NEW AMERICA

FIU FLORIDA INTERNATIONAL UNIVERSITY

July 2019

Are China and Russia on the Cyber Offensive in Latin America and the Caribbean?

A Review of Their Cyber Capabilities and Implications for the U.S. and its Partners in the Region

Robert Morgus, Brian Fonseca, Kieran Green, & Alexander Crowther

Last edited on July 26, 2019 at 9:20 a.m. EDT

newamerica.org/cybersecurity-initiative/reports/russia-china-cyber-offensive-latam-caribbean/

Acknowledgments

This paper was produced as part of the Florida International University - New America Cybersecurity Capacity Building Partnership (C2B Partnership) and is part of the Florida International University—United States Southern Command Academic Partnership. United States Southern Command provides funding to support this series as part of its academic outreach efforts. Academic outreach is intended to support United States Southern Command with new ideas, outside perspectives, and spark candid discussions. The views expressed in this findings report are those of the authors and do not necessarily reflect the official policy or position of the United States Government, United States Southern Command, Florida International University, or any other affiliated institutions.

About the Author(s)

Robert Morgus is a senior policy analyst with New America's Cybersecurity Initiative and International Security program and the deputy director of the FIU-New America C2B Partnership.

Brian Fonseca is a fellow in New America's Cybersecurity Initiative. He is director of the Jack D. Gordon Institute for Public Policy at Florida International University's (FIU) Steven J. Green School of International and Public Affairs.

Kieran Green is a China analyst at SOS International.

Alexander Crowther, Ph.D., is a Cyber Policy Specialist at the Center for Technology and National Security Policy at National Defense University.

About New America

We are dedicated to renewing America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Cybersecurity Initiative

The goal of New America's Cybersecurity Initiative is to bring the key attributes of New America's ethos to the cybersecurity policy conversation. In doing so, the Initiative provides a look at issues from fresh perspectives, an emphasis on cross-disciplinary collaboration, a commitment to quality research and events, and dedication to diversity in all its guises. The Initiative seeks to address issues others can't or don't and create impact at scale.

About FIU-New America C2B Partnership

The Cybersecurity Capacity Building (C2B) Partnership is a partnership between Florida International University and New America designed to develop knowledge and policies aimed at building the cybersecurity capacity in the workforce, at the state and local level, within the U.S. government and industry, and internationally.

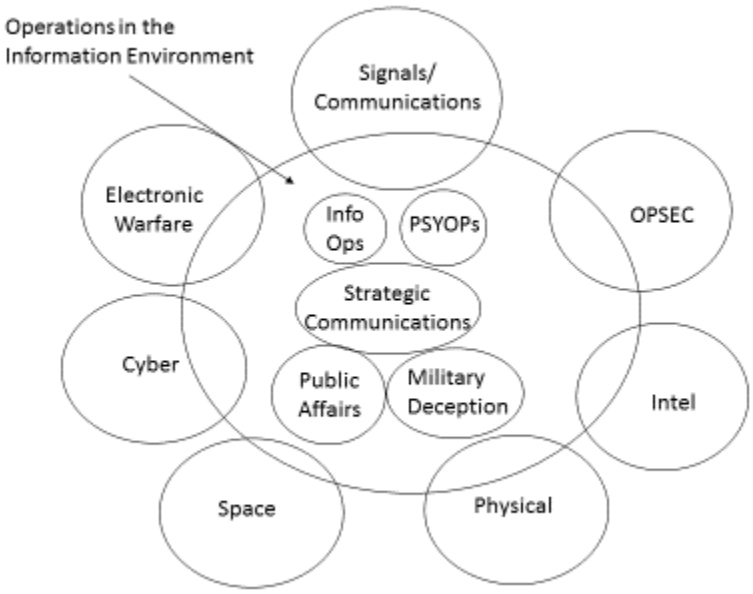
Contents

Introduction

Cyberspace—the newest domain of conflict—is among the most prominent forums of conflict in the twenty-first century. Increasingly nation-states utilize cyber and information capability in pursuit of foreign policy and national security objectives. This report focuses on two nation-states that are leading the charge in this respect: China and Russia.

While Russia seeks to destabilize the global system for its own advantage, China's goal is to maintain the current system and replace the United States as the global hegemon. To that end, China and Russia are pursuing robust cyber capabilities to advance their respective geopolitical, economic, and security interests. Moreover, Chinese and Russian state-run enterprises use tools ranging from cyber espionage to weaponizing information in an effort to undermine the efficacy of democracy and, in general, western interests around the world.

Figure 1: U.S. Military Approach to Information[1]



In this report, we offer an overview of Chinese and Russian cyber capabilities. We interpret these broadly to include both computer network, or cyber, capabilities and internet-enabled information and influence capabilities. Their view of the use of information to influence or "operations in the information environment" are different from the point of view of the United States, in particular the U.S. military. Although the U.S. Department of Defense seeks a more unified theory of how to influence other actors, the reality is that each community involved

could be called a "cylinder of excellence." Each group is very good at what they do, but the efforts are not integrated in the planning or execution stages of the operations. Figure 1 shows the relationship of the various actors who operate in the information environment.

By contrast, Russia and China both have a more integrated view of the use of information. Russia's approach is called "information confrontation"[2] while the Chinese approach is one of "information dominance"[3] Figure 2 illustrates the Russian integration of all elements of information while Figure 3 shows a Chinese military theorist's conceptualization of the information domain.

Figure 2: The Russian Perspective on Information Competition[4]

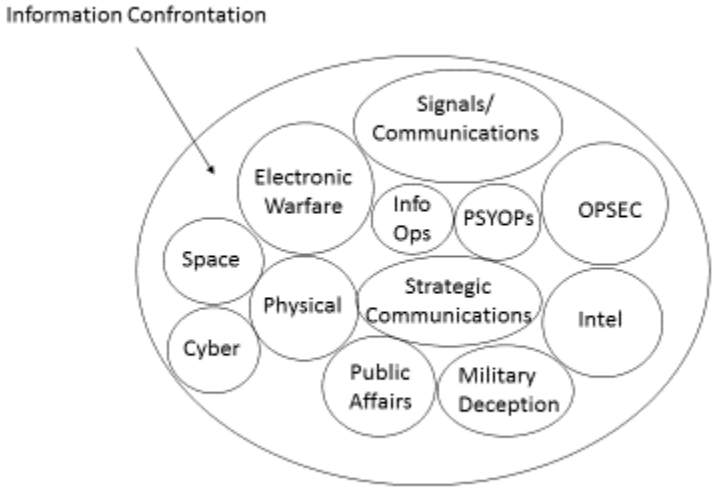
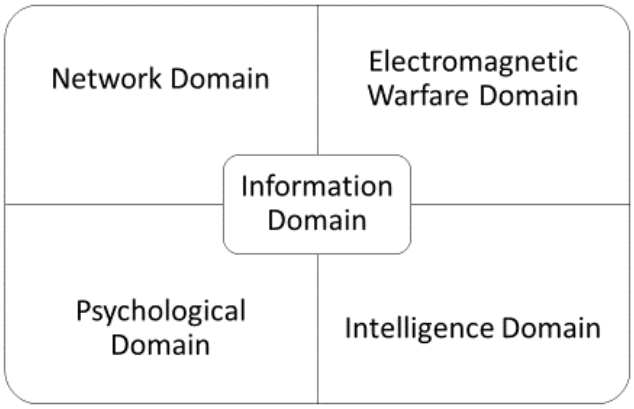


Figure 3: Chinese Military Theorist's Conception of the Information Domain[5]



This report flows as follows: We start with an overview of Chinese and Russian cyber capabilities. Contained within each of these sections is an overview of key state and non-state actors, as well as overviews of known operations and capabilities. We then provide an analysis of how these capabilities are or could be used in the future in Latin America and the Caribbean. While the focus of the analysis is on applications in Latin America and the Caribbean, the information about Chinese and Russian capabilities is also applicable to operations that they may undertake in other regions.

China and Cyberspace

The People's Republic of China (PRC) maintains a robust capacity to conduct cyber operations through the combined use of network and psychological operations, media propagation, and electronic warfare capabilities. China's People's Liberation Army (PLA), views these four forms of operations as occurring within one collective "information domain," control over which is critical for future great-power conflicts.[6] The Chinese notion of "information domain" encompasses cyberspace, but also includes other areas where information is present. In this section, we focus primarily on Chinese information capability in cyberspace.

