Pilgrims of Light*, an organization devoted to the introduction, explanation, and cultural construction of the Iran-Iraq War operations across media and the Internet.

Ayatollah Khamenei labeled the vast uprising of Iranians in the aftermath of the 2009 disputed presidential election an act of "devilry" conducted from abroad against the Islamic Republic primarily through cyberspace and social media outlets, like Facebook and Twitter. Soon after, in a meeting with university professors and students, Khamenei emphasized the dangers of the West's soft war against the Islamic Republic, and stated that students and instructors are "young officers and commanders," of the soft war, respectively; responsible to defend the Revolution's achievements and counter the West's cultural hegemony (Porseman Monthly 2010). In 2010, the Supreme Leader commanded his followers and those loyal to the regime to broaden the impact of their activities on society through cyberspace and populate the web with religiously oriented blogs and other web-based applications to counter the *cultural camisado* of the enemy, both domestic and foreign. He emphasized that the ongoing cyber war imposed on Iran by the West was not only against Islam and the establishment, bringing chaos to society, but more importantly it makes God angry at Iranians, if the nation remains passive (Aftab News 102010).

A Washington Post editorial reported that Confidential Saudi documents purportedly released by WikiLeaks appears to show links to Iranian hackers, based on cyber-attacks on more than a dozen countries, including the United States. The State Department released an unprecedented security warning in May 2015, indicating that U.S. businesses operating abroad have been impacted by Iran's increasing cyber warfare

capabilities. Iranian hackers have been focusing on oil and gas companies in Saudi Arabia and Qatar, launching an extended campaign (Operation Ababil), including attacks on Citigroup, JP Morgan Chase, Bank of America, and the US Navy and Marine Corps' Intranet since 2012. The Iranian-based cyber-attack on Saudi Aramco destroyed 30,000 computers, and the 2014 attack on the Sands Corporations computer servers caused 40 million in damages. These attacks were planned by Iran's cyber army, which is controlled by Iran's Revolutionary Guard.

There are two types of cyber militia in the Islamic Republic of Iran: offensive and defensive. Offensive forces such as Ababil group or Pistachio group, do not generally identify themselves with either civilian or military cyber units. Offensive cyber militia forces target the US and Israeli businesses and governmental institutions and their allies in the Middle East. Defensive cyber militia, however, in general, are affiliated to the Basij and advocate for the Islamic Republic ideological and religious values. The Young Officers cyber militia has three operational layers: regular officers, commanders, and propagators/ideologues. While the first two groups belong to academia, members of the latter force are clergymen and are recruited from seminaries. The clergy Officers generally raise awareness about *Velayat-e Faghih* (rule of the jurist) and revolutionary values (Fars News 062318).

In order to counter cyber-attacks Young Officers of Soft War should be equipped with the following:[23]

1. Listening and following the Supreme Leader's thoughts and insights,
2. Identifying Malware sites and destructive bases,
3. Being innovative,

[23] http://www.afsaranjnarm.ir/forum

4. Staying informed and tuned in on news from a variety of sources,
5. Possessing professional skills in media production and other professional software,
6. The ability to identify the enemy's tools,
7. Learning the enemies' language(s),
8. The ability to build up social skills and connections.

The recruitment process is by invitation only. There are two types of officers: Regular and In-Training. Their differences are that Officers-in-training who send web links or text messages require approval before those comments are posted; in addition, they cannot create a group or invite members.

The following are the operational responsibilities of Young Officers:[24]

1. Sending links and text messages
2. Multimedia
3. Topic of the Day: In order to coordinate activities and influence, the latest news to offer users in a defined subject day. When users send the link, if relevant to the subject as the subject can choose.
4. *Cator*: Officers patrol social news networks to facilitate the production of content in cyberspace. Cator is an online cartoon tool that allows users to participate in a few minutes without having to use any other desktop software. Cartoons are produced on a variety of topics and shared with cyber comrades.
5. Group: Different groups with various themes are currently active officers. An activity index of 500 or more is required for officers to create groups.
6. Topic of the Month: At the beginning of each month eight themes as well as faces are chosen by the users through a survey and they become targets of comments and debates throughout that month.
7. Poll taking
8. Treasure box: the most brilliant and innovative thoughts of the officers are kept in a cyber treasure box.
9. Arman TV Network: A TV channel that advocates an ideal Young Officer.
10. Follow other comrade officers
11. Invitation
12. Smartphone apps

[24] http://www.afsaranjnarm.ir/forum

Iran's Supreme Leader advised Young Officers to avoid inaction as it is like a cancer for a cyber officer. Currently the Young Officers have nine active groups:[25]

1. Press
2. Pen Club
3. Media and Operation
4. Graphic Designer
5. Animation
6. Camera
7. Poetry
8. Toranj – The purpose of the group: Simplification – to convey the most conceptually, through the least wordings.
9. Halal Laugh/Smile: Satire and cartoons that observes the society's morals; avoid themes and labels that cause societal disruption or bring shame and accusation to Iran, Iranians, and religious values.

One of the key duties of the Young Officers is to advocate and propagate for the global government of Mahdi across cyberspace. The Young Officers raise awareness about Iran's revolutionary values through variety of means such as blogs, webinars, chatrooms, and computer games. Their most popular website is *Entezar Patogh* (cozy place for awaiting the Mahdi), where members meet online and discuss variety approaches for advocacy as well as recruiting new members.

At Regional and International Levels: Iran doesn't take a public policy position on cyberspace, so the only rationale for strategic attacks is formed by historical events. Generally, Iran responds to domestic and international events; as an example, a cycle of disruptive attacks subsided following the 2015 nuclear deal between Tehran and Washington. But the full decision-making process for cyber-activity is not clear, and not all cyber-operations are controlled by the regime. While Iran's ability to challenge

[25] http://www.afsaranjnarm.ir/forum

opponents with stronger capability is limited, it has engaged in destructive attacks to demonstrate its capacity for reaction; implicit threats are particularly effective in the Middle Eastern region. The targets of Iranian cyber-operations often seem limited in scope, such as rival banks and airports in the region (Anderson and Sadjadpour 2018).

In addition, Tehran, like Russia, mobilizes its troll armies, to demonstrate its credibility to its domestic audience as well as its regional allies. Two objectives generally guide state's computational propaganda efforts in Iran; first, countering Western narratives and the 'soft war' of cultural ideology, and secondly, promoting pro-State ideology on the other (Bradshaw and Howard 2018). A group of Twitter accounts share Iranian propaganda in English, but it's unclear who is behind them. Dozens of "ghost" accounts with profile pictures made up of stock photos or celebrity photos tweet every few minutes throughout the day to thousands of followers. In one occasion, the regime mobilized its trolls across twitter and other social media platforms, the posts used the hashtag #Powerful_Iran; the momentum to the hashtag #Powerful_Iran seems to have increased following the nuclear deal; many hardliners in Iran oppose the deal as running counter to Iranian national interest and giving too much power to the West.

Viral social media campaigns run by Iran's cyber militias, such as those following the 2014 Paris terror attack and the subsequent letter to Western Youth from Ayatollah Khamenei seek to spread the peaceful vision of Islam and Iran. The letter and its hashtag #Letter4U spread on major social networks, accompanied by links and short messages, such as "Searching for the truth? Then Letter4u is what you might want to read first," etc. Coordinated campaigns been seemingly launched from Iran before, targeting Western Twitter users; the hashtag #Letter4u was used by bot-like accounts to follow up the

release of the Supreme Leader's open letter to Western youth as part of the regime retaliation to its perceived Islamophobia campaign lead by the United States (BBC News 031616).

5.4 US-Iran Cyber Relations: Challenges and Responses

Although Iran's size, geostrategic location, natural resources, ideology, and ambitions have made it central to at least eight major US foreign policy challenges, including Syria, Iraq, Afghanistan, the Israeli-Palestinian conflict, terrorism, energy security, nuclear proliferation, and cyber-security, On these issues and others, Tehran has defined its interests in direct opposition to Washington. The quandary this creates for any US administration is specific; although shunning Iran will not mediate issues, the Obama administration's eight-year effort to engage Tehran on issues produced very few successes, proving that the Islamic Republic of Iran is too big to isolate, too rigid to bend, and too pragmatic to break (Sadjadpour 2017).

Iranian incidents of cyberattack have been some of the most sophisticated, costly, and significant attacks in internet history; the U.S.-Iran 'cold war' coincided with the movement of information and activity to cyberspace. While Tehran has been one of the most frequent targets of destructive cyber-operations by the United States and other allies, Tehran has also ramped up cyber-espionage and disruptive attacks, both domestically and globally, against civil, governmental, and commercial targets (Anderson and Sadjadpour 2018).

Some of the measures that the United States and some human rights NGOs initiated to counter Iran's cyber posture are as follow:

We Digital Citizens: An educational campaign for digital literacy called "We Digital Citizens" was launched by Freedom House with the support of many web experts, journalists, and social scientists. The non-political initiative seeks to clear up confusion and share accurate information around uniquely internet-centered issues like distorted reality, fake news, digital security, and cyber-bullying, hoping to enable more people to be confident, safe, and healthy as online citizens. The campaign utilizes an online pedagogical game: Factbaan. It means "the guardian of fact" based on the original fake-news parable "The Boy Who Cried Wolf" is another tool raising awareness about fake news stories through fact-checking.

Factbaan educates users to identify the characteristics of credible news stories at two levels, beginner and advanced. The beginner level addresses broad criteria for detecting reliable news, and advanced goes into more complex and advanced detection. News reports are viewed by users, who then answer questions and ultimately decide if the story is credible or not. After viewing three reports, users can see a credibility score and compare it with the average score of all users on the site.[26]

The Iran Disinformation Project: Launched in 2018 and funded by the U.S. State Department's Global Engagement Center was originally developed under the Obama administration by Brett Bruen to counter Russian and Isis disinformation and propaganda; the Trump administration added Iran to that short list. The initiative reveals disinformation daily and in multiple languages, as it emerges from the Islamic Republic

[26] https://digitalshahrvand.com/

of Iran's official rhetoric, state propaganda outlets, and social media, seeking first to expose and then to counter the influence of the totalitarian regime.[27]

Tavaana: The main civic education initiative in Iran is Tavaana. Launched in 2010 with a seed grant from U.S. State Department's Bureau for Democracy, Human Rights, and Labor, the project speaks to a vision of a free and open society marked by equality, justice, and civil/political liberty for Iranian citizens. Strong civic networks have been fostered through Tavaana's action, engaging millions domestically and globally through timely social media posts amplifying civil society organization efforts throughout Iran.[28]

5.5 Concluding Remarks

The policies of the West, in particular the United States' democratization, its support for Israel and its presence in the Middle East, which are increasingly perceived as inherently threatening to Iran's interests, are one of the major international factors that appear to influence the Islamic Republic's international actions. In consequence, Iran, to gain instability at home and prestige in the region, initiated an expansion policy to export its revolutionary values since 1979. In recent years, by allying with China and Russia, Tehran hopes to gain its desired regional status. To achieve its strategic goals in addressing its national cybersecurity dilemmas (discussed in chapter two), Iran's preferences are as follows:

- Infrastructure Modernization vs. Critical Infrastructure Protection: Due to the escalation of the US sanctions the government warned Iran's tech industry to

[27] https://irandisinfo.org/about-us/
[28] https://tech.tavaana.org/index.php/fa

avoid Western/foreign high-tech hardware in their assembly lines. Iran also increasingly advocate for indigenous software, hardware and web technologies.

- Data Protection vs. Information Sharing: While Iran advocates and push for storing users' information an date across its data centers embedded in its National Information Network structure, the government has not been successful to force foreign tech companies to comply with its demands.
- Freedom of Expression vs. Political Stability: Iran, in particular its National Center for Cyberspace, was identified again in 2018 as the greatest threat to internet freedom; the IRGC and the Basij not only expanded their surveillance and oppressions across the net, but their members populated the internet with pro-regime's blogs. Like China and Russia, Iran continues to promote digital authoritarianism and its capacity for citizen control as a major advantage of internet and digital technology (Shahbaz 2018).

Chapter Six: Conclusion

6.1 Summary

This concluding chapter will first summarize some key findings of this study on cyber threat assessment, as well as how states respond to real and/or perceived cyber threats. Followed by a section on cross-case analysis, comparing the three cases across cybersecurity and cyber governance to tease out the most significant factors on state cyber-posture and policy outcomes, the final portion of the chapter discusses U.S. policy implications.

In all three case studies, certain factors seem to be more significant than others in explaining the divergent outcomes in threat assessment. On the international level, while China seeks to rewrite cyber norms and introduce an alternative cyber governance model to replace the current Western-led model, Iran works to export its revolutionary values and to bring about an Islamic awakening and develop a value system competitive with Western morality, and Russia seeks to control Eurasia and dismantle Western democratic systems. Domestically, all three countries retain authoritarian structure. However, there are variations in how each structure, ideology, and governance plays out, from China's concerted control mechanism, to Iran's evolution from a control to concerted-control regime. Russia, on the other hand, has moved to a control mechanism regime from its former position as a response regime.

