Nation-State Perspectives on Information Operations and the Impact on Relative Advantage

Brenna Cole, George Noel
Air Force Institute of Technology, WPAFB, USA
Brenna.cole@afit.edu
George.noel@afit.edu

Abstract: The United States government recognizes near-peer adversaries, specifically Russia and China, as the greatest threats to national security. A military encounter between the U.S. and Russia or China is unlikely to resemble past conflicts. Russia and China have recognized the power of cyber and information warfare capabilities and will leverage them heavily in battle. In fact, the U.S., China, and Russia continue to leverage these capabilities in a persistent, low-intensity conflict happening each day. This paper presents an understanding of what future, information-centric warfare might look like and suggests ways in which countries need to modify their perspectives towards information warfare to be successful. It does this by elaborating on Russia and China's perspectives towards information warfare, examining each country's cyber force structures, and studying past examples of how ~~such~~ information ~~operations~~ campaigns have been used to further national goals. It then compares those perspectives to that of the United States and analyzes how this impacts relative advantage on the battlefield. In order to maintain military advantage or even ensure capabilities remain on-par with near-peer adversaries, the United States must find ways to counter the information operation attacks conducted by Russia and China and to employ cyberspace operations as a primary objective rather than limiting it to a supporting role.

Keywords: Information Operations, Information Warfare, Cyber, Cyberspace Operations, Nation-States

1. Introduction

The defense of a country's people and values ~~One purpose of warfare is to ensure national safety by defending a country's people and values. To do so~~ requires a focused effort to identify, deter, and defeat threats to national security. This effort must ~~identify~~recognize where the ~~the~~ current, emerging, and future threats will come from and what shape they will carry. In the United States' National Defense Strategy, U.S. military leaders recognized the long-term strategic competitions with China and Russia as the primary threats to its ~~people's~~ security and prosperity (Mattis 2018). As such, the U.S. must be prepared to fight and win in a war with one or both of these nations. That preparation ~~requires~~necessitates an understanding of the ways in which Russia and China will fight. ~~foresight as to how a war with these countries would look.~~ For both ~~Russia and China,~~countries, warfare will significantly rely on cyber and information operations (Hans, 2018~~), (~~; Kolton 2017). Russia views these methods as a means to shape the strategic environment, disguise aggressive actions, degrade and disrupt enemy actions, and be a first-strike option in the advent of conflict (Bernstein and Ball, 2015; Zwack and Marie-Charlotte, 2019). China views informationized warfare as the key to military success. Their usage of "informationization" i~~, to i~~ncludes maintaining dominance in the information domain and crippling the enemy by exploiting reliance on information systems (Costello and McReynolds, 2018). C~~hina perceives c~~yber operations are perceived as a way to project power to protect national interests, maintain internal stability, and influence opinions (Clarke, 2019~~), (~~; Kolton 2017). For both Russia and China, the cyber domain is of central importance to military strategy. ~~They view cyber~~It is seen as a force multiplier—a mechanism to level the playing field when outmatched in other domains (Zwack and Marie-Charlotte, 2019; Costello and McReynolds, 2018). Therefore, they will extensively employ cyber capabilities to heighten and achieve a military advantage. Should the United States or other competing nations fail to adapt their cyber warfare strategies to counter these threats ~~effectively~~, they will lose ~~advantage~~ influence within the cyber domain. ~~Losing the advantage~~This could have devastating consequences in a future conflict, and therefore ~~jeopardizing~~ jeopardize national security. To ensure military advantage, the United States and its allies need to understand how Russia and China will employ cyber operations to win a global competition and modify their information warfare strategies to be capable of deterring and countering cyber threats.

The remainder of this paper is organized as follows. Section 2 describes the Russian view of information ~~operations~~warfare, to include how it relates to their national objectives, ~~their~~ the Russian cyber force organizational structure, and ~~past~~ examples of past information operations. Section 3 describes the Chinese view of information operations, again by explaining their perception of information warfare, their organizational structure, and historical usage. Section 4 presents how the United States' employment of information operations differs from that of China or Russia. Finally, Section 5 offers strategy considerations for gaining a strategic advantage within the information environment.