The Chinese Communist Party (CCP) has taken extensive steps to control internal and external information flow both at home and abroad.[7] To this end, the PRC has undertaken an extensive reorganization of its military and increased its efforts to expand its influence abroad. Collectively, these policies have been implemented with the dual purposes of advancing the PRC's diplomatic and economic interests on the world stage and bolstering China's military position in the event of a large-scale conflict.[8]

To fully understand how China conducts cyber operations, one must first understand the doctrinal basis for the PLA's approach to cyber warfare. Just as Russia draws much of its cyber conflict doctrine from the former Soviet Union, China also draws on the legacy of the CCP's Leninist organizational principles.[9] Indeed, CCP strategic planners dating back to Mao heavily emphasized the importance of the control of information and its role in subduing technologically and materially superior opponents. Hence, China's use of cyber capabilities should be viewed as an outgrowth of older doctrines, updated to meet new strategic and technological realities.

China's strategy of "informationization" (信息化) has its roots in a series of reforms made to the PLA in the wake of the Gulf War. Having witnessed the dismal performance of the Iraqi military during Operation Desert Storm, PLA military observers concluded that Coalition dominance of the C4ISR[10] sphere was the key factor in their subsequent dismantlement of the Iraqi military.[11] As a result, PLA observers concluded that control over the information space would be *the* decisive factor in future conflicts. Throughout the 1990s China's government embarked upon a project of extensive military modernization, with the goal of creating a fully "informationized" fighting force.[12] The importance of informationization has also been heavily emphasized in Chinese strategic planning since the early 2000s, through internal PLA publications and strategic planning documents released by China's National Defense University (中国人民解放军国防大学). Most recently, China's 2015 Defense White Paper outlined the need to have the capability to fight and win wars under "informationized

conditions."[13] Taken collectively, it is clear that China's leadership regards control of the information domain—and thus cyberspace—as an operational lynchpin in future conflicts.

As part of this focus on the importance of information, the PLA differs significantly from its Western counterparts in its approach to cyber and network operations. Rather than seeing cyber power as a distinct capability (in the same vein as air, land, sea, and space), China's military planners view cyber and network operations as occurring in an "information domain."[14] This domain encompasses network, psychological, and media operations, as well as electronic warfare.[15] To achieve control over the information domain, these parts must act in concert in peacetime and wartime. This view on how the information domain should be approached is reflected in the way the Chinese state organizes its military intelligence-gathering organs. Under current PLA doctrine, the ability to conduct informationized warfare requires extensive knowledge of a potential adversary's systems and capabilities. This necessitates constant operational preparation of the environment (OPE) which blurs the lines between peacetime and wartime operations.[16] Moreover, network operations are not undertaken with the sole purpose of preparing for military conflict. China also routinely uses network operations to advance other aspects of its national power.[17]

China's cyber capability is comprised of many military and non-military actors spanning the public and private sector. Given the CCP's somewhat byzantine bureaucratic structure, as well as the considerable overlap of Chinese public and private entities, it is somewhat difficult to assess how China's cyber and network capabilities are organized. However, some clues can be gained from doctrinal publications released by the PRC. According to the Science of Military Strategy (战略学), Chinese network forces are broken down into three categories:[18]

- **Specialized network warfare forces** (军队专业网络战力量): These forces comprise primarily PLA Units that are trained to conduct offensive and defensive network operations. It is likely that most, if not all, of these units are assigned a military unit cover designator (MUCD/部队代号).

- **Authorized nonmilitary forces** (授权力量): These comprise non-uniformed operators, such as the Ministry of State Security (MSS) and the Minister of Public Security (MPS).

- **Civilian forces** (民间力量): These can include cyber militia/auxiliary forces, which are embedded within civilian institutions such as universities and telecommunications companies.

Prior to China's 2015 military reorganization, it was understood that the PLA General Staff Department (GSD) Third Department, also referred to as 3PLA, was tasked with managing and coordinating lines of effort across all three of the

aforementioned types of forces.[19] This responsibility appears to have passed to the PLA Strategic Support Force following the 2015 military reorganization.[20] The main actors within these three branches are as follows.

Key Actors: The Military

As indicated earlier, the PLA appears to be the primary coordinating vehicle through which China conducts operations. Prior to 2015, China's capabilities were managed by the General Staff Department (中国人民解放军总参谋部), which was subordinated to China's Central Military Commission (中国共产党中央军事委员会). The General Staff Department, in turn, oversaw the Third Department of the People's Liberation Army's General Staff Department (3PLA) and the Fourth Department of the People's Liberation Army's General Staff Department (4PLA), which supervised signals intelligence gathering and electronic warfare, respectively. Starting in late 2015, China's military underwent a major reorganization, creating the PLA Strategic Support Force (中国人民解放军战略支援部队). The Strategic Support Force comprises elements of the former General Staff Department and General Armaments Department. According to testimony given to the U.S.-China Economic and Security Review Commission, the Network Systems Department (网络系统部) of the Strategic Support Force has inherited 3PLA's mission set, headquarters location, and much of its organizational structure.[21] Consequently, the former 3PLA SIGINT bureaus appear to be organized primarily according geographical location, with the lion's share of departments focused on targets in East Asia, Europe, and the United States. Their roles and organizational structures are as follows:

- *First Bureau:* Performs a supporting role to the rest of the department. The bureau appears to be tasked with maintaining information security within the former 3PLA, as well as handling cryptography.[22]

- *Second Bureau (Formerly known as Unit 61389):* [23] Also known as APT-1, this unit primarily conducts operations in the United States and Canada. It appears to collect data on military targets, as well as engaging in industrial espionage activity.[24] The bureau gained notoriety in 2013 after the cybersecurity firm Mandiant published a profile of its ongoing operations against the United States.[25] Tools that this group uses include WEBC2, BISCUIT, and COOKIEBAG.[26]

- *Third Bureau:* Appears to primarily collect radio communications from areas in China's periphery, including North and South Korea, Taiwan, and Central Asia.[27]

- *Fourth Bureau*: Collects signals intelligence on Korean and Japanese targets.[28]

- *Fifth Bureau:* Collects signals intelligence on Russian targets.[29]

- *Sixth Bureau*: Primarily tasked with surveillance targets in South and Southeast Asia.[30]

- *Seventh Bureau:* The exact nature of the Seventh Bureau's mission is unclear, though it appears to provide a supporting role to the rest of the former 3PLA. It maintains extensive network attack and defense capabilities, as well as other means for network-centric warfare.[31]

- *Eighth Bureau*: According to analysis from the Project 2049 Institute, it is possible that this bureau is focused on targets in Europe, as well as other parts of the world. Hence, it is possible that this bureau is primarily tasked with targeting Latin America.[32]

- *Ninth Bureau*: Focuses on absorption and analysis of strategic intelligence.[33]

- *Tenth Bureau*: Appears to be concentrated on surveillance of Russian-based missile sites.[34]

- *Eleventh Bureau aka the 2020 Unit*: The exact nature of this bureau's mission is unclear, though circumstantial evidence suggests that it focuses on Russian targets.[35]

- *Twelfth Bureau aka "Putter Panda"*: Targets space-based sensing and satellite capabilities, as well as tracking information from European aerospace and telecommunications agencies.[36]

Key Actors: Civilian State

Ministry of State Security (MSS)

The Ministry of State Security (中华人民共和国国家安全部), or MSS, is China's primary civilian intelligence organization, with a mission that is roughly analogous to that of both the FBI and CIA.[37] The MSS appears to be tasked with counterintelligence and elimination of dissent within China, as well as collecting on intelligence targets abroad.[38] This entails traditional intelligence gathering missions, as well as industrial espionage activity on the part of the PRC.[39]

Substantial evidence has emerged indicating that the MSS supports and directs China's cyber operations, such as APT3, also known as Gothic Panda.[40] Additionally, the MSS directly oversees the China National Vulnerability Database (国家信息安全漏洞库), or CNNVD, which catalogues known security vulnerabilities in the Chinese network space.[41] According to the threat intelligence research firm Recorded Future, the CNNVD routinely withholds or delays the release of vulnerabilities, with the intention of stockpiling them for exploitation.[42]

Ministry of Public Security (MPS)

The Ministry of Public Security (中华人民共和国公安部) is China's main internal security force. The MPS's responsibilities primarily cover domestic policing, counterterrorism operations, and domestic information control within the PRC, as well as managing the People's Armed Police (中国人民武装警察部队), the main gendarmerie force within China.[43] Consequently, the MPS has a substantial role in overseeing network governance within China and plays a key part in maintaining network security. As a result, the MPS has assisted in drafting the PRC's cybersecurity Multi-Level Protection Scheme (MLPS), which dictates security protocols for network operators within China.[44] The MPS acts in close conjunction with the Ministry of Science and Technology (中华人民共和国科学技术部), which oversees the creation and implementation of tech standards within China.[45] Many of these tech standards are written in a way that disadvantages foreign firms seeking to operate within China, and are commonly seen as a vector for technology transfer.