6.1.1 Major Arguments and Findings

Through seeking to understand more clearly why similar systemic pressures can produce different responses by states, this study makes two contributions to broader IR literature by first adding to the growing body of literature on cybersecurity and threat assessment. Secondly, this study introduces a cyber-threat assessment model – the Multi-tiered Cyber-threat Model (MCTM) – uniquely based on a neoclassical realist approach to the state and foreign policy

The MCTM is a neoclassical realist model for identifying Cyber-threats derived from other neoclassical realist models from scholars like Steven Lobell, Randal Schweller, and Jennifer Sterling-Folker. The MCTM identifies threats from international system, subsystem, and domestic environment shifts. However, distinctions between these tiers are not often clear, and shifts in one level may result in action or influence on another. Accurate threat assessment is predicated on understanding the interrelated nature of connections, threats, and the complexity of state and actor motives and intentions beneath any obvious threat indications.

6.1.2 Summary: China

China's cybersecurity strategy, in unison with its national security strategy, is bent on increasing cyber power through increasing offensive and defensive capabilities, continuing to reduce dependence on foreign technology, guarding and promoting national sovereignty in cyberspace, and maintaining 'harmonious' order and security in public cyberspace. However, the CCP defines security as an absence of threat, not the ability to counter it, a stance that explains past pre-emptive security measures toward potential

threats. Ideologically, the CCP goes beyond even this strict definition of security by allowing it to label even ideas as potential threats.

At an international level, China's cyber-strategy has undergone a shift from countering threat to controlling cyberspace. Previous approaches to cyber-activity have been reactive, in order to counter perceived threats; more recently, China's international cyber-activity has become more pro-active and policy oriented. China has doubled down on advocating for the defining idea of internet sovereignty in its calls for broader international cooperation. The focus on 'counter and control' strategy in international policy discussion strikes at the problem of U.S.-led Western dominance of internet infrastructure, but it also serves China's goal of strengthening the argument for greater domestic political control. Chinese commentators seem to increasingly view control over global internet policy development as a way to achieve the 'China Dream' goals of raising its international power status to match its global economic strength.

On the domestic level, the government essentially created a digital policy of a 'cordon regime,' in order to cut Chinese citizens off from any Western tools, platforms, or applications. The 18th CCP Central Committee's Third Plenary Session in November 2013 declared that 'social stability' is key consideration of internet and information security policy planning in addition to 'national security,' and balancing the two elements represents a 'comprehensive challenge.' This indicates a theme in China's thinking about cyberspace's potential to disrupt social stability and what that might mean in practical terms. While the CCP has kept the internet from being effectively used as a tool for meaningful political opposition, there is still plenty of tension in the party between

encouraging innovation and technical aspiration but controlling the potential disruption of dissent.

6.1.3 Summary: Russia

Nested within its national security strategy, Russia pursues an information security strategy comprised of various goals, including increasing Russian cyber power, guarding national sovereignty, and protecting Moscow's geopolitical interests. These major cybersecurity goals that define Russia's quest for cyber power can be categorized under four major headings: promotion of cyber sovereignty, securing information and data localization, advocating for an autonomous Russian internet, and reducing the nation's dependence on foreign tech.

At the regional and global level, Russia relies on information technology to spread doubt, division, and discord, and to promote key narratives in the interest of reducing anti-regime dissension. Moscow's destabilizing campaigns have pursued a host of objectives in as they seek to reinforce influence over various states, regions, and population segments perceived as vulnerable to Western/NATO ideals to any degree. It is also difficult to shake the implications of colonial hegemony of the RuNet; the simple fact that it is mono-linguistic represents a potential "neo-hegemony of cyber-colonialism." Beyond this, the RuNet is deeply connected to the geopolitical potential of the Russian World ideology, as an 'impersonal' but effective transfer zone of language, culture, and information, which, irrespective of citizenship, aims to broaden the Russian-speaking space.

Domestically, we can identify political changes that have transformed Russia from a response regime to a control regime; in 2000, Boris Yeltsin was succeeded by Vladimir Putin, a political event which heralded the development of what is now called 'virtual political technology' in Russia. This informational manipulation of public opinion was propelled by the lightning-fast development of the Russian internet's growth boom over the late 1990s and early 2000s. As the internet in Russia, as well as worldwide, became an increasing factor in political life, societal consciousness, and ideological development, controlling it also became a source of deep concern. Ever since they recognized its power, authorities have been trying to contain and control the internet.

Regimes like People's Republic of China and Iran's Islamic Republic rely on very strict technological and political censorship. Russia is not quite in the same camp and has frequently occupied a middle space between the Western-style freely communicative internet and the authoritarians, preferring instead to control internet technology from the inside by the use of political technology, state-generated content, and tactical propaganda.

6.1.4 Summary: Iran

Nested within its national security strategy, Iran pursues a soft war based cyber strategy comprised of various goals: to launch the National Information Network, to shape a second internet, to form a global coalition to challenge the American leadership/hegemony, to create a dominant discourse for an alternative governance model, to invest in indigenous high-tech industries, and to mobilize the general public in cyberspace to protect culture and traditions.

The state's information and communications monopoly has faced increasing challenges; the government has employed a rotating menu of responses, from mandatory content filtering to blocking access to sites deemed pornographic, antireligious, or politically subversive. As circumvention tools became more sophisticated, such filtering became less effective; but essential offensive cyber-operations revealed by major events like the Green Movement, allowed the regime to show more power and dominance. At the regional and international level, Tehran has engaged in destructive attacks to demonstrate its capacity for reaction; implicit threats are particularly effective in the Middle Eastern region, in particular against Israel and Saudi Arabia. The targets of Iranian cyber-operations often seem limited in scope, such as rival banks and airports in the region.

6.2 Cross-Case Analysis on China, Russia, and Iran: A Summary

The interest of strategically challenging American power has of necessity drawn Russia and China together; while the relationship is unequal and unstable, each nation's leadership has a stake in undermining U.S. power, any exploitation of global capitalism, and in any resistance of the progress of democratic values (Suri 2018). Each nation represents a unique challenge. Even each nation's vision of multipolarity shows distinct differences; while Russia intends to counter U.S. influence and reinforce its historical claim to power, China's perception of power sharing presents a more mutual process of gains. In Russia's perspective, multipolarity is always a competition against the top player.

While both China and Russia seek to change their status quo, it is Russia that has acted on the offensive by annexing territories, attacking neighboring states and taking subversive actions to support insurgents in other areas. Opponents have been assassinated, foreign elections have reported interference, and various institutions are undermined by Russian influence. As a peer competitor, China is motivated to contribute to developing an international order that it may potentially influence or dominate; by contrast, Russia is more accurately described as a rogue state, and seeks to subvert international order.

State Ideology: In both China and Russia the use of ideology is fluid. Kremlin frames its ideology in a manner that appeals to a broader base, offering space to ideological entrepreneurs and a broader audience (Laruelle 2017). The CCP references to both Confucius and communism, and while it salutes Maoist propaganda songs, it shows its supports of the Shanghai stock market. In this way, China's and Russia's propaganda strategies are similarly concerned as much with signaling as indoctrination (Pomerantsev 2015b).

Both the 'Chinese Dream' and Russkiy Mir have cast the respective visions for a strategic narrative solution to global and economic order. Each of these respective visions engage different mechanisms and institutions in a similar approach; the Russkiy Mir proposes a strategy led by the Eurasia Economic Union (EEU), while the Chinese Dream nominates the Silk Road Economic Belt (SREB) as a key leader in strategic implementation. Both have their advantages and drawbacks; however, as some studies

show the SREB has a slight advantage in being less explicitly political, more flexible, and better funded (Kanet and Sussex 2015).

Cyber Threat Assessment: China and Russia exploit their complex warfare approaches – the three-warfare and information war respectively – to respond to any real/perceived threat – that originates from shifts either in the international system, sub-system (regional), or in the domestic politics – endangers its national priorities within cyberspace. As regional powers, China and Russia, perceive American leadership in cyberspace and the Western-led cyber governance model (multi-stakeholderism) as systemic threats to their national cybersecurity and national information security priorities respectively. Both countries, in order to protect their culture, crafted alternative narratives – Chinese Dream and Russian World – to Western values for their domestic and regional audience. Additionally, China and Russia, through variety of regional and global initiatives try to manipulate actors and interest groups located in other states to advocate and institutionalize their preferred cyber governance model (multilateralism).

As for engagement with cyber threats, in addition to civilian and military units, all three countries benefit from cyber militia units and have formed such forces corresponding to the threat perception of each. China sees cyber-space as a key portion of informatization war, and so its cyber-militia unit focuses on that area, while Iran sees cyberthreats as a function of "soft-war" mechanics, and so its militia is geared toward soft-war tactics. Russia's militia units are activated to operated disinformation campaigns, as Russia categorizes cyberthreat as information warfare.

In China, Iran, and Russia both hackers who work for the government, and individual hackers who act on behalf of the government are encouraged. In the name of patriotism, a large number of students, academics, or otherwise interested individuals are encouraged to experiment hacking at any skill level. Some of these patriotic hacker groups have initiated attacks against people or groups who have offended or threatened the country.

Table 3– State's Cyber Units

	Civilian	Military	Cyber Militia
China	Cyberspace Administration of China (CAC) (2014)	PLA Strategic Support Force (2015)	PLA Unit 61398 (MUCD)
Iran	The Supreme Council of Virtual Space (2011)	Passive Defense Organization (2010): Iran's Cyber Iron Dome IRGC/Basij forces	Young Officers of the Soft War
Russia	Internet Research Agency (IRA)	Information Troopers	Unit 26165: Elite Military Hacking Center
The United States	Homeland Security – National Cyber Security Division (NCSD) (2003)	USCYBERCOM (2009)	780th Military Intelligence Brigade (2011)

6.2.1 Digital Authoritarianism

Information infrastructure is not exempt from politics. Information infrastructure is used not only by political elites, but increasingly by citizens themselves, who are becoming more and more used to having access and ability to consume and produce political content. From raising awareness about political events by real-time commentary on social media, documenting abuses and human rights violations with cell phone camera

technology, to pooling information about political corruption and state finances, citizens are used to a level of connectivity that is instantly disrupted when regimes shut it down in a bid for control (Howard, Agarwal and Hussain 2011).

China, Russia, and Iran are actively seeking ways to improve their control over social media, from blocking access to discussion forums and sites where they find dissents or critics gathering, to developing their own state-owned social media platforms where they are free to monitor and direct conversation. Most of these sites are far less popular than the international social media platforms like Facebook and Twitter (Bialy and Svetoka 2016). The authorities in Beijing, Moscow, and Tehran restrict internet freedom and block or order the removal of content on the following topics, which they consider endangers either the security of their regimes or the spiritual well-being and cohesion of their society. In fact, the 2017 Freedom on the Net (pp 14-21) report identifies China, Russia, and Iran the only countries in their respective regions that utilize a widespread ongoing censorship mechanism to filter contents on all of the following topics: criticism of authorities, corruption, conflict, political opposition, satire, social commentary, mobilization for public causes, blasphemy, LGBTQ issues, ethnic and religious minorities (Figures 14-16).

Figure 14 – Censored Topics by China

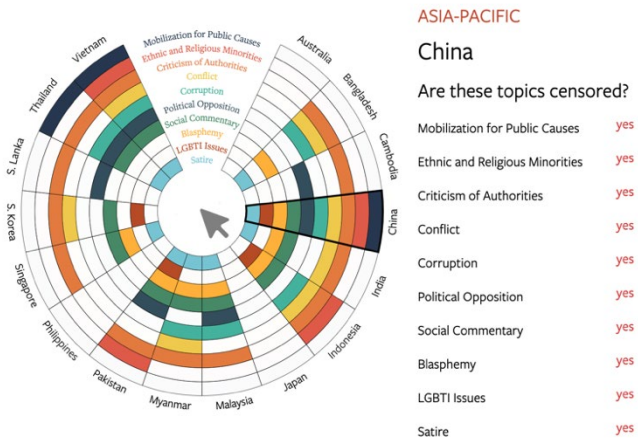
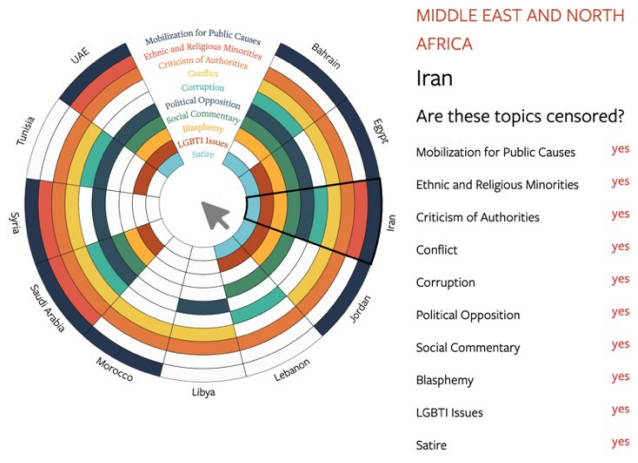


Figure 15 – Censored Topics by Russia

Figure 16 – Censored Topics by Iran



6.2.2 Cyber Sovereignty and Information Flow

Cyber Sovereignty: On the surface, Russia and China have similar interests when it comes to internet sovereignty; they both see the free flow of ideas on the internet as a potential security threat. But the technological divide between the two is significant. China's massive tech industry fuels the key pillars of its national policy, while Russia is less advanced. Even as they both control hacking operations abroad, they diverge in function. Russia trolls, while China steals. Comparing the two reveals an image of China as a rising digital superpower fueled by long-term ambitions and serious technological and cultural investment. Russia, by contrast, uses the power of the internet as a blunt instrument abroad, and fears the same use of that weapon at home (Saakashvili 2019).