2. Russian ~~information~~ Information W~~w~~arfare

2.1 Russian perspective

Russia perceives the United States and the North Atlantic Treaty Organization (NATO) as existential threats to its existence (Zwack and Marie-Charlotte, 2019). It views western nations as actively trying to displace the regime and disarm its military capability (Costello and McReynolds, 2018). In response to this danger, real or perceived, Russia has exerted itself more aggressively across the globe (Zwack and Marie-Charlotte, 2019). Power projection and global influence are means for Russia to elevate itself to a world power and discourage threats to its survival.

Russia's quest to achieve global influence rests heavily on the use of information operations. This spans a wide set of options~~margin~~, ranging from strategic deception and information manipulation to hybrid warfare and offensive attacks (Krinstiina, 2016; Zwack and Marie-Charlotte, 2019).

One of the primary ways Russia uses cyber and information operations is to shape the geopolitical environment by manipulating public opinion, both across the globe and within its borders (Hans, 2018~~), (~~; ICA, 2017). Russia uses information campaigns to destabilize democracies and incite domestic chaos in the nations it views as opponents (Hans, 2018). Russia ~~views~~ uses ~~the~~ information shaping conducted in peacetime as a method to deter aggression and erode adversary readiness~~, thereby reducing the likelihood of direct conflict or weakening the adversary's capabilities should one arise~~ (Zwack and Marie-Charlotte, 2019). In addition to manipulating foreign perceptions, Russia uses information operations to influence its own populace by spreading anti-West sentiment across the nation (Kostyuk, Powell, and Skach 2018). This is a way to ~~By uniting its citizens against the external threat, Russia attempts to~~ temper domestic unrest by ~~focusing~~ uniting its citizens against a common enemy (Costello and McReynolds, 2018).

Another way Russia ~~views~~ perceives cyber and information operations is as a way to conduct aggressive actions under a veil of deception and shadow (Hans, 2018). The concept of *maskirovka*, or military deception, is a fundamental part of Russian thinking (Zwack and Marie-Charlotte, 2019). Cyber operations ~~tend to be~~are conducted with less visibility than kinetic operations, can be difficult to attribute, and are employed not only within the boundaries of a military engagement, but across all of society. This is because the battlefield is primarily logical and has unclear borders between military forces and civilians. Russia leverages these features of cyberspace to conduct actions within a "gray zone," where their actions fall short of inciting conflict yet still degrade adversary military capabilities (Bernstein and Ball, 2015; Zwack and Marie-Charlotte, 2019).

Thirdly, Russia views information warfare as a new and transformational method of waging war ~~and prevailing~~to prevail in conflict (Hans, 2018). Russia's political and military strategy will use hybrid warfare by emphasizing non-traditional weapons of power, such as cyber, information, and psychological effects (Krinstiina, 2016). Kinetic forces will still be employed, but not as the primary tool relied upon for success. Instead, they will be used alongside asymmetric warfare operations, as well as ~~or~~ to protect information security and the cyber domain (Hans, 2018; Kostyuk, Powell, and Skach 2018). Cyber operations will be used as a combination of indirectly shaping adversary decisions and directly delivering effects to destroy or degrade a target (Zwack and Marie-Charlotte, 2019).

2.2 Organization

Russian information operations are executed by both government and non-government entities (Connell and Vogler, 2017). Within the government, major players are the Federal Security Service (FSB), the Foreign Intelligence Service (SVR), and the Ministry of Defense (MOD) (Connell and Vogler, 2017). Another information-related organization is the Federal Service for Supervision in the Sphere of Telecommunications, Information Technologies, and Mass Communications (Roskomnadzor), responsible for media regulation (Connell and Vogler, 2017). By regulating what ideas are presented in the media, this organization influences domestic opinion in favor of national goals.

An important element of Russian information warfare is that many of the attacks are conducted by organizations not directly affiliated with the Russian government but believed to be sponsored by it (Zwack and Marie-Charlotte, 2019). Adding to the deception of cyber warfare, Russia denies the awareness or support of these groups. However, the actions conducted by them match Russian objectives well (Connell and Vogler,

2017). Russia is believed to work with criminal networks, such as the Russian Business Network (RBN), ~~(Connell and Vogler, 2017)~~and commercial companies such as media outlets~~, among others~~ (Connell and Vogler, 2017; Krinstiina, 2016). Partnership with these companies allows the government to exert greater control over the narrative and ideas presented to its populace.