Key Actors: Non-State

Cyber Militias

The PLA has partnered with numerous institutions within China's civilian sector to create a number of "cyber militias" that are called upon to perform network operations. These institutions range from telecommunications companies to academic institutions and municipal governments within China. The exact means by which these cyber militias are incorporated into the PLA's order of battle is not entirely clear. However, from the limited information that is available, it seems that they serve as nodes for civil-military integration between the PLA and China's civilian economy, as well as being a source of technical expertise that China's military can draw upon.[46] It does not appear that China's cyber militias are currently tasked with conducting offensive CNO or other sensitive tasks such as industrial espionage.

China's Internet Service Providers and Telecommunications Firms

Although they are not assigned a formal intelligence gathering or military role, China's telecommunications firms play a key supporting role in bolstering the PRC's strategic position within the network domain.

China's telecommunications firms are not technically part of the PRC governmental apparatus, nor are they officially classified as State-Owned Enterprises. However, there are indications that major Chinese telecommunications firms such as Huawei may act as de facto proxies of the PRC.[47] These firms enjoy extensive financial backing from the Chinese state, and play a supporting role in advancing China's strategic interests abroad. For example, Chinese telecom firms have taken an extremely proactive role in attempting to influence international standards, such as those governing 5G networks.[48] This drive to sway standards directly impacts China's efforts to improve its position within the network domain. The dual nature of standards writing is aptly summarized by one commentator who noted that authorship of telecom standards is a "commercial advantage which parlays itself into a security advantage...Whoever controls the technology knows, intimately, how it was built and where all the doors and buttons are."[49] Critically, Chinese telecom firms that operate abroad are still subject to PRC law.[50] Hence, these firms would be required to divulge information that passes through their networks to PRC military and intelligence authorities.

Another risk is posed by the prospect of Chinese firms acquiring and compromising elements of foreign supply chains. For example, in 2005 the Chinese firm Lenovo acquired IBM's PC manufacturing division.[51] Lenovo has strong ties to institutions such as the China Academy of Sciences (中国科学院), which in turn has a close working relationship with both the Chinese government and the PLA's information warfare organs.[52] It has also been implicated in past cyber-espionage activity conducted by the PRC.[53]

Overview of Operations

China's cyber capabilities render it a tier-1 cyber operator, whose competencies are comparable to that of Russia and other large nation states. Officially, China spends $154.3 billion annually on its military, although that number is probably closer to $190 billion when the "unofficial" is factored in.[54] The exact breakdown of China's defense budget is classified, and so it is difficult to estimate the total spent on cyber capabilities. Given that cyber capabilities are identified as one of four critical domains in China's 2015 Defense White Paper, it is likely that a considerable amount of money is devoted to developing network capabilities.[55]

Moreover, China is in the process of aggressively expanding its high-tech manufacturing sector through state-directed initiatives such as the "Made In China 2025" (中国制造2025) program, as well as long-term planning initiatives,

including the Medium- And Long- Term Plan for Development of Science and Technology (国家中长期科学和技术发展规划纲要).[56] It is clear that China seeks to direct the necessary funds to achieve self-sufficiency in critical sectors such as information technology, which could lead to the erosion of the U.S.'s advantage in this area.[57] The PRC has also invested considerable sums of money in critical dual-use technologies such as artificial intelligence and quantum computing, both of which have a variety of potential military applications, such as machine learning systems and cryptography.[58]

In both peacetime and wartime, China employs its cyber warfare abilities to enhance its overall strategic position. Critically, these network capabilities are not employed in a vacuum but work as part of a cross-domain effort to incorporate elements across the DIME[59] spectrum. Put another way, China's network capabilities support "cyber-enabled operations" across lines that can be grouped into several broad categories:

Advancing Diplomatic Claims

China has routinely employed cyber operations as a means of exerting influence over adversaries and potential partners. For example, its routine penetration of Taiwanese networks is part of a more extensive effort to exert economic and military pressure on the island to reduce its autonomy.[60] China has also used network operations to support diplomatic and trade efforts, even in cases where the PRC does not necessarily have an actively antagonistic relationship with the target entity. In late 2018, for instance, substantial evidence emerged indicating that network operators supported by the PRC had targeted the Alaska State Government in the midst of ongoing trade negotiations between China and the state government.[61] Interestingly, a large number of the network operations undertaken by the PRC target sub-state actors, many of which are associated with the so-called "Five Poisons" (五毒): Tibetan separatism, Uigher separatism, Falungong activity, Taiwanese independence, and pro-democracy activism.[62]

There have been numerous documented cases of groups tied to the Chinese government employing network operations to harass activist groups abroad, especially those tied to minority ethnicities within China.[63] For example, the Red Alpha and Ghostnet campaigns featured highly sophisticated attacks targeting Tibetan advocacy groups.[64] These phishing and watering hole attacks, along with software exploits and malware, were designed to work across multiple platforms (e.g. Windows, MacOS, Android, etc.).[65] In the aggregate, the large number of sophisticated operations against dissident groups suggests that the CCP considers their suppression to be a high priority, and worth the risk of international backlash in order to silence groups it perceives as threats to the PRC's internal stability.

While China routinely employs cyber operations to support its diplomatic efforts, these campaigns do not appear to share a uniform modus operandi. Moreover,

the exact identities of the actors undertaking these operations is difficult to ascertain, since actors associated with the PRC government take steps to obfuscate their role. For example, in the case of operations undertaken against the government of Alaska, the attackers employed an IP address associated with Tsinghua University to conduct their network reconnaissance.[66]

Improving International Perceptions of China

Unlike the Russian Federation, China does not appear to employ large-scale "troll farms" tasked with shaping the public perception of the PRC abroad. Instead, China seems to shape its perception abroad using groups like the United Front, which seeks to shape discourse among foreign policymaking and business spheres.[67] China also routinely utilizes other soft power instruments, such as the work of Confucius Institute and Chinese-backed think tanks, to mold foreign perception within academia.[68] There have been a few operations undertaken by Chinese "patriotic hacking" groups. For example, the "Honkers Union/Red Guest (红客) group targeted U.S. websites in the wake of the 2001 Hainan Island Incident involving the collision of U.S. and Chinese military aircraft and has remained semi-active since. However, these incidents almost never escalate beyond the level of petty site vandalism and do not appear to be closely coordinated by the Chinese government.[69]

Bolstering China's Military Capabilities

As discussed earlier, the PRC considers "network warfare" to be one of the four key components of the information domain, which it views as being of paramount importance in future conflicts. In a wartime situation, it is likely that China would employ network operations to disrupt the U.S. military's supply chain and C4ISR capabilities, thus dramatically reducing its combat effectiveness.[70] Additionally, the PLA augments its capabilities with large segments of the civilian cyber economy, which could support network operations in the event of a conflict.[71]

Advancing China's Economic Interests

Perhaps the most consequential component of Chinese cyber activity is their use of network capabilities to conduct industrial espionage against foreign targets. These operations have been undertaken by organs of the Chinese military (such as the former 3PLA Second Bureau), as well as groups such as APT 12/Gothic Panda, whose affiliations are less clear-cut but are still clearly backed by the PRC government.[72] Network-based industrial espionage is a favored strategy of the PRC in part because it enables China to intake vast amounts of proprietary information at comparatively little cost, and also because the difficulty of attribution grants them a veneer of plausible deniability.[73] It has been noted that many of China's cyber operators that conduct industrial espionage use relatively unsophisticated methods with comparatively poor tradecraft practices, perhaps

suggesting a preference for bulk collection over plausible deniability.[74] Regardless, when left unchallenged, it is clear that PRC-backed cyber operators have a record of accomplishment, being extremely adept at using network operations to obtain key intellectual property, thereby enabling China to leapfrog its technological and economic competitors.

Russia and Cyberspace

Just as war is the continuation of politics by other means, for Russia, cyber operations are a continuation of intelligence operations enabled by other means. For decades, the Russian Federation, and before it the Soviet Union, has been a keen observer of developing intelligence and military tactics, which they are prone to adopt and adapt to a relatively contiguous strategy.

In his exposition on Russia's spetsnaz (Спецназ), or Special Forces, retired Main Intelligence Directorate (GRU) officer Vladimir Kvachkov observed, "A new type of war has emerged, in which armed warfare has given up its decisive place in the achievement of military and political objectives of war to another kind of warfare — information warfare."[76] Kvachkov elucidates two types of information warfare: (1) information-psychological warfare, which is "conducted in conditions of natural rivalry, i.e. always," and (2) information technology warfare, which targets IT systems and is conducted "during wars and armed conflict." This first definition of information warfare largely comports with Western conceptualizations of the same term. The second is what the West often refers to as either cyber or computer network warfare. In recent years, the Kremlin has begun to leverage both methods and has spawned a third, hybrid method between the two in the form cyber-enabled information operations. In Russian parlance, these psychological information operations are referred to as active measures.