Information Flow: (Ferracane, Lee-Makiyama and Van Der Marel 2018) As interconnectivity increases globally, every nation risks greater exposure to security risks and expenses. Similarly, the trade empowered by the positive effects of interconnectivity such as efficient communication, e-commerce, access to information and innovation, is always countered by the cybersecurity risks of openness.

The privacy laws of each nation reflect their individual priorities, cultures, and legal organizations; the Digital Trade Restrictiveness Index survey of 64 nations lists China as the most restrictive on digital trade, followed by Russia, India, Indonesia, and Vietnam. China tops the index in several digital trade restrictions, from public procurement and foreign investment, to Intellectual Property Rights, competition, and content access and standards. In some areas, restrictions merely increase costs around certain internet trade, but in other places trade can be blocked altogether. Between the

extreme data restriction and the quantitative trade restrictions, it can be extremely difficult for companies to do business in China.

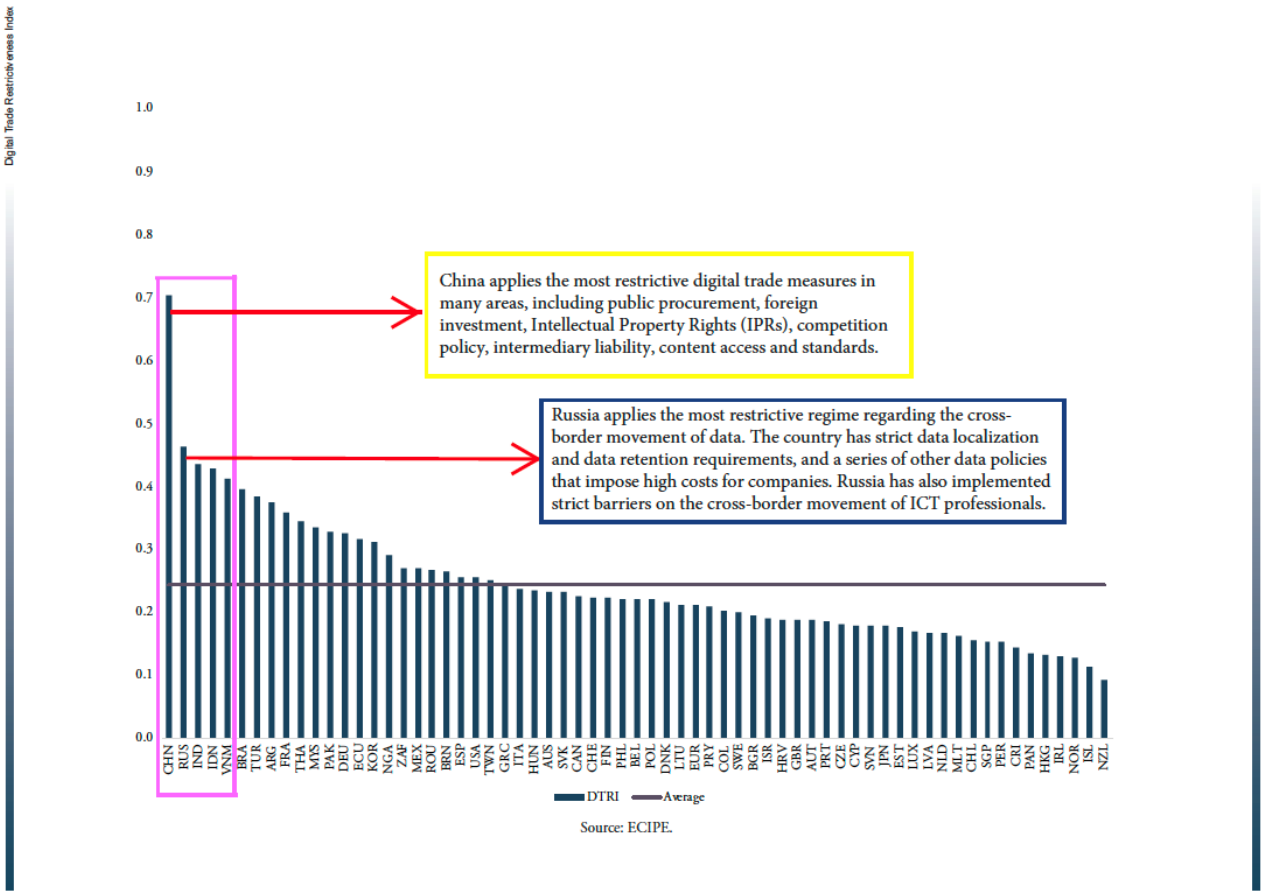
China's version of data localization is startlingly comprehensive, not only covering personal data collection, but also the broad categories of "important data" about "critical information infrastructure," a phrasing so categorical as to include every type of everyday information. "Critical information infrastructure" was the first legal phrase, broadened even more in later legal terms as "important data." The encompassing language essentially allows unconstrained government intervention, and actually increases the likelihood of international business to be subject to Chinese surveillance (Yuxi 2018).

The category covering "restrictions on data" includes privacy and security measures and other data policies in the index. In this category, Russia tops the list of 64, followed by Turkey and China. Russia's restrictive data policies include data localization requirements, and retention and transfer limitations. Russia, one of the most digitally restricted nations on tariffs, trade defense, foreign investment, content access, and e-commerce, also enforces policy restrictions on international travel for ICT professionals.

While both the EU and China have strong data policies, they are driven by different goals. The EU's General Data Protection Regulation (GDPR), motivated by personal privacy, gives individuals greater control over data, and requires certain protections of personal data. China's policies are more focused on policy control and justifying security restrictions on information flow and individual privacy. If restrictions were lifted on cross-border data flow in these nations, imports of services could rise by an average of 5%, in addition to the trade gains currently held subject by data policies. Local

companies and consumers, too, could benefit from cheaper or better online services from outside their own borders. Russia and China alone, if they removed restrictions on cross-border data movement, could see a service imports increase of over 50%, especially in computer and telecom services, the financial sector, and R&D services (Ferracane, Kren and van der Mare 2018).

Figure 17 – Digital Trade Restrictiveness Index (DTRI)



6.2.3 Influence Operation: The Case of Facebook and Instagram

In October of 2019, Facebook removed several networks of Pages, Groups, and individual accounts originating from Iran, Russia, and China, but the potential audiences

of these accounts concerned various regions, including the U.S., North Africa, Latin America, and Hong Kong. The reason given for removing these was engaging in *coordinated inauthentic behavior* on both Facebook and Instagram. Networks of accounts were certainly created with the goal of misleading other users of these platforms about who they were and what they were doing. Using compromised and fully fake accounts, the users behind this activity masqueraded as locals, managed Pages, joined Groups, and encouraged other users to click through to off-platform domains. The accounts, Groups, and Pages were managed according to best practices for increasing engagement, including liking and commenting on posts from other users (Gleicher 2018).

Focusing primarily on Hong Kong, the Chinese users posted under concealed identities about local political news, and controversial issues and events, like the protests in Hong Kong. These accounts reveal some links to individual users who may be connected to the regime (Gleicher 2019a). The activities originating in Russia which focused on U.S. audiences indicated a more consistent and well-organized endeavor and included some proactive attempts at security and privacy protections. These activities also show some connection to the *Internet Research Agency* (IRA). In this case, the active users took a more balanced approach, posting on both sides of political issues and events to generate reaction and participation in discussions on elections and candidates, environmental issues, racial tensions, LGBTQ concerns, and even confederate ideals. Some users posed as local accounts, positioned as either conservative or progressive, in swing states (Gleicher 2020).

Some activities originating in Iran reached French-speaking audiences in North Africa, although the bulk of the activities were directed toward the U.S. Posted content

was often tailored for each country's audience, including domestic and geopolitical news, and stories on public figures. In addition, posts included recycled reports from the Iranian state media reflecting the state position on various controversial topics, from Hezbollah activities to regional and international tensions and conflicts, including the war in Yemen, Iran-U.S. tensions, and conflicts between Israel and Palestine. Page admins and account owners perpetuating the activity also posted on U.S. political news and events, such as race relations events and the Black Lives Matter movement, criticisms toward the U.S. and Israel-defined Iranian policy, and other stories concerning Iranian foreign policies (Gleicher 2019b).

6.2.4 Cyber Governance/Diplomacy

The lack of governance in cyberspace, as in any space, represents the major difficulty as innovation outstrips regulatory management. To keep the system running smoothly and effectively, governance must solve market failures and deal with transgressions like cyber-warfare; however, issues of who owns the responsibility of governance and how it should be enforced continue to be debated, causing further delay in implementation. The five competitors currently contending for control over internet regulation are political states, international organizations, the private sector, non-government organizations, and academia. Each of these stakeholders are negotiating a "Wild West" world that lacks rules, norms, definitive expectations, and accountability for actions.

While cyber diplomacy is important to confronting threats, it is more critical for determining and maintaining the optimal balancing point between open and interoperable infrastructure, and reliable security of that infrastructure. Diplomacy in cyberspace

requires that states participate as a "whole of government dialogues," where states with a similar interest in preserving online freedoms should work together externally and push internal government departments to exert simultaneous effort toward the same goals, as well. Effective Cyber-diplomacy should also foster international operational cooperation between various actors, in order to build good common ground for necessary negotiations.

The 2015 cybersecurity pact between Russia and China features mutual assurance on non-aggression in cyberspace, and language which advocates for cyber-sovereignty. The pledge includes an agreement to prevent the progress of technologies with any potential to destabilize internal political and socio-economic atmosphere, interfere with internal state affairs, or disturb public order (Wei 2015).

6.3 Policy Recommendations for the United States

Internet and information security status is rapidly reaching crisis levels, and the vulnerabilities threaten nearly the whole nation. The landscape of cybersecurity today is far from the one promised by U.S. policy decisionmakers when cyber-security concerns were added to the national agenda more than two decades ago.[1] A threat which was once considered the domain of isolated hackers is now occupied by highly sophisticated criminal organizations often with powerful nation-state capabilities (Kelly and Hunker 2012). Cyber security was identified as early as 2000 as the third-highest national

[1] The Report of the President's Commission on Critical Infrastructure Protection. Critical Foundations Protecting America's Infrastructures. October 1997. Available at: https://fas.org/sgp/library/pccip.pdf

security priority concern for U.S. following counterterrorism and counterintelligence (Kshetri 2016).

The international balance of power is also more increasingly influenced by the growing disagreement in the global information space on the use and control of information and communication technologies. While some countries prioritize access to these technologies as a human rights issue, others seek to accomplish their regime's information-based objectives by controlling the information and content so that it reflects their preferred—and sometimes patently false—narratives in order to have more influence over citizens' thoughts and opinions.[2]

In 2008, Russian hackers penetrated the U.S. military network through cyber-attack, which infected broad range of computers and accessed both classified and unclassified data. The attack, which a senior military official labeled the "worst breach of U.S. military computers in history" (Prince 2010) was a wake-up call for strengthening cybersecurity measures and resulted in the establishment of the United Sates Cyber Command (USCYBERCOM) and the formation of the Cybersecurity Coordinator at the White House a year later. In 2011, U.S. Rep. Mike Rogers, Chairman of the House Permanent Select Committee on Intelligence, in an open hearing session on *Cyber Threats and Ongoing Efforts to Protect the Nation* identified China's economic espionage as "intolerable" and an act of "piracy". "Beijing is waging a massive trade war on us all" Rogers (2011) said and recommended to stop China's disruptive cyber

[2] Presidential Decree N 683, On the Russian Federation National Security Strategy, Moscow, 31 December 2015. In Fridman, Ofer. "The Russian perspective on information warfare: conceptual roots and politicization in Russian academic, political, and public discourse." Defense Strategic Communications 2, no. 2 (2017): 61-86.

behavior the United States and its allies in Europe and Asia should pressure Beijing through diplomatic and economic leverages they have over China. Since 2015, the US Intelligence Community has listed Iran as one of the major cyber threat actors (Clapper 2015), however, the country's cyber-attacks against the US infrastructure and institutions dates back to December 2009, when Iran's Cyber Army hacked Twitter in response to the widespread use of the microblogging platform as organization, information, and mobilization tool by Iranian activists after the disputed Presidential election.