2.3 Examples

Many examples could be used to demonstrate Russian use of cyber operations. Below are two selected to show how Russia uses information operations to shape the strategic environment and to assist in military conflict.

A well-publicized example of Russia using information operations to influence the geopolitical environment is the Russian election meddling in the 2016 United States presidential election. In the unclassified report on these activities, the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), and the National Security Agency (~~–~~NSA) assessed "with high confidence that Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election, the consistent goals of which were to undermine public faith in the U.S. democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency" (ICA, 2017). Regardless of whether President Trump would have been elected without the Russian interference, this act demonstrated the disruptive effect information operations could create. This is evidenced by the consistent media attention on the possibility of a Russian influence campaign and the public outcry of the invasion into the American democratic process. As stated earlier, one of the goals of using information operations to shape the strategic environment is to cause chaos and uncertainty, thereby weakening the united strength of a democracy (Hans, 2018). As President Lincoln famously stated, "A house divided against itself, cannot stand." By generating domestic turmoil, Russia has at the least caused internal conflict within the U.S., which stole attention that could have been focused on other international issues.

An example of Russian information operations employed during military conflict can be seen from the conflict in Ukraine. Russia has been in conflict with Ukraine since 2013, with particularly strained relations since Russia annexed Crimea in 2014 (Zwack and Marie-Charlotte, 2019; Connell and Vogler, 2017). Russia has used information operations of various types throughout the entirety of this conflict. One type ~~involved~~ had similar intent ~~to~~ as that in the U.S. election meddling – to destabilize public support by creating an air of confusion and mistrust (Krinstiina, 2016). For example, Russia used media in Ukraine and Russia to negatively portray Ukrainian soldiers and criticize the Ukrainian government (Krinstiina, 2016). However, in this case, the use of information operations did not stop at causing chaos. Escalating from creating an atmosphere of confusion, pro-Russian groups ~~have~~ caused soldiers to mistrust their information systems and data via cyber attacks (Connell and Vogler, 2017). Escalating even further, a presumed Russian or Russian-sponsored group known as Sandworm conducted a cyber-attack directed at the Ukrainian power grid (Kostyuk, Powell, and Skach 2018~~), (~~; FireEye, 2016). The attack resulted in the western part of the country losing power for several hours (Kostyuk, Powell, and Skach 2018). These information operation activities provide a real-world example of how Russia will use cyber and information effects in a declared conflict.

3. Chinese Information Warfare

3.1 Chinese p~~P~~erspective

Globalization has forced China to confront a world order that challenges its traditional governance and regime (Waldron, 2019). China is a leader in the international system but did not become one until more than a century of lagging behind further developed nations (Kissinger, 2011). These years of "suffering" are a lesson and motivator for China to gain and maintain a position of strength (Kolton 2017; Kissinger, 2011). Once it entered the international arena, China emerged as a world power, primarily due to its economic influence (Waldron, 2019). Economic prowess alone, however, is not enough to preserve China's global standing. To protect its national sovereignty, regime stability, and regional dominance, China looks to expand its influence to other areas. A primary way China has been doing this is by modernizing and expanding its military to gain strategic influence and be prepared for future conflict (Kania and Costello, 2018; Domingo, 2016).

China views "informationized" warfare as the key to military success and national security (Kolton, 2017). This emphasis on information warfare stems from the study of previous conflicts and factors that led to the victor's success (Clarke, 2019). The start of this realization was in 1991 with the Persian Gulf War, where China concluded that an advantage in information technology could lead to overwhelming military advantage.

Additionally, China observed ~~and~~ that an opponent's dependency on ~~such~~ information systems was a vulnerability that could be exploited (Costello and McReynolds, 2018). In this conflict and others since then, China has observed how technological strength contributes to military success. ~~Additionally,~~ In addition to military support, China views information and technology as a way to maintain internal stability. It ~~sees~~ is perceived ~~it~~ as a method to ~~achieving~~ achieve and ~~maintaining~~ protect domestic and regional sovereignty. It, therefore, uses information superiority to project power, strengthen military capabilities, and maintain domestic control (Clarke, 2019).