Former KGB Major General Oleg Kalugin has described active measures (активные мероприятия) as actions taken by the then-Soviet Union to discredit geopolitical adversaries and "conquer world public opinion."[77] Active measures are a key tenet in what is often referred to as "hybrid warfare" in the West, where non-military measures are used in concert with military measures to achieve a strategic objective. However, according to Russian doctrine they are used during times of peace and war.

In testimony to the Senate Select Committee on Intelligence in March 2017, King's College London War Studies professor Thomas Rid described the historical evolution of Russian active measures well, saying they seek to exploit existing cracks in adversaries.[78] He further identified three trends necessary to understand today's circumstances. First, for the last 60 years, active measures have become the norm. Second, for the last 20 years, aggressive Russian digital espionage campaigns (i.e. hacking key targets to gather intelligence) have become commonplace. Third, in the last two years, we have seen the Kremlin merge these two trends in the form of cyber-enabled active measures, or—put simply—hacking and leaking.

Before exploring how strategy has evolved and manifested in the real world in recent years, it is important to note that, like cyber operations, active measures

are not an end, but rather a means. Since the Soviet Era, the Kremlin has employed active measures in an attempt to achieve what the West calls "reflexive control" over adversaries, or the ability to alter an adversary's perception of the world. Russian pursuit of reflexive control is the product of decades of psychological and mathematical research at Russian military universities on how best to manage and influence an opponent's perception of the world. Crucially, distorting an adversary's conception of reality not only influences that adversary's decision-making calculus, but also makes it more predictable.

The General Staff of the Russian Armed Forces is led by General Valery Gerasimov. Like many Russian military strategists before him, Gerasimov is a keen observer of military and strategic trends in and out of combat. In 2014, he authored a short paper entitled "The Value of Science in Prediction," in which he examines—in great detail—Western military strategy and outlines the current and future operational environment from his perspective.[79] While the document should not be considered ironclad doctrine as some have dubbed it, it does, nonetheless, provide insight into the most powerful military minds in the Kremlin. Gerasimov notes that "the use of political, diplomatic, economic and other non-military measures in combination with the use of military forces" will normalize globally as a part of new, non-linear warfare.[80] In short, Russia views the world as locked in ongoing and perpetual conflict between powers where the lines between war and peace are blurry at best and nonexistent at worst.

As Charles Bartles observes, "One of the most interesting aspects of Gerasimov's article is his view of the relationship on the use of nonmilitary and military measures in war. The leveraging of all means of national power to achieve the state's ends is nothing new for Russia, but now the Russian military is seeing war as being something much more than military conflict."[81] For Gerasimov, warfare has become decreasingly linear, and the previously well-defined space between wartime and peacetime has been blurred. To Gerasimov, "wars are no longer declared and, when they begin, unfold according to an unusual pattern."[82] Notably, Gerasimov's long-term view appears to have been molded by observations of U.S. military strategy and action, particularly operations rightly and wrongly attributed to the U.S. in the Balkans in the 1990s and more recent actions in Libya.

Against that broader doctrinal backdrop, it's important to draw back the curtain and provide insights on how the government of the Russian Federation leverages information and cyber capabilities as influential tools of state power in the digital age. From here, we will describe the major Russian threat actors, their capabilities and past operations, our analysis of where these teams may apply their capabilities in Latin America and the Caribbean, and the broader implications for the United States and its partners in the region.

A complex web of actors from intelligence agencies and the military to industry, criminal organizations, and the media underpins Russian cyber, information, and

influence capacity. The pieces of this network have different—yet often overlapping and competing—roles, responsibilities, and influence in implementing cyber-enabled active measures against domestic and foreign adversaries.

Key Actors: The Russian Intelligence Community

The Russian foreign intelligence apparatus consists of the following three primary organizations. These agencies possess overlapping or unclear responsibilities or remits and compete with one another for political influence and funding.[83]

- The Main Intelligence Directorate (GRU)
- The Federal Security Service (FSB)
- The Foreign Intelligence Service (SVR)

The Main Intelligence Directorate (GRU)

The Main Intelligence Directorate (Главное Разведывательное Управление or GRU in Russian) is the sole intelligence agency surviving from the Soviet era. As the long-standing military intelligence agency, the GRU is primarily tasked with gathering military intelligence and conducting active measures, but plays a subsidiary role in political intelligence, economic intelligence, and counterintelligence.[84]

In the context of offensive cyber operations and cyber-enabled operations, the GRU is staffed with both network operators and information operators. Referred to variously as Sofacy, APT 28, and Fancy Bear in cybersecurity circles, the GRU's network operators exhibit characteristics very similar to the National Security Agency in the United States: a very formal code environment with complex research into cyber vulnerabilities, exploits, and code development.[85] The GRU contains Unit 26165, the group accused of compromising the U.S. DCCC and Hillary Clinton presidential campaign.[86]

The GRU's information operations team works closely with its network operators to disseminate stolen and sometimes fake information to the press and public. This group, which is separate from those gathering information, consists of regional experts to craft messaging and operational security specialists to obfuscate the source of messaging. Unit 74455, the unit accused of primarily orchestrating the dissemination of DCCC and Hillary Clinton campaign communications via Guccifer 2.0, DCLeaks, and other personas, also sits within the GRU.

In general, GRU teams target political opposition (domestically and internationally) and the fruits of their hacking activity often support in-house information operations. Cybersecurity firm Crowdstrike has assessed with a medium level of confidence that the team known as Fancy Bear or APT28 is the GRU.

The Federal Security Service (FSB)

The Federal Security Service (Федеральная Служба Безопасности or FSB in Russian) is the main successor to the Soviet-era KGB and is a jack-of-all-intelligence-trades, though its primary remit is in counterintelligence and political security.[87] Like the GRU, network and information operators sit within the agency, likely in the Second Division of FSB Center 18, also known as the FSB Center for Information Security.[88]

The agency's network operators typically utilize a hacking toolkit with add-ons to customize the tool to a given mission.[89] This suggests at least some internal code development and research expertise. The activity of the FSB's information operators appears to display slightly different traits from that of their military counterparts. Where the GRU typically co-opts well-known brands on social media and works through traditional media, the FSB takes a noisier approach, creating and using a large number of fake social media accounts to spread information and leverages non-state actors, like the Internet Research Agency, to magnify messaging.[90]

The Foreign Intelligence Service (SVR)

The Foreign Intelligence Service (Служба Внешней Разведки or SVR in Russian) is Russia's external intelligence agency. Despite its title and status as the primary foreign intelligence service, little evidence exists that the SVR is involved in cyber or cyber-enabled operations. Instead, the SVR focuses on the cultivation and maintenance of human intelligence networks.

Uncertain Teams—Energetic Bear, Palmetto Fusion, Sandworm Team

In addition to the known activities of the FSB and GRU, three teams—one no longer operating and two conducting active campaigns—have yet to be attributed to one of the two agencies, though it is assessed with a high level of confidence that the teams are Russian state actors. These teams are:

- **Energetic Bear**: Operating from the late 2000s until 2014, Energetic Bear conducted economic espionage on the oil and natural gas industry. In 2014, the group began gathering information on SCADA and industrial control system vulnerabilities and was exposed by threat researchers. It promptly ceased operations.[91]

- **Palmetto Fusion**: Operating from 2015 to present, the group consistently compromises or attempts to compromise critical infrastructure, focused primarily on energy utilities. Some threat researchers assess with low confidence that Palmetto Fusion is the same group of individuals as Energetic Bear, operating with new tools and techniques[92]

- **Sandworm Team**: Operating from 2015 to present, the Sandworm Team has repeatedly sabotaged the Ukrainian power grid.[93] The NotPetya ransomware displayed operational traits led to the belief by some that the Sandworm Team developed and released the worm.[94] Because NotPetya has been attributed by multiple intelligence agencies to the GRU, if the Sandworm Team developed and deployed NotPetya, it team likely resides within the GRU.[95] It is also likely that Sandworm operators perpetrated the 2018 attacks on the International Olympic Committee at the start of the Winter Games in Pyeongchang, South Korea, and other global sports governing bodies.

Key Actors: Private and Criminal Groups

In 2017, in response to a question about Russian meddling in U.S. elections, Russian President Vladimir Putin denied state involvement but acquiesced that some "patriotic hackers" may have attempted to influence the American election. President Putin's assertion that the Russian state played no role is deemed false with high confidence. However, it is nonetheless important to recognize the non-state groups that support the activity of the intelligence agencies. These "Patriotic Hackers" private, non-criminal groups include:

- **Concord Consulting**: Concord Consulting and Catering is an organization run by Yevgeny Prigozhin, one of President Putin's closest confidants. Prigozhin and Concord Consulting provided the financial backing to the Internet Research Agency. Prigozhin also likely funds Wagner Group, the private military firm active in Syria.