Despite public acknowledgement of the threat, policy response in the U.S. has been concerningly passive, lacking any clear, effective, strategic legislation on cybersecurity, even though disruption, theft, espionage, and attack incidents are clearly on the rise. President Obama defined cyber security as one of the most significant security challenges for the U.S., increasing as critical infrastructure dependence on it grows (Kshetri 2016). In 2012, Gen. Keith Alexander, the former NSA chief and the first commander of the USCYBERCOM, said, cyber espionage attacks that target intellectual property and industrial data constitute the "greatest transfer of wealth in history" (Rogin 2012). The passivity of the legislative response (Table 4) only exacerbates the threats, and while Congress has debated comprehensive legislation, only modest steps have been agreed upon. The private sector's increasing dependence on the Internet leaves them seriously at-risk and yet it has not offered any solution (Washington Post 091919).

In its 2019 Worldwide Threat Assessment report to the Senate Select Committee on Intelligence, the U.S. Intelligence Community refers to China and Russia as the US adversaries and strategic competitors that not only "posed the greatest espionage and cyber-attack threats" over the past decade, but also they have advanced their cyber

capabilities to shape their target audiences' views – both their citizens and the US citizens – and interfere and undermine the US and Western democratic systems and values.[3] Gen. Keith Alexander warned us, "what we need to worry about is when these [cyber operations] transition from disruptive to destructive attacks" (Rogin 2012). Less than a decade not only China's and Russia's degree of attacks escalated from disruptive to destructive, but also their cyber capabilities transitioned from influence to interference.

Table 4 – Key Events and Milestones in the U.S. Response to Cybersecurity[4]

Administration	Time	Key Event/Document
President Bush	2003	National Strategy for Securing Cyberspace (NSSC)
	2006	National Infrastructure Protection Plan (NIPP)
President Obama	2008	Comprehensive National Cybersecurity Initiative (CNCI)
	2009	Cyber Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure
	2009	The Pentagon established the U.S. Cyber Command
	2009	The White House established the Cybersecurity Coordinator
	2013	Executive Order – Improving Critical Infrastructure Cybersecurity
	2015	Executive Order – Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities
	2015	Obama-Xi Cyber Agreement
	2016	Executive Order - National Emergency with Respect to Significant Malicious Cyber-Enabled Activities
President Trump	2018	The National Institute of Standards and Technology (NIST) Small Business Cybersecurity Act
	2018	The New US National Cyber Strategy
	2018	DHS as the primacy the Cybersecurity and Infrastructure Protection Agency
	2018	The White House authorized Offensive Cyber Operations
	2018	The U.S. rejected Russia's proposed cooperation on cyber issues

[3] Director of National Intelligence, *Worldwide Threat Assessment (WTA)*, US Intelligence Community, 29 January 2019.
[4] Source: Kshetri 2016, p. 90. (I added the events after 2013)

The United States lacks precise definitions of key related terms – such as cyber war, digital safe haven, expectations of privacy, and what constitutes acceptable and unacceptable cyber behavior – data privacy law; comprehensive cybersecurity legislation; information sharing protocol – especially within its private sectors – and as a superpower it has failed to create and enforce international norms for cyberspace or to join the existing global cyber agreements.

A major pressing matter that the U.S. has not figured out in cyber domain is precise definition of key related terms. Adam Segal (2011), Director of the Digital and Cyberspace Policy Program, Council on Foreign Relations argues that at the very least, two cyber declaratory statements should be issued by the United States to define terms, such as what kind of cyber activity constitutes an act of war, and to designate digital safe havens for civilians, which would be off-limits in the case of offensive operations. Gen. Michael Hayden, former CIA chief, adds "privacy" to this list; referring to the San Bernardino mass shooting incident and FBI's legitimate request to access the iPhone of the predator (Selyukh, 2016), Hayden questions the correlation between a "reasonable expectations of privacy" and "high-end unbreakable encryption" – is the relationship a linear industrial notion or a broader concept linked to national security (Ravich and May 2016).

Such declarations are critical to the adoption of international normative practices, another major priority that need to be addressed in cyber domain. Segal argues that precise definitions and declarations encourage cooperation and facilitates strategic stability not only by their presence, but by necessarily compelling actors to discuss the issues and consider the attainability and desirability of the norms as they build the

statements. Thus, the U.S. adversaries and competitors have "a more concrete picture of what type of attacks the United States will respond to and how, making signaling easier and improving stability" (Segal 2011). A concern recently raised on Capitol Hill by lawmakers. Senator Mark Warner (D-VA), the vice-chairman of the Senate Intelligence Committee, advocates for international rules being an essential piece of any cyber doctrine, citing the need for international norms to inform response strategy to problems (Zakrzewski 2018).

The United States' public conception of the web as an open commons space for commerce and information-driven exchange has been called into question with the elevated attention on domestic cyberspace security in the United States after the Russia's cyberattack at the Pentagon in 2008. In addition, refusing to enter negotiations concerning international cyber norms and regulations only reinforced the idea that the U.S. is quietly seeking dominance and control in cyberspace. International skepticism around U.S.-led cyber-governance mean that the U.S. will have to build a coalition of states who can work together to legitimize norms (Segal 2011). In addition to cyber alliances with partners, some cybersecurity experts also suggest that bilateral cyber agreements with adversaries might have some take away lessons that help in norm and regulation building in cyberspace (Ravich and May 2016).

The United States efforts for international norm building, partnership with allies and bilateral agreements with its adversaries in cyber domain are a mixed bag. Hillary Clinton's speech, as Secretary of State, on Internet's freedom and the United States stance on "single Internet" as a backbone of freedom of speech and equal access to

information was a historical moment in the U.S. leadership in cyberspace.[5] The Obama administration certainly conducted successful bilateral cyber agreements with both China and Russia. For instance, Washington-Moscow Cooperation on Information and Communications Technology Security in 2013 and Obama-Xi cyber agreement in 2015. As a part of the 2018 National Cyber Strategy, the "Cyber Deterrence Initiative" was announced, to foster coalition-building among ideologically compatible nations. The coalition is now comprised of 27 international members including the Five Eyes countries (Austin 2019).

But the United States experienced remarkable failures, including refusal of Trump administration to endorse the 2018 Paris initiative on Trust and Security in Cyberspace, where the U.S. allies as well as U.S. high-tech companies such as Google and Microsoft supported the call (Archer 2018). The White House also rejected Kremlin's multiple proposals for cooperation over cyber issues since 2016 (Council on Foreign Relations 082718). As Rep. Warner (D-VA) argued the lack of any comprehensive cyber-intelligence guide throughout the Bush and Obama administrations has led to the re-emergence of strong adversaries in Russia and China, in turn, leading to a virtual "open season" on American intellectual property and election interference (Zakrzewski 2018).

In the wake of countless cyber-attacks, Trump administration introduced two new federal cyber-related policies that map out and guide improvements to defend national cyber-infrastructure, networks, and data from cyberattacks. The National Institute of Standards and Technology (NIST) Small Business Cybersecurity Act, was signed into

[5] Clinton, Hillary Rodham. "Remarks on Internet Freedom". U.S. Department of State. 21 January 2010.

law in 2018, the same year the Trump Administration presented the new US National Cyber Strategy, the most comprehensive effort in 15 years. This strategy outlines a critical multi-agency path to securing infrastructure, promoting responsible international behavior, preventing the spread of malicious information, fighting cyber-crime, and fostering a strong cybersecurity workforce (Conner 2018).

Also, in 2018, President Trump signed a bill designating the Department of Homeland Security as the primary agency in charge of securing federal networks, protecting critical infrastructure, and overseeing civilian cybersecurity. The bill essentially rebrands the DHS' central cybersecurity unit as the Cybersecurity and Infrastructure Protection Agency (Beavers 2018). As a result, the priority for cybersecurity concerns has been elevated within the DHS, according to Krebs, and DHS will coordinate with both the private sector and other government agencies on critical infrastructure programs, under legislation with a specific intention of making communication between the private sector and the government more efficient (Zakrzewski 2018).

The Trump administration has significantly elevated cyberspace confrontation with China and Russia, recently signing an Executive Order to identify sabotage, rather than espionage, as the key foreign threat to the U.S., also declaring a national emergency. In the context of President Trump's statement, the term sabotage specifically means the idea that an adversary will have control of some or all of our critical infrastructure in case of a political crises, war, or other disaster (Austin 2019). New policies, outlined in the Defense Department Cyber Strategy and the National Cyber Strategy were introduced by

the Trump administration in 2018, which exert punitive measures toward countries engaging in malicious cyber activity (Austin 2019).

The offensive cyber operations authorized by the White House against U.S. adversaries is in line with the new policy that allows for some use of digital weapons in the name of national defense, a certain change from the Obama administration to the Trump administration, according to the then National Security Advisor John Bolton. As Hayden mentions in the absence of global cyber norms "all advantageous goes to the offense. Defense is an afterthought and very difficult and much more expensive than offense."[6] The focus of the Trump administration's strategy is foreign government attempts at targeting U.S networks, a strategy that includes a new classified presidential directive which allows military and other agencies to engage cyber operations when it is necessary to protect systems and national critical networks (Nakashima 2018).

While the United States represents their position toward cyberspace in the 2011 White House International Strategy documents as making progress toward more open, interoperable, reliable and secure infrastructure, China and Russia consistent argue for a principle of cyber-sovereignty, where each state should retain control over their own cyber-territory (Segal 2017). According to Segal policy makers in the U.S. tend to overly rely on a private-sector-led model for internet governance. They might see more progress by offering a positive, workable vision that provides a realistic alternative to the UN for developing nations (Segal 2018). However, Segal's view is in minority both on the Capitol Hill and amongst his colleagues. Former NSA chief, Michael Hayden, contends,

---

[6] "Fight of Our Lives: Michael Hayden on Intelligence, Security, and Transparency". *The Octavian Report*. May 2016.

"the first line of American defense in the cyber domain is the private sector, it is not the government" (Ravich and May 2016). And Robert Knake (2015), another cybersecurity expert with Council on Foreign Relations, advocates for private-private partnership and information sharing protocols within the private sector: "In a domain in which almost everything that needs to be protected is not in a commons (like air, space, or water) but is owned by private companies, there is only a limited number of things that private companies should look to government to do" (Knake 2015).

Unlike European Union, the United States lacks a comprehensive legislation for data protection law. Silicon Valley's biggest tech players assume that new regulations will be levied soon, and seek to work with regulators to influence the outcome, as much as they can, to favor their interests, and ensure the rules are clear about what they do—and don't—need to do in order to comply. Facebook and other large companies favor a wider adoption of the European Union's General Data Protection Regulation (GDPR), not because they agree with it entirely, but because working with a consistent set of regulations would be much more efficient than complying with each country's specific laws (Kafka 2019). Back in March, Mark Zuckerberg, CEO and Founder of Facebook endorsed stronger data protection laws and called for a more active role for governments. Future regulation should really be founded on the individual protections provided in the EU's GDPR, to specifically indicate how information is stored and how companies may use it, and in what ways information needs to be secured and protected, as well as what happens when companies such as Facebook fail to adhere to requirements. Zuckerberg continues, "the rules governing the Internet allowed a generation of entrepreneurs to build services that changed the world and created a lot of value in people's lives. It's time

to update these rules to define clear responsibilities for people, companies and governments going forward" (Zuckerberg 2019).

REFERENCES

"Teach Students How to Deal with Soft War". *Aftab News*. 20 October 2010.

"The platform For the Creation of a New Civilization Is Cyberspace". *Afkar News*. 26 December 2018.

Al-Khateeb, Samer, and Nitin Agarwal. "Understanding Strategic Information Maneuvers in Network Media to Advance Cyber Operations: A Case Study Analyzing Pro-Russian Separatists' Cyber Information Operations in Crimean Water Crisis." *Journal on Baltic Security* 2, no. 1 (2016): 6-27.

Anderson, Benedict. *Imagined communities: Reflections on the origin and spread of nationalism*. Verso books, 2006.

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

Applegate, LTC Scott D. "Leveraging Cyber Militias as a Force Multiplier in Cyber Operations." *George Mason University: Center for Secure Information Systems* 5 (2012).

Archer, Joseph. "US, Russia and China Refuse to Back French Cybersecurity Initiative". The Telegraph. 12 November 2018.

Arimatsu, Louise. "A treaty for governing cyber-weapons: Potential benefits and practical limitations." In *4th international conference on cyber conflict (CYCON 2012)*, pp. 1-19. IEEE, 2012.

Artusy, Donna V., and David V. Gioe. "Information Dominance between War and Peace: China as the 'Informationized' State." International Journal of Intelligence and Counterintelligence. (2018): 626-631.

Austin, Greg. *Cyber policy in China*. John Wiley & Sons, 2014.

Austin, Greg. "US ban on Huawei likely following Trump cybersecurity crackdown – and Australia is on board", *The Conversation*, 16 May 2019.