3.2 Organization

The emphasis China puts on information ~~technologies~~ technology is apparent in its military ~~organizational~~ force structure. In late 2015, the Chinese military underwent extensive reforms to restructure the People's Liberation Army (PLA). One of the significant changes was the creation of the Strategic Support Force (SSF), which was a new branch on the same level as the Army, Navy, Air Force, or Rocket Force (Kolton 2017; South China Morning Post, 2016).

The SSF consists of space, cyber, electronic, and psychological warfare units (Costello and McReynolds, 2018). These are the areas that China deems critical for future warfare, the "strategic frontiers" which it must dominate to achieve military superiority (Kania and Costello, 2018). The SSF is divided into two departments – the Space Systems Department and the Network Systems Department (Kania and Costello, 2018). The Network Systems Department (NSD) consists of cyber warfare, electronic warfare, psychological warfare, and technical reconnaissance units. The grouping of these functions demonstrates how the PLA ~~sees~~ percieves network operations as spanning ~~the range of~~ the information spectrum ~~and~~ to allow~~s~~ for an inherently integrated approach to information warfare (Costello and McReynolds, 2018).

In addition to creating the SSF and NSD, the 2015 reforms created the Political Work Department, which controls the TV and radios. Like Russia, China exerts influence on media and social platforms, thereby controlling what ideas are presented to the public. This allows the government to control the image received by its citizens, and, to some extent, the ~~what narrative its citizens, and to some extent, the~~ international audience ~~, perceive~~ (Posard et al., 2020).

3.3 Examples

Unlike Russia, there have not been observed Chinese-backed cyber-attacks during conflict. Chinese cyber activities have stayed in the pre-conflict realm. In that realm, however, China has been notably active. The examples below show two areas that China has demonstrated the use of cyber capabilities: expanding military strength via cyber espionage and exerting domestic influence in support of regime control.

Industrial and economic espionage attributed to China shows how China uses the information environment to gain a strategic advantage~~.~~ (Oxnevad, 2019). ~~This i~~Information theft provides a means for China to improve military capabilities, increase commercial advantage, and expand international influence (Kania and Costello, 2018; Oxnevad, 2019). China has been accused of targeting a wide gambit of technological information, to include space, energy, nuclear power, information technology, military technology, and biotechnology (Gilli and Gilli, 2019; Iasiello, 2016). One specific example is the use of~~using~~ a mixture of traditional espionage and cyber espionage techniques to gain technical information on military aircraft (Gilli and Gilli, 2019).

Another ~~aspect~~ example of China's power projection strategy is ~~using~~ the use of information to influence foreign and domestic opinions (Clarke, 2019). Internal control, in particular, is of great ~~concern~~ importance to China because ~~maintaining~~ domestic order is viewed as critical to regime survival (Waldron, 2019). Exposing citizens to "dangerous" Western ideas ~~could~~ is feared to incite rebellion and threaten the government's power (Kostyuk, Powell, and Skach 2018). China seeks control of the cyber domain so that it can regulate ~~what~~ the information ~~is~~ exposed to its citizens, in order to stop potential internal threats (Kostyuk, Powell, and Skach 2018). ~~It~~ China uses censorship, propaganda, and media sites to shape ~~what~~ the messaging ~~is~~ received by the populace. Additionally, while not to the same scale as Russian external influence operations, China attempts to influence international perception via social media influence or propaganda (Posard et. Al., 2020).

4. United States Information Warfare

To better understand the Russian and Chinese perspectives of information operations, they can be compared to a Western perspective, such as that of the United States. Like Russia and China, the United States relies

heavily on cyber and information operations. How it relies on ~~information~~ these technologies, however, differs in ~~some~~ key areas.

One way that ~~the~~ United States information operations differs from that of Russia and China is that the ~~United States has a greater~~ distinction between government and civilian ~~stakeholders~~organizations within the cyber domain. Commercial companies are autonomous and can choose whether ~~or not~~ their actions support the United States or adhere to the government-recommended cybersecurity postures. The separation between government and commercial entities is a foundational element of American democracy; yet, it presents an additional challenge as adversarial cyber activities do not respect such bounds. They can therefore ~~and~~ pose a threat to the American people by targeting civilian institutions. Furthermore, this separation limits the extent to which the military and government can defend commercial organizations from cyber attacks, reducing their role to primarily providing threat information, recommendations, or stopping the threat before it reaches U.S. targets.