- **Internet Research Agency**: This agency is the so-called "Russian Troll Farm" that targeted and scaled messaging to key constituents in swing states during the 2016 U.S. election.

- **Digital Security**: Accused of providing technical support to the FSB.

- **Kvant Scientific Research Institute**: Accused of providing technical support to the FSB.

- **Kaspersky Labs**: The relationship between the anti-virus and threat intelligence company and Russian security services is unclear.

In addition, the Russian cybercrime network sometimes works in support of Kremlin objectives. The exact level of coordination and direction exercised over these patriotic hackers is unclear from open-source research. However, activities likely fall somewhere on the spectrum between state-integrated and state-ignored:[96]

- **State-integrated**: The national government conducts the attack using integrated non-state and state resources.
- **State-ordered**: The national government directs the attack.
- **State-coordinated**: The national government coordinates attacks by suggesting operational details.
- **State-shaped**: The state provides some support, but third parties shape and control the operations.
- **State-encouraged**: The state encourages activity as a matter of policy, but third parties shape, conduct, and control the operations.
- **State-ignored**: The state knows about the activity but is unwilling to prevent it.

A shift in the tenor of Russian non-state cyber activity can be observed around the time the Russian Federation annexed the Crimean Peninsula in Ukraine. According to at least one observer, the pre-annexation attitude was one of state-ignorance. Around and following the culmination of the Sochi Olympics and the annexation of Crimea, the activities of the oligarch-led patriotic hackers followed a model of state shaping, coordination, or even integration much more closely.

Overview of Operations

Trends in Russian cyber activity over the past three years suggest that the Kremlin is, and has been, investing significantly in developing strategy, tactics, and tools to leverage cyber capability. A study conducted by Russian data security company Zecurion Analytics posits that the Kremlin controls a "top 5" cyber army. According to reports on the Zecurion study, the Kremlin dedicates approximately $300 million per year to offensive cyber forces and employs some 1,000 on-keyboard personnel.[97] However, beyond Russian-authored reports that

may or may not be Kremlin propaganda, experts have observed a steady increase in both the number and sophistication of Russian-originated cyber activity, suggesting that the Kremlin is investing in this space.

Russian state or state co-opted cyber capability generally follows a number of trends. First, a disproportionate number of attacks exploit vulnerabilities in Adobe Flash, Java, and Internet Explorer. Second, campaigns typically reuse vulnerabilities multiple times, relying on the poor patching practices of their targets. Third, while the tools vary depending on the agency in question, some tactics are generally consistent. For example, the process for compromising targets is often:

1. Sending a spearphishing email with a malicious attachment or with a spoofed URL (often using bit.ly or other link-shortening tools);

2. Getting the user to download an attachment or visit a compromised URL to install tailored exploit;

3. Using newly created access to install a dropper with malware, usually an implant with a Remote Access Tool (RAT);

4. Creating a link with attacker command and control computer infrastructure using RAT.

Finally, if the objective of the campaign is informational, Russian intelligence services have become adept at integrating their network operators with their information operators. What this means is that the knowledge gained via offensive computer network operations is seamlessly integrated into ongoing or new information operations.

While these process and trends generally hold true for Russian state and criminal actors, different teams display unique strengths and abilities as dictated by their mission sets, budgets, and human technical capacity. Figure 4 outlines the cyber and information capabilities of the most prominent actors introduced above.

Figure 4: Russian Actors and the Capabilities

Actor	Operational Characteristics	Notable Tools	Cyber Capability	Informational Capability
The GRU (APT 28 or FancyBear)	- 97% of work completed during the working week - 88% of work done between 8 a.m. and 6 p.m. local (Moscow) time - Build malware in Russian-language settings	- Backdoor/ Exploit: Xagent - Backdoor/ Exploit/ Dropper: Sofacy - Credential Harvester: Sasfis	- Modular: developed a suite of tools that they are able to tailor to targets and "plug and play" - Formal environment and custom code - Highly obfuscated - Leverages open-source repositories to accelerate development and provide deniability - Once inside target network or device, completes multiple lateral movements via manual and "legitimate" means - Targeted	- Regional specialists - Not co-located with network operators, who are in a separate building about 5km away, but there is close coordination between teams - Quality over quantity: a tailored approach to information dissemination, using false identities (DCLeaks, Guccifer 2.0) and WordPress blogs to leak information and propagate narratives.

Actor	Operational Characteristics	Notable Tools	Cyber Capability	Informational Capability
The FSB (APT 29 or CozyBear)	- Lots of hacking activity rather than meticulously targeted activity - Many jobs, suggesting a good deal of behind-the-scenes coordination - Highly adaptable (able to counter defensive measures)	- Twitter Backdoor: HAMMERTOSS	- Modular - High obfuscation - Scattershot: lots of hacking of many different accounts - Use of open-source repositories	-Quantity over quality: use of bots and fake accounts to disseminate information

Actor	Operational Characteristics	Notable Tools	Cyber Capability	Informational Capability
Grid Teams (Sandworm Team & Palmetto Fusion)	-	- Energy Grid Malware: Crash Override/ Industryoer - Energy Grid Malware: Black Energy 3.0 - Ransomware: NotPetya (alleged)	- Highly sophisticated: obfuscated, targeted, modular, and manipulable - Generally targets industrial sectors and industrial control systems - May use DDoS or Ransomware attacks to obscure or distract from grid attacks - Creates persistent grid access (have access to grid infrastructure in the U.S. and elsewhere), but rarely delivers payload to manipulate systems (Ukraine)	-

Actor	Operational Characteristics	Notable Tools	Cyber Capability	Informational Capability
				- The so-called "Troll Factory" - Non-governmental organization, funded by Yevgeny Prigozhin (aka "Putin's Chef") and his Concord Consulting firm - Magnifies and amplifies key information to support Kremlin narratives at home and abroad
The Internet Research Agency	-	-	-	- Uses a combination of fake social media accounts run by humans and bots; also creates and administers fake "groups" on social media websites to organize in-person protests and rallies - Hundreds of employees - Well financed (monthly budget of over USD$1.2 million for a single project)

Globally, Russia has leveraged cyber capability in three primary ways: (1) operational preparation of the environment (OPE), (2) cyber warfare, and (3) cyber-enabled influence operations. Here, we describe individual operations of each of these types, in order to help build understanding of how a Russian adversary might leverage cyberspace for strategic gain in Latin America and the Caribbean.

Operational Preparation of the Environment (OPE)

Like most tier-1 cyber powers, Russia engages in robust operational preparation of the environment (OPE), largely as a "just in case" exercise, not necessarily as a sign of impending military operations. Russian cyber operators, most likely from Sandworm team and Palmetto Fusion (likely both within the GRU), consistently develop access to key communications systems (military and civil) and critical infrastructure in adversaries they anticipate could one day engage in active hostilities. Because the high degree of research, time, and effort needed to create and maintain access in adversary critical infrastructure systems, Russia seeks to maintain access points should they wish to conduct cyber warfare (as described below) in the future.

In most cases, these accesses are largely benign and have not been used to create any disruption during peacetime. This type of operation is what has led to recent reporting in the United States regarding Russian cyber activity targeting energy and other critical infrastructure sectors.[98] It is also possibly the activity that led to an accidental blast furnace explosion in Germany.[99] However, access can go from benign to malicious rapidly, and most of the Russian cyber actors outlined above possess the tools and capability to rapidly escalate its actions to cyber warfare.

Cyber Warfare

The clearest case of intentional cyber warfare conducted by Russian services is currently taking place in Ukraine during ongoing kinetic hostilities. In Ukraine, Russian cyber warfare has taken two shapes: information operations and critical infrastructure attacks.

By targeting mobile networks, Wi-Fi, mobile phones, and other military and civilian communications networks, Russian actors are able to conduct extensive in-theatre information operations. In Ukraine, these activities have included:

- Psychological and friction operations against troops on the front lines—and their families—via direct text messages to individuals including things like:
    - "Your battalion commander has retreated. Take care of yourself."
    - "You are encircled. Surrender. This is your last chance."

    - "Ukrainian soldier, what are you doing here? Your family needs you alive."
    - "You will not regain Donbas back. Further bloodshed is pointless."
    - "Ukrainian soldier, it's better to retreat alive than stay here and die."[100]

- Distributed Denial of Service (DDoS) attacks against government and non-government communication systems

In addition to compromising communications systems, Russian actors have demonstrated a proclivity for targeting critical national infrastructure systems for compromise and manipulation. This type of operation relies on the robust OPE described above. The most notable case in the Ukraine occurred during the 2015 and 2016 BlackEnergy attacks on its power grid, which shut power off to more than 200,000 Ukrainians during the cold winter months.