Bahree, Megha. "India Leads the World in The Number of Internet Shutdowns: Report". *Forbes*. 12 Nov 2018.

"What Is the Reason Behind the Filtering of Facebook?". *Balatarin*. 2 December 2013.

Ball, N. "Civil Society, Good Governance and the Security Sector". In Marina Caparini, Philip Fluri, and Ference Molnar (Eds.), *Civil Society and the Security Sector,*

Concepts and Practices in New Democracies. Geneva Center for Democratic Control of Armed Forces (DCAF), Lit Verlag: Berlin, 2006.

Barlow, John Perry. *Declaration of Independence for Cyberspace*. 1996. Available at: https://www.eff.org/cyberspace-independence

Bandurski, David. "College Teachers Must Be More 'Positive'", *China Media Project*, November 15, 2014.

Bandurski, David. "China Launches Cybersecurity Week", *China Media Project*, September 18, 2017.

Bandurski, David. "Yan Xuetong On the Bipolar State of Our World", *China Media Project*, 26 June 2018.

"Edward Snowden: Leaks that Exposed US Spy Programme", *BBC News*. 17 January 2014.

"Who's at the controls of Iran's bot army?". *BBC News*. 16 March 2016

"China Internet: Xi Jinping Calls for 'Cyber Sovereignty'", *BBC News*, December 16, 2015.

Bajoria, Jayshree. "Nationalism in China", *Council on Foreign Relations*, 22 April 2008.

Barbashin, Anton, and Hannah Thoburn. "Putin's Brain: Alexander Dugin and the Philosophy Behind Putin's Invasion of Crimea". Foreign Affairs. 31 March 2014.

Barbashin, Anton, Olga Irisova, Fabian Burkhardt, and Ernest Wyciszkiewicz. "A successful failure: Russia after Crime (a)." MISC, 2017.

Barry, Ellen and Andrew E. Kramer. "Billionaire Condemns Party He Led as a Kremlin 'Puppet'". *The New York Times*. 15 September 2011.

Bassin, Mark, and Gonzalo Pozo. *The politics of Eurasianism: identity, popular culture and Russia's foreign policy*. Rowman & Littlefield International, 2017.

Beavers, Olivia. "Trump Signs Bill Cementing Cybersecurity Agency at DHS", *The Hill*, 16 November 2018.

Beehner, Lionel. "Iran's Multifaceted Foreign Policy". *Council on Foreign Relations*. 7 April 2006.

Berzinš, Janis. "The New Generation of Russian Warfare". *Aspen Review*. Issue 3. 2014.

Bialy, Beata and Sanda Svetoka. "New Trends in Social Media". *NATO Strategic Communications Centre of Excellence*. December 2016.

Blasko, Dennis J. "Chinese Strategic Thinking: People's War in the 21st Century". The Jamestown Foundation. *China Brief*. Vol. 10, No. 6. 18 March 2010; Inkster, Nigel. *China's Cyber Power*. Routledge, 2018.

Boghardt, Thomas. "Soviet Bloc intelligence and its AIDS disinformation campaign." *Studies in Intelligence* 53, no. 4 (2009).

Bowles, Anna. "The changing face of the RuNet." *Control+ Shift. Public and private usages of the Russian Internet* (2006): 24-33.

Bradshaw, Samantha, Laura DeNardis, Fen Osler Hampson, Eric Jardine, and Mark Raymond. "The emergence of contention in global Internet governance." (2015).

Bradshaw, Samantha, and Philip N. Howard. "Challenging truth and trust: A global inventory of organized social media manipulation." *The Computational Propaganda Project* (2018).

Brangetto, Pascal, and M. K. S. Aubyn. "Economic aspects of national cyber security strategies." *Brangetto P., Aubyn MK-S. Economic Aspects of National Cyber Security Strategies: project report.* (2015).

Breslin, Shaun and Simon Shen. "When China Plugged In". In Simon Shen and Shaun Breslin (Eds) *Online Chinese nationalism and China's bilateral relations*. Lexington Books, 2010.

Buckland, Benjamin S., Fred Schreier, and Theodor H. Winkler. *Democratic governance challenges of cyber security*. Geneva: DCAF, 2010.

Buckley, Chris. "Crackdown on Bloggers Is Mounted by China", *the New York Times*, Sep 10, 2013.

Buzan, Barry. *People, States & Fear: An agenda for international security studies in the post-cold war era*. European Consortium for Political Research Press, 2008.

Campbell, Alexia Fernández. "The Employee Backlash Over Google's Censored Search Engine for China, Explained", *Vox*, 17 August 2018.

Carr, Madeline. "Power plays in global internet governance." *Millennium* 43, no. 2 (2015): 640-659.

Cavelty, Myriam Dunn. *Cyber-security and threat politics: US efforts to secure the information age*. Routledge, 2007.

"Guards at the Gate: The Expanding State Control Over the Internet in Iran". *Center for Human Rights in Iran*. January 2018.

"Institutional Development". *Center for Human Rights in Iran*. 9 January 2018.

"Security and Intelligence Agencies". *Center for Human Rights in Iran*. 9 January 2018.

Chang, Amy. *Warring State: China's Cybersecurity Strategy*. Center for a New American Security, 2014.

Cheng, Dean. *Cyber Dragon: Inside China's Information Warfare and Cyber Operations: Inside China's Information Warfare and Cyber Operations*. ABC-CLIO, 2016.

Chernenko, Elena. "Russia's cyber diplomacy". In Nicu Popescu and Stanislav Secrieru (Eds.). *Hacks, Leaks and Disruptions: Russian Cyber Strategies*. Chaillot Papers. (Paris: European Union Institute for Security Studies). October 2018.

"Xi Vows to Build China into a Cyber Power", *China Radio International's English Service*, 27 February 2014.

Chubb, Andrew. "Xi Jinping: A Hardline Nationalist in Control of China?", *South Sea Conversations*, 14 December 2012.

Clark, David. "A Cloudy Crystal Ball: Visions of the Future". *24th Internet Engineering Task Force*, 1992.

Clapper, James R., *Worldwide Threat Assessment of the US Intelligence Community*, Senate Committee on Armed Services, January 31, 2012.

Clapper, James R., *Worldwide Threat Assessment of the US Intelligence Community*, Senate Committee on Armed Services, April 18, 2013.

Clapper, James R., *Worldwide Threat Assessment of the US Intelligence Community*, Senate Committee on Armed Services, January 29, 2014.

Clapper, James R., *Worldwide Threat Assessment of the US Intelligence Community*, Senate Committee on Armed Services, 2015.

Clover, Charles. "Xi Jinping signals departure from low-profile policy", *Financial Times*, 20 October 2017.

Coats, Daniel R., *Worldwide Threat Assessment of the US Intelligence Community*, Senate Committee on Armed Services, January 29, 2019.

Connell, Michael, and Sarah Vogler. *Russia's Approach to Cyber Warfare (1Rev)*. No. DOP-2016-U-014231-1Rev. Center for Naval Analyses Arlington United States, 2017.

Conner, Bill. "Two Cybersecurity Policies, One Clear New Objectives", *The Hill*, 20 November 2018.

Cook, Sarah. "China's Cyber Superpower Strategy: Implementation, Internet Freedom Implications, and U.S. Responses", House Committee on Oversight and Government Reform, Subcommittee on Information Technology, 26 September 2018a.

Cook, Sarah. "China's Cyber Superpower Strategy: Implementation, Internet Freedom Implications, and U.S. Responses", Freedom House, 28 September 2018b.

Cooley, Alexander, and Daniel H. Nexon. "How Hegemony Ends." *Foreign Affairs.* 99 (2020): 143.

"Russia Wants a Deal with the United States on Cyber Issues. Why Does Washington Keep Saying No?". Council on Foreign Relations. 27 August 2018.

Creemers, Rogier, Paull Triolo, and Graham Webster. "Translation: China's new top Internet official lays out agenda for Party control online", New America, 24 September 2018.

Creemers, Rogier. "China's Social Credit System: An Evolving Practice of Control." *Available at SSRN 3175792* (2018).

Dai Qingli. "China Itself Is Facing Growing Cyber Crime and Attacks". *Financial Times*. November 10, 2011.

Delia, L. I. N., and Susan TREVASKES. "Creating a Virtuous Leviathan: The Party, Law, and Socialist Core Values." *Asian Journal of Law and Society* 6, no. 1 (2019): 62.

DeLisle, Jacques, Avery Goldstein, and Guobin Yang, eds. *The internet, social media, and a changing China*. University of Pennsylvania Press, 2016.

DeNardis, Laura. *The Global War for Internet Governance*. Yale University Press, 2014.

De Putter, Jos. "Backlight: the Chinese World Order". VPRO Backlight/NPO. 2016 (Video File).

"China cracks down on social media giant Weibo to maintain 'social stability'". Deutsche Welle. 28 January 2018.

Diamond, Larry. “Chinese Influence and American Interests: Promoting Constructive Vigilance.” *YouTube: Hoover Institution*. 14 Feb 2019.

Diamond, Larry, and Orville Schell, eds. *China's influence and American interests: Promoting constructive vigilance*. Hoover Press, 2019.

DiResta, Renee, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, and Ben Johnson. “The tactics & tropes of the Internet Research Agency.” (2019).

“Assessment on U.S. Defense Implications of China’s Expanding Global Access”, U.S. Department of Defense, December 2018.

Durden, Tyler. “Gen. Dunford Slams Google's ‘Inexplicable’ Deepened Ties with China as It Cuts Pentagon Projects”, *Zero Hedge*, 7 December 2018.

“The East is Pink”. The Economist. 13 August 2016.

Economy, Elizabeth C. *The Third Revolution: Xi Jinping and the New Chinese State*. Oxford University Press, 2018, p. 72.

Eisenstadt, Michael. “Iran’s Lengthening Cyber Shadow”. *Research Note No. 34*. The Washington Institute for Near East Policy. July 2016.

“CPC’s Fearless Campaign of Self-Reform”, English Edition of Xinhua, 3 June 2019.

Esfahlani, Mohammad Sadeghi. “The politics and anti-politics of Facebook in context of the Iranian 2009 presidential elections and beyond.” *Social Media in Iran: Politics and Society after* (2009): 144.

“The IRGC’s Instruction on How to Counter Soft War”. *Etemad Newspaper*. 3 September 2012.

“University Professors Should Pay Attention to Confronting the Soft War of the Enemy”. *Fars News*. 19 September 2012.

“In Soft War, Enemies Have Targeted Ideological Resistance”. *Fars News*. 20 September 2012.

“Spreading the Culture of Martyrdom Is the Best Way to Deal with Soft War”. *Fars News*. 22 September 2012.

“The Enemy’s Tactic Is to Attack the Iranian Intellectual Frontiers”. *Fars News*. 24 September 2012.

"The Period of the Sacred Defense Should Be the Model of Victory in Soft War". *Fars News*. 26 September 2012.

"It Is Necessary to Control Cyberspace". *Fars News*. 2 Oct 2012.

"The Ministry of Defense Unveils 'Safe Mobile' Project and Other Indigenous Cyber-Related Products". *Fars News*. 14 Dec 2013.

"Basiji Artists are the Officers of Soft War". *Fars News*. 11 July 2015.

"Clergymen Are at the Forefront of the Soft War," editorial, *Fars News.* 23 June 2018.

Faris, David M. "Architectures of Control and Mobilization in Egypt and Iran." *Social Media in Iran: Politics and Society after 2009* (2015): 199.

Faris, Robert, Hal Roberts and Stephanie Wang. "China's Green Dam: The Implications of Government Control Encroaching on the Home PC", *OpenNet Initiative Bulletin*, OpenNet Initiative. 2009.

Farley, Robert. "Did the Obama-Xi Cyber Agreement Work?", *The Diplomat*, 11 August 2018.

Farnsworth, Timothy. "China and Russia Submit Cyber Proposal". *Arms Control Today*. October 2011.

Farrell, Henry, and Abraham L. Newman. "Weaponized interdependence: How global economic networks shape state coercion." *International Security* 44, no. 1 (2019): 42-79.

Ferracane, Martina Francesca, Hosuk Lee-Makiyama, and Erik Van Der Marel. "Digital Trade Restrictiveness Index." *European Center for International Political Economy, Brussels: ECIPE*. 2018.

Ferracane, Martina F., Janez Kren, Erik van der Mare. "The Cost of Data Protectionism". VOX. 25 October 2018.

Finnemore, Martha, and Kathryn Sikkink. "International norm dynamics and political change", *International organization* 52, no. 4 (1998): 887-917.

Fitsanakis, Joseph. "After China, Russia May Ban Some Apple Products, Fearing Espionage". *Intelnews*. 4 December 2014.

Foushee, Hampton. "Gray area: The future of Chinese internet." *Harvard International Review* (2006).

Freiberg, Phillip. “Putin's Russia-On a Path to Cyber Sovereignty?.” 2014.

Fridman, Ofer. “The Russian Perspective on Information Warfare: Conceptual Roots and Politicization in Russian Academic, Political, And Public Discourse”. *Defence Strategic Communications*. Vol. 2. Spring 2017.