Another way in which the United States differs from Russia and China is that the United States is supportive of free and open internet (Kolton, 2017). Freedom of speech is a fundamental right in the American constitution. While there are laws that criminalize certain actions on the internet, these laws are designed to safeguard against harm to individuals, not to censor ideas. Unlike competitor nations, the United States will not determine the information to which its citizens are exposed. Additionally, the U.S. is cognizant that the use of influence operations via regulating the information people are exposed to could result in the erosion of ~~can erode~~ trust in the government. Rather than garnering public support via information manipulation, the U.S. seeks to gain trust through transparency of ~~it as a result of its~~ actions.

A third way in which the United States differs from competitor states is how it views the role of cyber operations. U.S. leadership has repeatedly declared the importance of cyberspace and the need to defend against the threat presented to the nation. However, it still organizes cyber forces within traditional service branches. While cyber is embedded within air, land, sea, or space forces, it will continue to be a secondary consideration to the primary mission~~,~~. Viewing cyber from only ~~this~~ traditional perspectives limits its potential. Competing nations view cyber as a distinct asymmetric capability that brings new and unique elements to strategic influence and warfare (Swack and Marie-Charlotte, 2019; Costello and McReynolds, 2018). This means that they will ~~look~~ not look at cyber as simply ~~a~~ support to traditional methods, but as a primary domain from which to obtain their goals. To counter these new elements, the U.S. needs to create organizational environments that foster looking at problems from a cyber mindset.

5. Strategy Considerations

As the world pivots to an interconnected, data-based model, cyber and information operations will play an even more critical role in strategic advantage. Global leaders trumpet the necessity of cyber dominance and the vital part it will play in conflict. However, despite the public acknowledgment, there is still much to be ~~much~~ done ~~to~~ in order to prepare to fight and win in the competition for cyber and information dominance. How to ~~gain~~ achieve such~~cyber~~ dominance is a profoundly complex problem and will not be solved in the span of this paper. This paper will, however, propose three changes that would better posture nations for a position of advantage.

5.1 Increase mutual understanding of information operation triggers and consequences

As each nation-state views cyber and information operations through a unique lens, each will interpret adversary actions differently. This is especially true due to the ambiguity ~~and newness~~ of information operations conducted via cyberspace. A lack of ~~an identifiable~~ clear thresholds of war within this domain could yield misunderstandings that are interpreted as an escalation of conflict when only meant as a continuance of peacetime activities (Domingo, 2016). Russia may view an action as a peacetime operation, but the United States may interpret it as warfare (Connell and Vogler, 2017). Similarly, Russia or China may interpret ~~what~~ an action that the U.S. considers a minor operation as a threat to their tightly-controlled information spaces. This could result in quicker escalation that what ~~and escalate quicker than~~ the U.S. foresaw (Kostyuk, Powell, and Skach, 2018). Open dialogue~~s~~ between these countries about the types of activities that will result in escalation will give the competing ~~country~~ countries an understanding of the actions it can and cannot take ~~without~~ suffering consequences. The goal of this communication is to ensure that if a line is crossed, it is intentional. ~~escalating conflict, which is in all nations' best interests.~~

This is a crucial component in establishing an effective deterrence strategy. Deterrence requires knowing the consequences of specific actions and the belief that such actions will occur. Such mutual understanding does not currently exist for information warfare (Kolton, 2017). To generate an effective deterrence strategy against Russia or China, other nations must first understand what these countries view as the worst possible outcomes, then communicate ~~what~~ which actions will result in such consequences.

5.2 Establish a whole-of-society approach to information dominance

Unlike traditional warfare, ~~where~~ in which attacks are limited primarily to military forces or directly supporting elements, information warfare operations target people, data, and systems regardless of the civilian or military status. According to Russian military strategy, the first step towards warfare is to influence the public (Klein, 2018). Similarly, using information operations to influence public domestic and international opinion is a key element of China's "Three Warfares" strategy (Clarke, 2019). Influence operations on the public will affect military advantage and international standing—nations need a way to defend against it.