Cyber-Enabled Influence Operations

This final brand of operation, a cyber-enabled influence operation, is perhaps the most widely recognized Russian intelligence operation. While the well-documented activity around the 2016 U.S. presidential election elevated the profile of this tactic to the global political level, Russian intelligence services have engaged in similar information operations for the better part of a century, particularly in Eastern Europe.

Chinese and Russian Use of Cyber Capabilities in Latin America and the Caribbean

The Russian Federation and the People's Republic of China operate in cyberspace in pursuit of diplomatic, informational, military, and economic (DIME) interests around the globe. Although many in Latin America and Caribbean view cyber competition as an issue for Russia, China, the European Union, and the United States, they are discovering that, to paraphrase Leon Trotsky, "You may not be interested in cyber, but cyber is interested in you."

Based on U.S. performance in conflicts since 1990, Russia and China have both determined that armed conflict with the United States is a bad idea. Based on that same analysis, however, both have discovered that the way to confront the United States is through asymmetric means below the threshold of "armed attack" or "use of force" as mentioned in the Charter of the United Nations. Crossing that threshold allows the aggrieved state to use all means necessary to defend themselves (as with 9/11) or allows the United Nations to call for armed action under Chapter VII (as with Desert Storm). As such, both China and Russia have developed methods of operating in the "grey zone," or below the threshold that triggers a military response.

Russia and China have discovered the utility of these grey zone operations and pursue them globally. The techniques that were developed to confront the United States are now being deployed elsewhere, such as Taiwan and Ukraine. These techniques are demonstrated across the four elements of national power: diplomacy, information, military, and economy.

China seeks to play the long game and ensure that its interests are secured, including the Belt & Road Initiative (BRI) as well as access to natural resources and commodities. It seeks to improve its global perceptions and influence on issues like the South China Sea and Taiwan. Although Beijing does not seek military supremacy, it does want to bolster its military capabilities. Its economic interests, however, are its priority; increasing economic status will ensure a quiescent Chinese population and enable the other instruments of national power, like diplomacy, information, and military power.

Since the Moscow Security Conference in 2007, Russia has sought to contest the current global system that it believes is designed to give the advantage to the United States and partners to Russia's detriment. Moscow's strategic goal is regime survival and the morphing of the current system to a multipolar global system, but it will not challenge the system overtly, instead seeking opportunities to destabilize it. The intent is to fracture intergovernmental organizations, like NATO and the European Union, while undermining international institutions, like humanitarian law and norms. Through political warfare, they hope to contest

Western democracies, diminishing their power while bolstering Russian power, and regain a buffer zone in Eastern Europe. Although Latin America and the Caribbean are not strategic priorities for Russia, they will challenge the United States in its near abroad to reduce U.S. influence in the region.

Russian and Chinese options for leveraging cyber capabilities in Latin America and the Caribbean may be examined through the lens of the instruments of national power. As an example, the Chinese use diplomacy along with information and intelligence operations in support of its economic goals. These elements are interrelated and all are performed simultaneously in support of strategic goals. Figure 6 provides an overview of our DIME Framework as well as some examples of Chinese and Russian objectives falling under each category.

Figure 6: The DIME Framework and Cyber Operations

Instrument	Description	Examples of Chinese Objectives	Examples of Russian Objectives	Operative Question
Diplomatic	Efforts by a state to influence the policy or action of another state through negotiation.	- Grow global support for its territorial claims in the South China Sea. - Decrease the number of states that recognize the legitimacy of the Republic of China (Taiwan).	- Diminish international opposition to Russian military actions in Ukraine and Syria - Cast doubt on the legitimacy and primacy of multilateral forums - Cultivate partners in the region to enhance support for its legal and normative initiatives to bolster state sovereignty and provide international top-cover for authoritarianism.	What cyber and information operations could Russia or China conduct in the region support of regional or global diplomatic objectives?

Instrument	Description	Examples of Chinese Objectives	Examples of Russian Objectives	Operative Question
Information	Efforts by a state to influence the policy or action of another state or population by controlling or spreading information, targeted at the local population.	- Increase positive sentiment towards China in the region, likely in support of economic and market-share goals	- Sow discord and undermine democratic processes through misinformation - Enable populist politicians, which tend towards more favorable views of Russia.	What cyber and information operations could Russia or China conduct in the region in support of information objectives?
Military	Efforts by a state to influence the policy or action of another state or group via the use of military power.	- Build military to military partnerships - Collect military intelligence	-Support friendly militaries - Develop and maintain access to critical and critical information infrastructure.	What cyber and information operations could Russia or China conduct in the region in support of military objectives?
Economic	Efforts by a state to utilize economic power to influence another state or group, and to bolster its own economic strength and reach.	- Guarantee access to key resources - Bolster the local market for Chinese high-tech, telecommunications, and arms exports.	- Bolster the local market for Russian arms and energy exports - Maintain access to local black and criminal markets for Russian actors.	What cyber and information operations could Russia or China conduct in the region in support in support of economic objectives?

Here, we examine how China and Russia may use cyber and information operations in support of objectives in each of these areas.

China in Latin America and the Caribbean

In this section, we explore how China could use cyber and information operations in Latin America and the Caribbean in support of diplomatic, information, military, and economic objectives. The DIME objectives described herein are grounded in doctrine and analysis of the geopolitical goals of China. However, due to limited open-source material, the analysis of how China might apply cyber and information capabilities in the region to support these goals is largely based on extrapolation based on Chinese activity elsewhere and Latin American and Caribbean vulnerabilities.

Diplomatic Objectives

China performs cyber and information operations in order to build support from decision-makers and the general population for Chinese diplomatic priorities in much of the world. Current Chinese diplomatic priorities include building support for its initiatives as part of the One-China policy against the recognition of the government of the Republic of China (Taiwan), its territorial claims in the South China Sea, and its approach to multilateral forums like the UN. In addition, China increasingly provides support to those who oppose U.S. interests, where they do not align with Chinese interests, in an effort to frustrate the United States politically.[101]

The Taiwan issue is of potentially heightened importance in Latin America and the Caribbean, as nine of the 11 states that recognize Taiwan are located in the hemisphere: Belize, Guatemala, Haiti, Honduras, Nicaragua, Paraguay, Saint Kitts and Nevis, Saint Lucia, and Saint Vincent and the Grenadines.[102] Primary drivers of these states' loyalty to Taiwan are financial gifts and investments from Taiwanese companies.[103] Nonetheless, this support is challengeable, as shown by Panama switching sides in June 2017,[104] the Dominican Republic changing allegiances in April 2018,[105] and El Salvador recognizing the PRC in August of 2018.[106] Reporting suggests that China will likely accelerate its efforts to continue diplomatically to isolate Taiwan.[107] This push involves seizing control of online narratives regarding Taiwan's independence.[108] It could also include conducting cyber operations to determine the stance of key decision-makers vis-à-vis Beijing's interests as well as reach people either who sympathize with them or who are vulnerable to its influence and can be subordinated to their goals.

More generally, China will continue its somewhat unique approach to multilateralism, which is characterized by increasing engagement in existing multilateral forums, pushing hard on issues it deems in its interest and blocking those that are not, avoiding responsibility for particularly burdensome initiatives, and generally refraining from making grand proposals at multilateral forums.[109] Relevant to cyber and information operations, China has been a proponent of

cybersecurity conventions that would transfer greater responsibility over the internet to the hands of sovereign states and enabling greater state control of content and information online, as signaled by their repeated sponsorship of a letter to the UN General Assembly proposing discussions on the topic and co-signing a recent proposed resolution.[110] China may covertly engage in cyber and information activity that undermines existing international norms for the dual purpose of achieving other objectives and bolstering the case for new conventions.

Information Objectives

The Chinese government engages in public messaging campaigns in support of economic and political objectives. For example, in key markets, consumers campaigns to encourage consumers to buy Chinese products (advertising) or build popular support for Chinese diplomatic objectives (propaganda). Some of these campaigns are transparent, others less so.

Military Objectives

China actively works to build military-to-military partnerships with several militaries in the region. As part of this effort, China has, for example, built schools for military training professional military education in China similar to the Western Hemisphere Institute for Security Cooperation in the United States. [111] They invite participants from a variety of countries in the hemisphere to attend those schools. Militaries sending troops to train in these facilities should be cautious about bringing electronics and other communications systems with them, which may be vulnerable to exploitation during such visits providing novel collection platforms.