Gessen, Masha. “The Undoing of Bill Clinton and Boris Yeltsin’s Friendship, and How It Changed Both of Their Countries”. The New Yorker. 5 September 2018.

Ghafouri, Qassem. “Obama’s New Dreams”. *Siasat-e Rooz*. 9 Nov 2013.

Giles, Keir. "“Information Troops”-A Russian Cyber Command?" In *2011 3rd International Conference on Cyber Conflict*, pp. 1-16. IEEE, 2011.

Giles, Keir. *The next phase of Russian information warfare*. Vol. 20. Riga: NATO Strategic Communications Centre of Excellence, 2016.

Glasser, Susan B. “Putin the Great: Russia's Imperial Impostor.” *Foreign Affairs.* 98 (2019): 10.

Gleicher, Nathaniel. “Coordinated Inauthentic Behavior Explained”. *Facebook*. 6 December 2018.

Gleicher, Nathaniel. “Removing Coordinated Inauthentic Behavior from China”. *Facebook*. 9 August 2019a.

Gleicher, Nathaniel. “Removing More Coordinated Inauthentic Behavior from Iran and Russia”. Facebook. 21 October 2019b.

Gleicher, Nathaniel. “Removing Coordinated Inauthentic Behavior from Russia”. *Facebook*. 12 March 2020.

Golkar, Saeid. *Captive Society: The Basij militia and social control in Iran*. Columbia University Press, 2015.

Grace, Abigail. “Comprehensive National Power with Chinese Characteristics: Regional Security Partnerships in the Xi Era”, *Brookings Institute*, 22 January 2019.

Goldstein, Judith, and Robert Owen Keohane, eds. *Ideas and foreign policy: beliefs, institutions, and political change*. Cornell University Press, 1993.

Grothaus, Michael. “China’s Orwellian Social Credit System Is Expanding Overseas”, *Fast Company*, 28 June 2018.

Graff, Garrett M. “How the US Forced China to Quit Stealing – Using A Chinese Spy”, Wired, 11 October 2018.

Hai-Li, Wang. “Informatization Development Status of Russia and Its Enlightenment to China.” In *2014 Sixth International Conference on Measuring Technology and Mechatronics Automation*, pp. 345-348. IEEE, 2014.

Hare, Forrest. “Borders in cyberspace: can sovereignty adapt to the challenges of cyber security.” In Czosseck, C., and K. Geers (eds.). *The Virtual Battlefield: Perspectives on Cyber Warfare* 3 (2009).

Hathaway, Melissa E., and Alexander Klimburg. “Preliminary considerations: on national cyber security.” *National Cyber Security Framework Manual. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn* (2012).

“Virtual Space: A Bridge to Transfer Iranian-Islamic Culture to the World”. *Hawzah News Agency*. 4 December 2018.

Häußler, Ulf. “Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO Treaty.” *International Cyber Security Legal & Policy Proceedings* (2010): 104-5.

Heath, Timothy. “Strategic Consequences of the U.S. Withdrawal from the TPP”, *The Cipher Brief*, 26 March 2017.

Heath, Timothy R., Kristen Gunness, and Cortez A. Cooper. *The PLA and Chinas Rejuvenation: National Security and Military Strategies, Deterrence Concepts, and Combat Capabilities*. No. RR-1402-OSD. RAND Corporation-National Defense Research Institute Santa Monica United States, 2016.

Heginbotham, Eric, Michael Nixon, Forrest E. Morgan, Jacob Heim, Jeff Hagen, Sheng Tao Li, Jeffrey Engstrom, Martin C. Libicki, Paul DeLuca, David A. Shlapak, David R. Frelinger, Burgess Laird, Kyle Brady, and Lyle J. Morris, *The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996–2017*. Santa Monica, CA: RAND Corporation, 2015.

Heilmann, Sebastian, “Distinctive Features of the Policy Process”, *China's Political System* (Kindle Locations 1354-1355). Rowman & Littlefield Publishers. 2016. Kindle Edition.

Heilmann, Sebastian and Moritz Rudolf, “The Constitution of the Party-State”, *China's Political System* (Kindle Locations 1354-1355). Rowman & Littlefield Publishers. 2016. Kindle Edition.

Heilmann, Sebastian and Lea Shih, “The Central Government”, *China's Political System* (Kindle Locations 1354-1355). Rowman & Littlefield Publishers. 2016. Kindle Edition.

Heilmann, Sebastian. “How the CCP Embraces and Co-opts China’s Private Sector”. MERICS. 21 November 2017.

Hern, Alex. “May Calls Again for Tech Firms to Act on Encrypted Messaging”. *The Guardian*. 25 January 2018.

Hernandez, Javier C. “China’s Propaganda Machine Takes Aim at U.S. Over Trade War”. The New York Times. 14 May 2019.

Hillman, Jonathan. “Influence and Infrastructure: The Strategic Stakes of Foreign Projects”. *Center for Strategic and International Studies*. January 2019.

Hirschman, Albert O. *Exit, voice, and loyalty: Responses to decline in firms, organizations, and states*. Vol. 25. Harvard university press, 1970.

Hoffman, Samantha. "Social credit." *Australian Strategic Policy Institute* 28 (2018).

Howard, Philip N., Sheetal D. Agarwal, and Muzammil M. Hussain. "When do states disconnect their digital networks? Regime responses to the political uses of social media." The Communication Review 14, no. 3 (2011): 216-232.

Howard, Philip N., Sheetal D. Agarwal, and Muzammil M. Hussain. “The Dictators’ Digital Dilemma: When Do States Disconnect Their Digital Networks?” (2011).

Howard, Philip N., Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille François. “The IRA, social media and political polarization in the United States, 2012-2018.” (2019).

Hussain, Muzammil M. *State power 2.0: Authoritarian entrenchment and political engagement worldwide*. Routledge, 2016.

“As Fragile as a Crystal Glass: Press Freedom in Iran”. Human Rights Watch. 1999.

Ighani, Helia. “Facebook in Iran: The Supreme Leader”. *The Iran Premier*. 16 April 2013.

“What Were the Demands of the Supreme Leader in Cyberspace and What Was the Outcome?”. *Iran Hoshdar*. 10 March 2018.

Jackson, Laura. “Revisions of Reality: The Three Warfares—China’s New Way of War”, in *Information at War: From China’s Three Warfares to NATO’s Narratives*, Legatum Institute, September 2015.

"Sacred Migration: Boroujerdi's Recommendation to the Nation". *Jamaran News*. 9 April 2018.

"Japan, U.S., Australia and India look to establish alternative to China's Belt and Road Initiative", *The Japan Times*, 19 February 2018.

"Artists Play a Key Role in Countering the Soft War". Javan Online. 8 June 2010.

Jayawardane, Sash, J. E. Larik, and Erin Jackson. "Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance." *The Hague Institute for Global Justice Policy Brief* (2015).

Jean-Baptiste Jeangène Vilmer and Paul Charon. "Russia As A Hurricane, China As Climate Change: Different Ways of Information Warfare". *War on the Rock*. 21 January 2020.

Jiang, Min. "The Co-Evolution of the internet, (Un)Civil society & authoritarianism in China." In DeLisle, Jacques, Avery Goldstein, and Guobin Yang, eds. *The internet, social media, and a changing China*. University of Pennsylvania Press, 2016: 28-48.

Joubert, Vincent. "Getting the essence of Cyberspace; a Theoretical Framework to Face Cyber Issues." In Czosseck, Christian., and Karlis Podins (eds.). *Conference on Cyber Conflict Proceedings.* CCD COE Publications, Tallinn, Estonia. 2010.

Kaarbo, Juliet. "Foreign policy analysis in the twenty-first century: back to comparison, forward to identity and ideas." *International Studies Review* 5, no. 2 (2003): 156-202.

Kafka, Peter. "Mark Zuckerberg Wants You — and Your Government — to Help Him Run Facebook". *Vox*. 31 March 2019.

Kaldor, Mary. *New and old wars: Organized violence in a global era*. John Wiley & Sons, 2013.

Kanet, Roger E., and Matthew Sussex, eds. *Russia, Eurasia and the new geopolitics of energy: Confrontation and consolidation*. Springer, 2015.

Kang, Cecilia and David E. Sanger. "Huawei Is a Target as Trump Moves to Ban Foreign Telecom Gear", *The New York Times*, 15 May 2019.

Kania, Elsa, Samm Sacks, Paul Triolo, and Graham Webster. "China's Strategic Thinking on Building Power in Cyberspace". New America. 25 September 2017.

Kargar, Simin, and Keith McManamen. “Censorship and collateral damage: Analyzing the Telegram ban in Iran.” *Berkman Klein Center Research Publication* 2018.

Keck, Zachary. “Four Things China Learned from the Arab Spring”. *The Diplomat*. 4 January 2014; Parello-Plesner, Jonas. “China and the Arab Spring: External and Internal Consequences and Implications for EU-China Cooperation”. *ISPI Analysis*. No. 53. May 2011.

Kelly, Sanjay., Sarah Cook, and Mai Truong (Eds.). *Freedom on the Net 2012: A Global Assessment of Internet and Digital Media*, Washington D.C.: Freedom House, 2013.

Kelly, Sanjay. Madeline Earp, Laura Reed, Adrian Shahbaz, and Mai Truong (Eds.). Freedom on the Net 2014. *Tightening the Net: Governments Expand Online Controls*. Washington D.C.: Freedom House, 2015.

Kelly, Sanjay et al (Eds.). *Freedom on the Net 2015: Privatizing Censorship, Eroding Privacy*. Washington D.C.: Freedom House. 2016.

Kelly, Sanjay et al (Eds.). *Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy*. Washington D.C.: Freedom House. 2018.

Kelly, Terrance K., and Jeffrey Hunker. "Cyber policy: Institutional struggle in a transformed world." *ISJLP* 8 (2012): 210.

Kennedy, Paul. *The rise and fall of the great powers*. Vintage, 2010. Cited in Randall L. Schweller. “Managing the Rise of Great Powers: History and Theory.” *Engaging China: The Management of an Emerging Power* (1999): 1-31.

Khoshnevis, Yaser. “Multilateral Governance in Virtual Space”. *National Center for Cyberplace*. Report No. 3, June 2018.

King, Gary, Jennifer Pan, and Margaret E. Roberts. "How censorship in China allows government criticism but silences collective expression." *American Political Science Review* 107, no. 2 (2013): 339.

Kirchner, Emil J., and James Sperling, eds. *National security cultures: patterns of global governance*. Routledge, 2010.

Kitchen, Nicholas. “Systemic Pressures and Domestic Ideas: A Neoclassical Realist Model of Grand Strategy Formation.” *Review of International Studies* 36, no. 1 (2010): 117-43.

Kissinger, Henry. *A world restored: Metternich, Castlereagh, and the problems of peace, 1812-22*. Pickle Partners Publishing, 2017.

Klimburg, A. (Ed.). *National cyber security framework manual*. NATO Cooperative Cyber Defense Center of Excellence. 2012.

Klimburg, Alexander, and Philipp Mirtl. *Cyberspace and Governance – A Primer* (Working Paper 65). 2012.

Klimburg, Alexander, and Jason Healey. "Strategic Goals and Stakeholders." *National Cyber Security Framework Manual* (2012): 66-107.

Knake, Robert. "Business Risk: Focus on Private-Private Partnerships". *Security Roundtable*. 7 December 2015.

Krauthammer, Charles. "The unipolar moment." *Foreign Affairs.* 70 (1990): 23.

Kremer, Jan-Frederik, and Benedikt Müller, eds. *Cyberspace and international relations: Theory, prospects and challenges*. Springer Science & Business Media, 2013.

Kremer, Jan-Frederik, and Benedikt Müller. "SAM: A Framework to Understand Emerging Challenges to States in an Interconnected World." In *Cyberspace and International Relations*, pp. 41-58. Springer, Berlin, Heidelberg, 2014.

Korsunskaya, Darya. "Putin says Russia must prevent 'color revolution'". *Reuters*. 20 November 2014.

Kovaleva, Natalya. "Russian Information Space, Russian Scholarship, and Kremlin Controls". *Defense Strategic Communications* 4, no. 4 (2018): 133-171.

Kshetri, N., *The Quest to Cyber Superiority*, Springer, Switzerland, 2016, p. 123.

Kurowska, Xymena, and Anatoly Reshetnikov. "Russia's trolling complex at home and abroad." *Hacks, Leaks and disruption Russian cyber strategies* (2018).

Kurlantzick, Joshua. "The Belligerents: Meet the Hardliners Who Now Run China's Foreign Policy". *The New Republic*. 26 January 2011.

Kynge, James, and Chris Campbell, Amy Kazmin and Farhan Bokhari. "How China Rules the Waves". *Financial Times*. 12 January 2017.

Kynge, James. "China, America And the Road to A New World Order", Financial Times, 6 December 2018.