An effective defense from adversary disinformation campaigns requires a whole-of-society approach across military, government, and commercial organizations. Each element has different roles in this effort. Among the various roles are informing the public of adversary actions in the information sphere, establishing, publicizing, and protecting a source that people can trust for information, and establishing deterrence to prevent adversarial actions. Additionally, once adversary actions have been identified, parties across the board need to take an active role in securing against adversary actions and limiting the impact. To establish this cooperation, nations will have to heighten cooperation and communication between existing government entities and form cooperative and trust-based relationships with commercial organizations so that they freely and willingly choose to help protect citizens from information attacks. There will have to be clear communication on what the threat is, what is expected of each organization, and how they can work together to defend against it. The U.S. has taken steps towards this by outlining plans in the DoD Cyberstrategy to disseminate threat information to the private sector and establishing communication agreements between different government agencies to collaborate on planning and response to a cyber attack (Rockwell, 2020).

5.3 Organize cyber forces to capitalize on information operation potential

Russia and China look at cyber and information operations as a unique domain that brings new ideas and capabilities ~~into~~ to warfare. To compete in the information environment, other nations need to do the same. This means recruiting the right people to be cyber warriors or information operation planners, generating unique ways to conduct cyber warfare, and effectively training and resourcing cyber units. Planning and executing successful joint operations require personnel who consider problems from distinct viewpoints, then combine those viewpoints to establish a stronger solution. While cyber is embedded in the traditional branches, there is not a focus ~~will not be~~ on how cyber can solve the problem; rather, the focus will be on how can cyber augment the land, sea, or air assets to ~~solve the problem~~do so. To capitalize on what cyber can bring to the fight, the military needs members that look at ~~each~~ problems through a uniquely cyber ~~viewpoint~~mindset. They can ~~join discussconversebrainstormconsolidate~~then work with their joint brethren to ~~advocate~~ promote new cyber-focused possibilities that were not previously considered so that the best multidomain solutions can be generated. ~~for~~ This ~~is what~~ will allow nations to achieve ~~power~~ advantage in the cyber domain as well as ~~the~~ traditional domains, thereby strengthening their standing in the great power competition.

One way this could be achieved is through the creation of a distinct cyber branch. It would encourage processes and policies that facilitate innovation, talent, and growth in the information environment. Current recruitment strategies are directed at gaining personnel that are well-suited to be a soldier, sailor, airman, or marine. As the skillsets to be a good cyber warrior or planner are different than skillsets for traditional roles, the recruitment strategy should be different as well. A separate branch would allow for that. Furthermore, it could establish a culture that is able to foster and retain these personnel to provide the needed cyber perspective when conducting joint operations.

6. Conclusion

Achieving a position of power within the information environment is crucial to securing strategic and military advantage. To reach such a position, nations must understand the threat that competing countries pose ~~in information operations~~ and adapt their strategies to overpower that threat. This entails understanding how ~~competing~~ adversarial nations view information operations, what actions they intend to conduct within

cyberspace, and the goals that they are trying to achieve. Furthermore, after better understanding how adversary nations intend to employ information operations, the U.S. and allies need to take preventative measures to detect and counter malicious actions within this realm. This includes establishing a united goal between government and civilian entities to defeat adversarial action, communicating what is perceived as a threat and what type of consequences will occur, and posturing military forces for success. ~~is important for preventing the unnecessary escalation of conflict.~~ Creating a national strategy with these considerations in mind will benefit the United States and allies in achieving ~~enable a country to establish~~ relative advantage within the information sphere.

References

Bernstein, P. and Ball, D. (2015) "Putin's Russia and U.S. Defense Strategy," National Defense University, Washington D.C, Aug. 19. [online], inss.ndu.edu/Portals/82/Documents/conference-reports/Putins-Russia-and-U.S.-Defense-Strategy.pdf.

Clarke, M. (2019) "China's Application of the 'Three Warfares' in the South China Sea and Xinjiang", *Orbis*, Vol 63, No. 2, April, pp 187-208, [online], doi:10.1016/j.orbis.2019.02.007.