In addition, China provides low-tech supplies such as boots and uniforms to regional militaries through state and quasi-state enterprises. These activities are all part of a long-term Chinese strategy to become the partner of choice of militaries in the region, though it is unclear how, apart from traditional advertising and propaganda, cyber and information operations would be used in support of these objectives.

However, it is reasonable to expect that the Chinese military services currently and will continue to use cyber means to conduct intelligence operations against influential regional military powers, like Brazil, Chile, Argentina, and Mexico.

Furthermore, like most tier-1 cyber powers, Chinese military entities are likely to conduct cyber operations to generate access to key communications systems, though no evidence of such activities exist in open source material. Likely targets for such access operations include command and control (C2) infrastructure of potential military adversaries and government communication systems. These operations may come in the form of traditional computer network operations, but

may also take the shape of strategic supply chain compromises on high tech and telecommunications exports.

Economic Objectives

Economic goals are likely to continue to be a top priority for China in the Western Hemisphere and much of their cyber and information activity will be designed to pursue these interests. To that end, China seeks to guarantee access to resources and to open up new markets, while diminishing the economic might of competitors. Some commentators suggest the goal of this activity is to become the world's predominant economic hegemon. Specifically, Chinese companies, often with governmental assistance, continue to work open new markets to Chinese high tech, telecommunications, and arms exports.[112] In addition, China seeks to retain access to critical resources such as Venezuelan oil and a Chinese-dominated Nicaraguan canal.

Companies typically attempt to obtain favorable contracts and take-overs of local companies to guarantee resources and achieve monopolies in states to ensure not only access to resources, but to coerce the target state if necessary. In the past, Chinese government entities have been accused of conducting cyber operations in support of those goals, namely though intelligence operations to determine opportunities; influence operations to decrease local resistance to Chinese economic interests; and intellectual property theft to help Chinese firms emulate locally successful products and services.[113]

In spite of bilateral agreements with the likes of Australia, Germany, and the United States, aimed at blunting Chinese cyber industrial espionage, evidence from each country suggests that Chinese firms and state organizations have continued this activity.[114] It is highly likely that Chinese entities will engage in similar activity in markets of interest.

Although the theft of intellectual property is the most often cited form of Chinese industrial espionage, the Chinese also undertake intelligence operations to obtain local market advantages. For example, a common Chinese tactic for bolstering economic reach involves the acquisition of local companies in foreign markets. In the past, Chinese state security services have assisted corporate takeovers by providing intelligence on the internal deliberations and potential vulnerabilities of local companies targeted for mergers or acquisitions.[115] Some of this intelligence is gathered through open-source and human collection methods; some intelligence is collected via illicit breaches of company and government computer systems. As China becomes more interested and assertive in Latin American and Caribbean markets, they can be expected to replicate many of the cyber and information operations and tactics they have employed elsewhere.

Russia in Latin America and the Caribbean

In this section, we explore how Russia could use cyber and information operations in Latin America and the Caribbean in support of diplomatic, information, military, and economic objectives. As with our China in Latin America and the Caribbean section, the DIME objectives described herein are grounded in doctrine and analysis of the geopolitical goals of Russia. However, as with China, due to limited open-source material the analysis of how Russia might apply cyber and information capabilities in the region to support these goals is largely based on extrapolation based on Russian activity elsewhere and Latin American and Caribbean vulnerabilities.

Media in the region have been quick to point to Russian meddling in elections in Latin America and the Caribbean.[116] In open source material, there exists limited evidence of past or ongoing cyber-enabled influence operations in the region akin to those around the 2016 presidential election in the United States. Where social media bots and fake accounts have spread political messaging around key elections and votes in the region, this activity had largely been attributed to domestic actors deploying similar tactics to those used by Russian intelligence services in the lead up to the U.S. election.[117] However, recent events in Venezuela point to increased Russian activity.[118]

Notably, however, major media platforms—RT and Sputnik—have developed a stronger presence in Latin America and the Caribbean in recent years and have increased their Spanish and Portuguese language coverage.[119] In addition, while Russia has a history of using cyber and information capabilities in the event of hot conflicts, there is no public evidence of Russian actors penetrating civil communication systems or critical infrastructure for exploitation in the region. Nonetheless, in October 2018, Symantec reported that GRU operators targeted a government in Latin America. No more information was provided, including which government and the type of system targeted. However, this is the first open-source claim that Russia is targeting Latin American or Caribbean assets.[120]

Diplomatic Objectives

Russia's global diplomatic priorities include diminishing international opposition to Russian military actions in Ukraine and Syria, casting doubt on the legitimacy and primacy of multilateral forums that have been dominated by the United States and Europe and traditionally underpinned liberal democratic order, and spreading support for its legal and normative initiatives to bolster state sovereignty and provide international top-cover for authoritarianism domestically. Russia's regional diplomatic priorities are to bolster partnerships in the region and weaken U.S. influence, while possibly cultivating support for initiatives and proposals at multilateral forums like the UN General Assembly. In

addition, no Latin American or Caribbean countries have joined the U.S.-led sanctions on Russian individuals. The Kremlin would most likely prefer to keep it that way.

Much of Latin America and the Caribbean are part of the Cold War-era Non-Aligned Movement. Today, this means that they are potentially swing states on international policy issues. In recent years, Russia has made a concerted push at the United Nations in favor of an international convention on information security. While seemingly innocuous on the surface, the proposal represents an attempt to diplomatically legitimize authoritarian approaches to controlling information and the internet. As New America has noted, Latin American and Caribbean countries are likely to be crucial "digital deciders" in that particular diplomatic debate.[121]

Russia, like any well-resourced country, assists their diplomatic efforts with intelligence, and increasingly cyber-enabled intelligence. It is reasonable, therefore, to expect decision makers in countries deemed of diplomatic interest to be under surveillance. In addition, Russia may continue to conduct cyber operations that undermine international law in an effort to create more urgency and purchase for a binding international agreement.[122]

Information Objectives

Outside of its near abroad, the Russian government has shown a proclivity towards leveraging information to exert influence and sow discord over other instruments of national power like diplomacy, the military, and trade or investment. As we note above, the Russian government views information campaigns as a relatively cheap and scalable means to attain its national goals. Russia's information objectives globally include undermining democratic processes, in part to seek greater legitimacy for its own authoritarian approach to governing, and enabling populist politicians in democratic parts of the world, many of whom have exhibited more favorable views of Russia in recent years.

Russia is likely to operate in the information environment throughout the hemisphere as part of its strategy to provide low-cost irritation to the United States. They are and will continue to conduct white[123] and grey[124] propaganda through their traditional media outlets such as *Actualidad RT* or RT (the former Russia Today) in Spanish. This propaganda will support Moscow's global interests such as gathering support for Russian activities in Ukraine and Syria and diminish international support for U.S. interests. Although it is not clear from open-source information whether Russian actors have engaged in more covert information operations in the region, the cost of doing so in the region would be low. They could, therefore, periodically participate in black propaganda[125] operations such as the campaign in Central America to persuade the population that Americans were adopting children to take them back to the United States to be used for body parts.[126]

Military Objectives

Russia has two priorities for military activities in the Western Hemisphere. The first is to support friendly regimes. The second is to develop and maintain access to critical military and infrastructure systems in order to exploit them in the event of hot conflict. Here we unpack those objectives in greater detail and explore how cyber and information operations might be used to support them in the region.

In order to support friendly regimes, the Russians could penetrate the networks of two groups of states: the friendly states and those states who might endanger them. They would monitor networks in friendly states to ensure that they maintain situational awareness of the military situation and to identify potential military problems (i.e. coup plans) within friendly countries, particularly Venezuela and to a lesser extent Cuba.

The potential adversaries to friends in the region really only include the Colombians and the United States. In particular, the Russian armed forces are most likely seek to enter Colombian and U.S. intelligence and command and control (C2) networks to both build better awareness of military plans and to conduct operational preparation of the environment so that they could slow down or take out C2 networks in case of conflict. In addition, the Russians have perhaps the most advanced capability in the world to disrupt delivery of critical infrastructure services, like power delivery. In order to conduct such operations, they work to create and maintain access to critical infrastructure systems in adversarial or potentially adversarial countries. They already engage in similar activities in the United States and may do the same in other adversarial countries in the Americas.

Economic Objectives

Identifying Russia's economic objectives can be difficult. Its legitimate trade with Latin America and the Caribbean is miniscule in comparison to both China and the United States. In addition, Russian exports to Latin America and the Caribbean make up a small fraction of their total export. Globally, Russia's exports are primarily in the arms, energy, and metals sectors. However, 39 percent of Russia's domestic economy is underground—in the so-called shadow economy.[127] Here we will unpack Russian objectives in the arms, energy and raw materials, and underground markets and then explore how cyber or information operations might be used to support those objectives in Latin America and the Caribbean.