Laruelle, Marlene. "The "Russian World": Russia's soft power and geopolitical imagination." *Center on Global Interests* (2015).

Laruelle, Marlene. “Putin’s Regime and the Ideological Market: A Difficult Balancing Game”. *Task Force White Paper*. Carnegie Endowment for International Peace. 16 March 2017.

Laskai, Lorand. “What Will the U.S.-China Cyber Relationship Look Like in the Trump Era? A View from China”, *Council on Foreign Relations*, 11 October 2017.

Laurinavičius, Marius. “Dmitry Rogozin’s Clan: Visionaries and Executors Behind Aggression Towards Ukraine”. 2014.

Levin, David. “At U.N., China Tried to Influence Fight Over Internet Control”, *The New York Times*, 16 December 2015.

Levitsky, Steven, and Lucan A. Way. *Competitive authoritarianism: Hybrid regimes after the Cold War*. Cambridge University Press, 2010.

Lewis, J. A. “Cybersecurity and critical infrastructure protection”. *Center for Strategic and International Studies*. 2006.

Lewis, J.A. (2011) ‘Confidence-building and international agreement in cybersecurity’, *Disarmament Forum: Confronting Cyberconflict*. Vol.4, pp. 51–62.

Lewis, J.A. and Timlin, K. *Cybersecurity and cyberwarfare: Preliminary assessment of national doctrine and organization*. Center for strategic and international studies. (2011).

Lewis, J.A. (2014) ‘National Perceptions of Cyber Threats’, *Strategic Analysis*, 38(4), pp. 566–576.

Li, Cheng. "One Party, Two Factions: Chinese Bipartisanship in the Making?." In *Conference on Chinese Leadership, Politics, and Policy, Carnegie Endowment for International Peace, Washington, DC*. 2005.

Lin, Herbert. “Thoughts on threat assessment in cyberspace.” *I/S: A Journal of Law and Policy for Information Society,* 8 (2012): 337.

Lind, Jennifer, and William C. Wohlforth. “The Future of the Liberal Order is Conservative: A Strategy to Save the System.” *Foreign Affairs.* 98 (2019): 70-80.

Lindsay, J. (2012) ‘China and Cybersecurity: Political, Economic, and Strategic Dimensions’, *report from workshops held at the University of California, San Diego*. pp. 21–22.

Lindsay, J.R., Cheung, T.M. and Reveron, D.S. (2015) *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Oxford University Press.

Lindsay, J.R. (2015) 'The Impact of China on Cybersecurity: Fiction and Friction', *International Security*, 39(3), p. 12.

Lim, Kevjin. *Grand Strategic Adjustments in Post-Revolutionary Iran: A Neoclassical Realist Account*, Yuval Ne'eman Workshop for Science, Technology and Security officials, Tel Aviv University Press, Tel Aviv, 2016.

Lipman, Maria. Putin's "Sovereign Democracy". *Carnegie Moscow Center*. Washington Post. 15 July 2006.

"Kremlin's millions: How Russia funds NGOs in Baltics", Lithuania Tribune. 4 September 2015.

Lobell, Steven E., Norrin M. Ripsman, and Jeffrey W. Taliaferro, eds. *Neoclassical realism, the state, and foreign policy*. Cambridge University Press, 2009.

Lobell, Steven E. "Threat assessment, the state, and foreign policy: a neoclassical realist model." *Neoclassical realism, the state, and foreign policy* (2009): 42-74.

Luckerson, Victor. "Why China Is a Nightmare for American Internet Companies". TIME. 27 February 2014.

Luiijf, H. A. M., and Jason Healey. *Organizational structures & considerations*. Tallinn: NATO CCD COE Publication, 2012.

Lyall, Nicholas. "China's Cyber Militias". *The Diplomat*. 01 March 2018.

Lysenko, Volodymyr, and Catherine Brooks. "Russian information troops, disinformation, and democracy." *First Monday* (2018).

M-Trends 2019: FireEye Mandiant Services, Special Report, FireEye, VA, 2019.

MacFarquhar, Neil. "A Powerful Russian Weapon: The Spread of False Stories". The New York Times. 28 August 2016.

Majidyar, Ahmad. "Iran Revokes Telegram License as Authorities Step Up Internet Crackdown". *The Middle East Institute*. 26 April 2018.

"The Effective Role of the Ministry of Intelligence in Countering the Enemy's Cyber War". Mardomsalari Newspaper. 4 July 2012.

McKune, Sarah. "An Analysis of the International Code of Conduct for Information Security", *The Citizen Lab*, University of Toronto, 28 September 2015

Malle, Silvana. "The All-Russian National Front–for Russia: a new actor in the political and economic landscape." Post-Communist Economies 28, no. 2 (2016): 199-219.

Manzo, Vincent. “Deterrence and escalation in cross-domain operations: Where do space and cyberspace fit?” In *Strategic Forum*, no. 272, p. 1. National Defense University, 2011.

Mateski, Mark. “Russia, Reflexive Control, and the Subtle Art of Red Teaming” Red Team Journal, October 13, 2016. Cited in Kowalewski, Annie. “Disinformation and Reflexive Control: The New Cold War”. Georgetown Security Studies Review. 1 February 2017.

Mattis, Peter. “China's International Right to Speak”. *Jamestown Foundation*. 19 October 2012.

Mattis, Peter. “An American Lens on China’s Interference and Influence-Building Abroad”. The Asian Forum. 30 April 2018.

Maurer, Tim, and Garrett Hinck. "Russia: Information Security Meets Cyber Security." *Russia: Information Security Meets Cyber Security* (2018): 39-57.

McBride, James and Andrew Chatzky. “Is ‘Made in China 2025’ a Threat to Global Trade?”, *Council on Foreign Relations*, 7 March 2019.

McGregor, James. “How Trump Can Win with China”, Foreign Policy, 3 February 2017.

Mearsheimer, John J. “Can China rise peacefully?”. *The National Interest* 25 (2014): 23-37.

Meltzer, Joshua P. “Cybersecurity and Digital Trade: What role for international trade rules?”. *Brookings Institute*. November 2019.

Moore, Malcolm. “Blocked by police, Chinese campaigners get creative”, *The Telegraph*, March 2, 2012.

Mshvidobadze, Khatuna. “The Battlefield on Your Laptop”. *Radio Free Europe*. 21 March 2011.

Mueller, Milton. *Will the Internet fragment? Sovereignty, globalization and cyberspace*. John Wiley & Sons, 2017a.

Mueller, Milton. “Internet Fragmentation Exists, But Not in the Way That You Think”. *Net Politics and Digital and Cyberspace Policy Program*. Council on Foreign Relations. 12 June 2017b.

Mueller, Milton, Andreas Schmidt, and Brenden Kuerbis. “Internet security and networked governance in international relations.” *International Studies Review* 15, no. 1 (2013): 86-104.

Nakashima, Ellen. “The White House has authorized offensive cyber operations to deter foreign adversaries”, *The Washington Post*, 20 September 2018.

“Cyberspace Strategy of the Islamic Republic of Iran”. *National Center for Cyberspace*. July 2018.

“National Network of Information”. *National Center for Cyberspace*. 5 September 2017.

“Protecting the Communication and Information Infrastructure of the Country's Cyberspace”. *National Center for Cyberspace*. 10 March 2020.

“Telegram: A Project for Specific Countries”. *National Center for Cyberspace*. March 2018.

Naughton, John. “The evolution of the Internet: from military experiment to General Purpose Technology.” *Journal of Cyber Policy* 1, no. 1 (2016): 5-28.

Newton, Matthew and Julia Summers. “Russian Data Localization Laws: Enriching “Security” & the Economy”. The Henry M. Jackson School of International Studies. University of Washington. 28 February 2018.

Nocetti, Julien. “Contest and conquest: Russia and global internet governance.” *International Affairs* 91, no. 1 (2015): 111-130.

Nye Jr, Joseph. *Cyber power*. Harvard University. Belfer Center for Science and International Affairs, 2010; “Iran’s Cyber Threat”.

Nye, Joseph. “Nuclear lessons for cyber security?” *Strategic Studies Quarterly* 5, no. 4 (2011): 18-38.

Nye, Joseph. “The Mouse Click That Roared.” *The Korea Times* (2013).

Obama, Barack. “Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities”, *The White House*, 01 April 2015.

Ogrysko, Volodymyr. *Russian Information and Propaganda War: Some Methods and Forms to Counteract*. NATO Strategic Communications Center of Excellence. 2016.

Ostrom, Elinor. “Beyond markets and states: polycentric governance of complex economic systems.” *American Economic Review* 100, no. 3 (2010): 641-72.

Ottis, Rain. “Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability.” In *8th European Conference on Information Warfare and Security*, pp. 177-182. 2009.

Ottis, Rain. "Theoretical offensive cyber militia models." *Leading Issues in Information Warfare and Security Research* 1 (2011): 135.

Pieper, Moritz. “Russkiy Mir: the geopolitics of Russian compatriots abroad.” *Geopolitics* (2018): 1-24.

Paris, Francesca. “U.S. Leadership Falls Further Behind China in Global Regard, Gallup Poll Finds”, *National Public Radio*, 28 February 2019.

Patrick, Stewart M., “Belt and Router: China Aims for Tighter Internet Controls with Digital Silk Road”, *the Internationalist*, Council on Foreign Relations, 2 July 2018.

Paulson, Hank. *Dealing with China*. Hachette UK, 2015.

Pigman, Lincoln. “Russia’s Vision of Cyberspace: A Danger to Regime Security, Public Safety, and Societal Norms and Cohesion." *Journal of Cyber Policy* 4, no. 1 (2019): 22-34.

Pomerantsev, P. “Introduction”, in *Information at War: From China’s Three Warfares to NATO’s Narratives*. London: Legatum Institute. 2015a.

Pomerantsev, Peter. “Inside Putin’s Information War”. *Politico*. 4 January 2015b.

Pomerantsev, Peter. “The Kremlin’s Information War”. *Journal of Democracy*, Vol. 26. No. 4. October 2015c: 40-50.

“Today’s War is the Soft War”, editorial board, *Porseman Monthly*, Tehran, No. 83, 2010.

Prince, Brian. “Defense Department Confirms Critical Cyber-Attack”. *eWeek*. 25 August 2010.

Pu, Xiaoyu. “Controversial identity of a rising China.” *The Chinese Journal of International Politics* 10, no. 2 (2017): 131-149.

Pu, Xiaoyu. *Rebranding China: Contested status signaling in the changing global order*. Stanford University Press, 2019.

Qiang, Yang and Wang Chao. “The Fourth Revolution”, *UNESCO Courier*, July-September 2018, pp. 22-24.

Quinn, Tyler. “The Bear’s Side of the Story: Russian Political and Information Warfare”. *Real Clear Defense*. 27 June 2018.

Radin, Andrew, and Clint Reach. *Russian views of the international order*. RAND Corporation, 2017.

Ragulina, Julia V., Svetlana V. Lobova, and Alexander N. Alekseev. "Informatization of the Russian Society: Evaluation and Perspectives." In *International Conference Project “The future of the Global Financial System: Downfall of Harmony”*, pp. 341-347. Springer, Cham, 2018.

Rajan, D. S. “Making Sense of China’s New National Security Law”. South Asia Analysis Group. Paper 5972. 19 July 2015.

Ramicone, A., Williams, C., Gisser, S., Raynis, M., Ceballos, M.P., Saltzman, J., Kania, E., Betik, B., O’brien, M., Cooper, A. and others. ‘*National Security in Cooperation*’. (2014).

Rathinavel, Pavithra. “Apple iPhones And iPads Will Be Banned in Russia From New Year’s Day 2015”. *International Business Times*. 5 November 2014.

Ravich, Samantha, and Clifford D. May. “Discussion of Cyber Warfare in the Next Administration”. *Foundation for Defense of Democracies*. 18 November 2016.

Rawnsley, Gary D. “‘Thought-Work’ and Propaganda: Chinese Public Diplomacy and Public Relations After Tiananmen Square”. In Auerbach, Jonathan, and Russ Castronovo, eds. *The Oxford handbook of propaganda studies*. Oxford University Press, 2013: 147-162.

Rawnsley, Gary. “Why China’s Propagandists Love the Internet”. *Foreign Policy*. 21 July 2015.

Ripsman, Norrin M. “Neoclassical realism.” In *Oxford Research Encyclopedia of International Studies*. 2011.

Rogers, Mike. “Cyber Threats and Ongoing Efforts to Protect the Nation”, Open Hearing, the U.S. House, Permanent Select Committee on Intelligence, 4 October 2011.

Rogin, Josh. “NSA Chief: Cybercrime Constitutes the ‘Greatest Transfer of Wealth in History’”. *Foreign Policy*. 9 July 2012.

Rollins, John. “US-China Cyber Agreement”, *Congressional Research Service Insight*, 16 October 2016.

Rudolph, Jennifer. The China Questions: Critical Insights into a Rising Power. Harvard University Press, 2018.

Rudolph, Josh. “Minitrue: No News on U.S. Trade Dispute”, *China Digital Times*, 7 May 2019.