Connell, M. and Vogler, S. (2017) "Russia's Approach to Cyber Warfare", Center for Naval Analyses Arlington United States, No. DOP-2016-U-014231-1Rev. [online], https://apps.dtic.mil/dtic/tr/fulltext/u2/1032208.pdf.

Costello, J. and McReynolds, J. (2018) *China's Strategic Support Force: A Force for a New Era*. Washington, DC: National Defense University Press.

Domingo, F. (2016) "Conquering a new domain: Explaining great power competition in cyberspace," *Comparative Strategy*, Vol 35, No. 2, pp 154–168, July. [online], https://doi-org.afit.idm.oclc.org/10.1080/01495933.2016.1176467.

Gilli, A. and Gilli, M. (2019) "Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage", International *Security*, Vol 43, No. 3, pp 141-189.

Hans K. (2018) "Information Warfare and Information Operations: Russian and U.S.. Perspectives", *Journal of International Affairs*, Vol 71, January, pp 135–142. [online], EBSCOhost, search.ebscohost.com/login.aspx?direct=true&db=bth&AN=132491879&site=eds-live.

Hultquist, J. (2016) "Sandworm Team and the Ukrainian Power Authority Attacks," FireEye. [online], https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html.

Iasiello, E. (2016) "China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities," *Journal of Strategic Security*, Vol 9. [online], http://dx.doi.org.afit.idm.oclc.org/10.5038/1944-0472.9.2.1489.

ICA. (2017) *Assessing Russian Activities and Intentions in Recent U.S. Elections 2017-01D*. Technical report, Office of the Director of National Intelligence. [online], https://www. dni. gov/files/documents/ICA_2017_01. Pdf.

Kania, E. and Costello, J. (2018) "The Strategic Support Force and the Future of Chinese Information Operations," *The Cyber Defense Review*, Vol 3, No. 1, pp 105-122. [online], https://www.jstor.org/stable/10.2307/26427379.

Kissinger, H. (2011) *On China*. Penguin Books Limited.

Kolton, M. (2017) "Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence" *The Cyber Defense Review*, Vol 2, No. 1, pp 119–154. [online], www.jstor.org/stable/26267405.

Kostyuk, N., Powell, S. and Skach, M. (2018). "Determinants of the Cyber Escalation Ladder", *The Cyber Defense Review*, Vo. 3, No. 1, pp 123–134. [online], www.jstor.org/stable/26427380.

Kristiina, M.A., et al. (2016) "Russian Information Operations against the Ukrainian State and Defence Forces: April-December 2014 in Online News", *Journal on Baltic Security*, Vol 2, No. 1, January, pp 28-71. [online], doi:10.1515/jobs-2016-0029.

Mattis, J. (2018) Summary of the National Defense Strategy of the United States of America: Sharpening the Military's Competitive Edge. Washington DC: Department of Defense. [online], https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf?source=GovDelivery.

Oxnevad, I. (2019) "Corporate Privateering and Economic Counter-Espionage in U.S. Great Power Competition," *Orbis*, Vol 63, No. 3, pp 391-405. [online], https://doi.org/10.1016/j.orbis.2019.05.006.

Posard, M. et al. (2020) "From Consensus to Conflict, Understanding Foreign Measures Targeting U.S. Elections", *RAND Coorperation.* [online], https://www.rand.org/pubs/research_reports/RRA704-1.html?utm_source=WhatCountsEmail&utm_medium=RAND%20Policy%20Currents+AEM:%20%20Email%20Address%20NOT%20LIKE%20DOTMIL&utm_campaign=AEM:631600804

Rockwell, M. (2020). *Three agencies team on cyber defense of energy infrastructure.* FCW.

Waldron, A. (2019) “Reflections on China’s Need for a ‘Chinese World Order,’” *Orbis*, Vol 63, No. 1, pp 3–10, January. [online], https://doi.org/10.1016/j.orbis.2018.12.006
Zhen, L. (2016) “Chinese military launches two new wings for space and cyber age,” *South China Morning Post*, 1 January. [online], https://www.scmp.com/news/china/diplomacy-defence/article/1897356/chinese-military-launches-two-new-wings-space-and-cyber
Zwack, P. and Marie-Charlotte, P. (2019*) Russian Challenges from Now Into the Next Generation: A Geostrategic Primer*. National Defense University Press.