“MP urges ‘Nationalization’ of Google Over Security Fears”. *Russia Today*. 9 September 2014.

Rugge, Fabio. *Confronting an "axis of cyber"?: China, Iran, North Korea, Russia in Cyberspace*. Ledizioni-LediPublishing, 2018.

Sacks, Sam. “Beijing Wants to Re-Write the Rules of the Internet”, *The Atlantic*, 18 June 2018.

Sacks, Sam, Rogier Creemers, Lorand Laskai, Paul Triolo, and Graham Webster. “China’s Cybersecurity Reviews for ‘Critical’ Systems Add Focus on Supply Chain, Foreign Control [translation]”. *New America*. 24 May 2019.

Sabillon, Regner, Victor Cavaller, and Jeimy Cano. “National cyber security strategies: global trends in cyberspace.” *International Journal of Computer Science and Software Engineering* 5, no. 5, 2016.

Sadyki, Marina. “National report on e-commerce development in Russia”. Working Paper 13. United Nations Industrial Development Organization. Vienna, 2017.

Saakashvili, Eduard. “China & Russia: Two different approaches to ‘internet sovereignty’”. *Authoritarian Tech*. 28 November 2019.

Sadjadpour, Karim. “Ayatollah Machiavelli”. *Hoover Institution Essay on Middle East Strategy Challenges* (2017).

Sanovich, Sergey. “Russia: The Origins of Digital Misinformation.” *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media* (2018): 21-40.

Schweller, Randall L. “Rise of Great Powers: History and Theory.” In *Engaging China: The Management of an Emerging Power*, edited by Alastair Iain Johnston and Robert S. Ross. London: Routledge. 1999.

Schweller, Randall L. "Unanswered threats: A neoclassical realist theory of underbalancing." *International security* 29, no. 2 (2004): 159-201.

Schweller, Randall L. “Neoclassical realism and state mobilization: expansionist ideology in the age of mass politics.” *Neoclassical realism, the state, and foreign policy* (2009): 227-250.

Schweller, Randall L., and Xiaoyu Pu. “After unipolarity: China's visions of international order in an era of US decline.” *International security* 36, no. 1 (2011): 41-72.

Schatz, Daniel, Rabih Bashroush, and Julie Wall. “Towards a more representative definition of cyber security.” *Journal of Digital Forensics, Security and Law* 12, no. 2 (2017).

Schell, Oliver. “Chinese Influence and American Interests: Promoting Constructive Vigilance.” *YouTube: Hoover Institution*. 2019.

Schenkkan, Nate, and Sarah Repucci. "The Freedom House Survey for 2018: Democracy in Retreat." *Journal of Democracy* 30, no. 2 (2019): 100-114.

Schmidt, Michael S. and David E. Sanger. “5 in China Army Face U.S. Charges of Cyberattacks”, *The New York Time*, 19 May 2014.

Schreier, Fred, Barbara Weekes, and Theodor Winkler. “Cyber Security: The Road Ahead.” *The Geneva Centre for the Democratic Control of Armed Forces* (2015).

Segal, Adam. “Cyber Governance: The Next Step”. Council on Foreign Relations. 16 March 2011.

Segal, Adam. “How China Becomes a Cyber Power”, Council on Foreign Relations, 30 June 2014a.

Segal, Adam. “The Top Five Cyber Policy Developments of 2014: China’s Great Leap Forward”, *Council on Foreign Relations*, 29 December 2014b.

Segal, Adam. “China Hosts Its Own Cyber Conference”, *Council on Foreign Relations*, 21 October 2014c.

Segal, Adam. “China’s Internet Conference: Xi Jinping’s Message to Washington”, *Council on Foreign Relations*, 16 December 2015.

Segal, Adam. “How China is Preparing for Cyberwar”, Christian Science Monitor, March 20, 2017. Available online at: https://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0320/How-China-is-preparing-for-cyberwar.

Segal, Adam. "China, Encryption Policy, and International Influence." Hoover Institution, Beyond Privacy and Security series paper (2016).

Segal, Adam. “When China Rules the Web”, *Foreign Affairs*, Vol. 97, No. 5 (2018): 10-18.

Selyukh, Alina. “A Year After San Bernardino and Apple-FBI, Where Are We on Encryption?”. National Public Radio, 3 December 2016.

Shackelford, Scott J. *Managing cyber-attacks in international law, business, and relations: In search of cyber peace*. Cambridge University Press, 2014: 5.

Shahbaz, Adrian. “Freedom on the Net 2018: The Rise of Digital Authoritarianism”. *Freedom House*. 2019.

Shi, Zengzhi, and Guobin Yang. "New media empowerment and state-society relations in China." *The Internet, social media, and a changing China* (2016): 71-85.

Shi-Kupfer, Kristin, Mareike Ohlberg, Simon Lang, and Bertram Lang. “Ideas and Ideologies Competing for China’s Political Future.” *European Research Council. Mercator Institute for China Studies* 5 (2016): 12.

Shirk, Susan L. *China: fragile superpower*. Oxford University Press, 2007.

Shirk, Susan. “The domestic context of Chinese foreign security policies.” In *the Oxford Handbook of the International Relations of Asia*, pp. 391-410. Oxford: Oxford University Press, 2014.

“The Enemy’s ‘Roadmap’ and ‘Soft War’”. *Siasat-e Rooz*. 8 Jan 2012.

“For Those, Who Are at the Forefront of Soft War”. *Siasat-e Rooz*. 22 June 2013.

“The Evolution of Chinese Nationalism”, *Stratfor*, 4 October 2012.

Snyder, Jack. *Myths of empire: Domestic politics and international ambition*. Cornell University Press, 2013 (Kindle Edition).

Sreberny, Annabelle, and Gholam Khiabany. *Blogistan: The internet and politics in Iran*. Bloomsbury Publishing, 2010.

Staedter, Tracy. “Why Russia Is Building Its Own Internet”, *IEEE Spectrum*, 17 January 2018.

Shekhovtsov, Anton. "Aleksandr Dugin's Neo-Eurasianism: The New Right à la Russe 1." *Religion Compass* 3, no. 4 (2009): 697-716.

Schneider, Florian. "China’s ‘Big V’ bloggers: how celebrities intervene in digital Sino-Japanese relations." *Celebrity Studies*8, no. 2 (2017): 331-336.

Schreier et al 2015.

Soldatov, Andrei and Irina Borogan. “Russia’s approach to cyber: the best defense is a good offence”. In Nicu Popescu and Stanislav Secrieru (Eds.). *Hacks, Leaks and Disruptions: Russian Cyber Strategies*. Chaillot Papers. (Paris: European Union Institute for Security Studies). October 2018.

Stadnik, Ilona. “Sovereign RuNet: What Does it Mean?”. *Internet Governance Project*. Georgia Institute of Technology. 2019.

Sterling-Folker, Jennifer. "Neoclassical realism and identity: peril despite profit across the Taiwan Strait." *Neoclassical realism, the state, and foreign policy* (2009): 99-138.

Stockmann, Daniela, and Ting Luo. "Which social media facilitate online public opinion in China?." *Problems of Post-Communism* 64, no. 3-4 (2017): 189-202.

Sukhankin, Sergey. “Russia's New Information Security Doctrine: Fencing Russia from the "Outside World"?” Jamestown Foundation. 16 December 2016.

Suri, Jeremy. “American Pressure Against “Revisionist” Russia and China”, Italian Institute for International Political Studies, 21 December 2018.

Swaine, Michael D. “Chinese Views on Cybersecurity in Foreign Relations.” *China Leadership Monitor* 42 (2013): 1-27.

Tabora, Vince. “The Evolution of the Internet, From Decentralized to Centralized.” *Hackernoon*, 24 March 2018.

Talbot, Strobe. “It’s Already Collusion”. Politico Magazine. 13 January 2019.

“The Supreme Council of Cyberspace Defined the National Information Network and Formulated Its Requirements”. *Tasnim News*. 4 February 2014.

“There Is a Coup d’état Under Way in Persian Instagram Pages”. *Tavaana Tech*. 27 June 2020.

Tsebelis, George. *Nested games: Rational choice in comparative politics*. Vol. 18. Univ of California Press, 1990.

Thomas, Timothy L. "Nation-state cyber strategies: examples from China and Russia." *Cyberpower and national security*. 2009.

Thomas, Timothy. “Psycho Viruses and Reflexive Control”, in *Information at War: From China’s Three Warfares to NATO’s Narratives*. London: Legatum Institute. 2015.

Tiezzi, Shannon. “The ‘China Can Say No’ Effect”, *The Diplomat*, 07 August 2014.

Tikk, Eneken, Kadri Kaska, and Liis Vihul. *International cyber incidents: Legal considerations*. Cooperative Cyber Defence Centre of Excellence (CCD COE), 2010.

Tikk, Eneken. “Ten rules for cyber security.” *Survival* 53, no. 3 (2011): 119-132.

Timmons, Heather. “Facebook Is Making Employees Read Chinese Propaganda to Impress Beijing”, *Quartz*, 8 December 2014.

Trubetzkoy, N. S. “The legacy of Genghis Khan: a perspective on Russian history not from the west but from the east.” *The legacy of Genghis Khan and other essays on Russia’s identity* (1991).

Tsonchev, T. S. “The Kremlin’s New Ideology”. *The Montréal Review*. January 2017.

Van Dijck, José. *The culture of connectivity: A critical history of social media*. Oxford University Press, 2013.

Van Herpen, Marcel H. *Putin's wars: the rise of Russia's new imperialism*. Rowman & Littlefield, 2015.

Vavra, Shannon. “The U.N. passed a resolution that gives Russia greater influence over internet norms”. *Cyberscoop*. 18 November 2019.

Wan, Adrian. “Chinese Academy of Social Sciences is 'infiltrated by foreign forces': anti-graft official”, South China Morning Post, June 15, 2014.

“America Should Not Shrug at Its Cyber Vulnerability”. *Washington Post*. 19 September 2014.

Weber, Valentine. “The Sinicization of Russia’s Cyber Sovereignty Model”. *Council on Foreign Relations*. 1 April 2020.

Wei, Yushi. “Chinese Data Localization Law: Comprehensive but Ambiguous”. The Henry M. Jackson School of International Studies. University of Washington. 7 February 2018.

Wei, Yuxi. “China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty”, Cybersecurity Initiative Highlights, 21 June 2016; Bennett, Cory. “Russia, China Unite with Major Pact”, The Hill, 8 May 2015.

Wei, Yuxi. “Chinese Data Localization Law: Comprehensive but Ambiguous”. *Newsletter*. University of Washington. 7 February 2018.

West, Darrell M. “Internet shutdowns cost countries $2.4 billion last year.” *Center for Technological Innovation at Brookings, Washington, DC* (2016).

“China Decides It’s Internet Crazy”, *Wired,* 21 August 2000.

Wohlforth, William C. “Unipolarity, status competition, and great power war.” *World politics* 61, no. 1 (2009): 28-57.

Wolfers, Arnold. *Discord and collaboration: essays on international politics*. Johns Hopkins University Press, 1965.

Wu, Wendy. “US and allies urged to increase digital investments in Asia to counter China’s belt and road tech projects”, *South China Morning Post*, 7 February 2019.

Wu, Xu. *Chinese cyber nationalism: Evolution, characteristics, and implications*. Lexington Books, 2007.

“Xi outlines blueprint to develop China's strength in cyberspace”, *Xinhua Headlines*, 21 April 2018.

Xuetong, Yan. Leadership and the Rise of Great Powers. Princeton University Press. 2011.

Yahyanejad, Mehdi. “The effectiveness of Internet for informing and mobilizing during the post-election events in Iran.” *Liberation Technology in Authoritarian Regimes* (2010).

Yaling, Pan. “The ‘Two Americas’ Dichotomy: Online Chinese Nationalism Towards the United States”. In Simon Shen and Shaun Breslin (Eds) *Online Chinese nationalism and China's bilateral relations*. Lexington Books, 2010.

Yan, Xiaojun, and Jie Huang. “Navigating unknown waters: The Chinese Communist Party's new presence in the private sector.” *The China Review* (2017): 37-63.

Yang, Yifan. “The Internet and China’s Foreign Policy Decision-making.” *Chinese Political Science Review* 1, no. 2 (2016): 353-372.

Yi, Shen. “New Challenges for China and the U.S. in a Networked World: Governing Global Cyberspace”, *China US Focus*, 28 June 2011.

Yukai, Wang. “Establishing a safe, orderly and cooperative Internet governance system”, CPS News, 2015.

Zakrzewski, Cat. “The Cybersecurity 202: Trump Set to Make a New DHS Agency the Top Federal Cyber Cop”, *The Washington Post*, 16 November 2018.

Zuckerberg, Mark. “The Internet Needs New Rules. Let’s Start in These Four Areas”. *The Washington Post*. 30 March 2019.

Zuo, Mandy. “China aims to become internet superpower by 2050”. *South China Morning Post*. 28 July 2016.