Annual Russian arms sales to Latin America and the Caribbean make up a relatively small percentage of their overall arms sales, with the LAC market hovering between 0 and 15 percent of annual arms exports. Nicaragua, Mexico, Venezuela, and Cuba are the primary arms customers in the region. Between 1992 and 2017, Venezuela accounted for 73 percent of the local market for arms.

[128] Apart from arms, the brunt of the Russian economy lies in raw materials in the form of crude and refined oil, as well as heavy metals, and the extraction and treatment of these materials. Russia has already made deals with the likes of Venezuela, Cuba, Bolivia, Mexico, and Argentina to provide or support energy production and could work to expand this effort.[129]

In addition to these legitimate economic activities, one estimate posits that 39 percent of Russia's domestic economy exists separately and underground.[130] Russian criminal activity is transnational, and some participants in Russian criminal activity are closely involved with decision-makers in the Kremlin.[131] Russian actors will continue to seek access to black markets around the world online and offline. Russians are crucial, for example, in the emerging underground economy for offensive cyber capability.[132] Russian business and criminal groups will also likely continue to use bank accounts in Latin America and the Caribbean to launder money in an effort to hide illicit activity.

In support of these economic interests, Russia could engage in a broad spectrum of cyber and information activity. On the far end of the spectrum, Russia could sabotage existing energy delivery systems via relatively cheap cyber means, opening up new markets to Russian energy procurement and delivery support and expertise. In addition, in order to create offensive cyber capability, developers need to discover vulnerabilities in software and hardware and—depending on the nature of the capability—develop working understanding of how the specific targeted system works. While this lends to the difficulty in scaling the sale of robust, targeted cyber capability, it means that, in order to continue to operate in this market, Russian actors will necessarily need to probe potential target systems. Cyber activities—likely by state and non-state actors—will likely continue to complement the development of offensive cyber capability for sale in black markets.

Conclusion

Russia and China are conducting cyber operations throughout the Western Hemisphere in support of their global policies and operations. While Russia seeks to destabilize the global system for its own advantage, China's goal is to maintain the current system and replace the United States as the global hegemon. Although their daily cyber operations will not pose a clear and present danger to U.S. goals and activities in the region, the cumulative effect of their cyber operations will endanger U.S. influence in the region, could circumscribe the U.S. ability to operate in the region and, in the worst case, cause the United States to allocate resources to the area in case of a global conflagration. To ensure that China and Russia do not achieve their objectives, the United States must operate in the region as well as build partner cyber capacity throughout the area.

Notes

1 Chart is the original work of G. Alexander Crowther, Ph.D.

2 "Information Confrontation over Ukraine," Cybernautika, February 27, 2014.

3 Dean Cheng, "Cyber Dragon: Inside China's Information Warfare and Cyber Operations,"(Keynote address, Heritage Foundation, Washington, D.C., March 20,2017).

4 Chart is the original work of G. Alexander Crowther, Ph.D.

5 Figure 3. "China and Cybersecurity" (Figure 8.2 in Chapter 8), Oxford University Press (Oxford, UK, April 2015)

6 John Costello, "Chinese Views on the Information 'Center of Gravity': Space, Cyber and Electronic Warfare," *Jamestown Foundation,* Volume 15, Issue 8 [2015], https://jamestown.org/program/chinese-views-on-the-information-center-of-gravity-space-cyber-and-electronic-warfare/

7 The term "informationization" started to enter the Chinese military lexicon around the late 90's and was routinely included in China's military white papers starting in 2002. It appears that PLA writings on dominance of the electromagnetic sphere (制电子权) grew to include network warfare. Collectively, this was referred to as dominance of the information space (制信息权); Dean Cheng, Cyber Dragon: Inside China's Information Warfare and Cyber Operations pp 33-34, 39-40.

8 John Costello, "China's Irregular Warfare in the Cyber Domain," Real Clear Defense, June 17, 2015

9 Phillip C. Saunders and Joel Wuthnow, "China's Goldwater-Nichols? Assessing PLA Organizational Reforms," *Institute for National Strategic Studies,* (April 2016): https://inss.ndu.edu/Portals/68/Documents/stratforum/SF-294.pdf

10 C4ISR stands for: Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance.

11 Cortez A. Cooper III, "PLA Military Modernization: Divers, Force, Restructuring, and Implications," [Testimony, U.S.-China Economic and Security Review Commission, Washington D.C., February 15, 2018].

12 Jaqueline Newmyer, "The Revolution in Military Affairs with Chinese Characteristics," *Journal of Strategic Studies* 33, no.4 (August 20, 2010): 483-504, https://doi.org/https://doi.org/10.1080/01402390.2010.489706; Cortez A. Cooper III, "PLA Military Modernization: Divers, Force, Restructuring, and Implications," [Testimony, U.S.-China Economic and Security Review Commission, Washington D.C., February 15, 2018].

13 中华人民共和国国务院新闻办公室 (State Council Information Office of the People's Republic of China, "China's Military Strategy)," China's Military Strategy (中国的军事战略), May 27, 2015 http://www.scio.gov.cn/zfbps/ndhf/2015/Document/1435161/1435161.htm

14 John Costello, "Chinese Views on the Information 'Center of Gravity': Space, Cyber and Electronic Warfare," *The Jamestown Foundation* 15, no.8 (April 16, 2015), https://jamestown.org/program/chinese-views-on-the-information-center-of-gravity-space-cyber-and-electronic-warfare/.

15 *ibid*

16 Dean Cheng, "*Cyber Dragon: Inside China's Information Warfare and Cyber Operations,"* [Westport, CT: Praeger Publishing, November 14, 2016], 37-44

17 William Hannas, James Mulvenon, Anna B Puglisi, *Chinese Industrial Espionage: Technology, Acquisition and Military Modernization, (Routledge, Abingdon on Thames, UK, 2013)*

18 The Science of Military Strategy is generally regarded as being one of the most authoritative representations of Chinese doctrine. The document was published through China's Academy of Military Science, which reports directly to the CMC; 军事科学院·军事理论著作(Military Academic Works , Academy of Military Science) https://fas.org/nuke/guide/china/sms-2013.pdf

19 Mark A. Stokes and L.C. Russell Hsiao, "Countering Chinese Cyber Operations; Opportunity and Challenges for U.S. Interests," *Project 2049 Institute*, [October 29, 2012], https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-079.pdf

20 John Costello, "China's Strategic Support Force: A Force for a New Era," [Testimony, U.S. - China Economic and Security Review Commission, Washington, D.C., February 15, 2018].

21 *ibid*

22 Mark A .Stokes, Jenny Lin and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," *Project 2049*, November 11, 2011

23 The number "61389" denotes Second Bureau's Military Unit Cover Designator (MUCD), which is a five-digit number assigned to all Chinese units (部队). Chinese sources will often refer to a unit by its MUCD rather than its true name in order to obfuscate said unit's role and capabilities. MUCDs correspond either to a unit's geographic location (e.g. forces in the Beijing Military Region was formerly assigned MUCD blocks 51/52xxx) or by service (e.g. the units assigned to the former 2nd Artillery Corps were assigned the 80xxx MUCD block). Prior to 2015 under the former General Staff Department including 3PLA were assigned the MUCD block 61xxx. However, after the 2015 reorganization all existing MUCD's became defunct, since the corresponding services/Military Regions that they were attached to were thoroughly altered. Units under the SSF appear to have been assigned the MUCD block of 320xx. However, further research is needed to determine the MUCDs attached to each specific bureau. See: John K Costello, Joe Mc Reynolds, "China's Strategic Support Force: A Force for a New Era," *China Strategic Perspectives 13, Institute for National Strategic Studies, National Defense University,* 2018, https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.Kevin Pollpeter, Kenneth W. Allen, *The PLA as Organization v2.0, Air University, 2002 – 2012,* https://www.airuniversity.af.edu/Portals/10/CASI/Books/PLA_as_Organization_v2.pdf.Mark A. Stokes, Jenny Lin, L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," *Project 2049 Institute* (November 11, 2011), https://project2049.net/2011/11/11/the-chinese-peoples-liberation-army-signals-intelligence-and-cyber-reconnaissance-infrastructure/.

24 *ibid*

25 Mandiant, "APT 1: Exposing Once of China's Cyber Espionage Units," (Alexandria, VA, 2013).

26 *ibid*

27 Mark A. Stokes, Jenny Lin, L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," *Project 2049 Institute* (November 11, 2011), https://project2049.net/2011/11/11/the-chinese-peoples-liberation-army-signals-intelligence-and-cyber-reconnaissance-infrastructure/.

28 *ibid*

29 *ibid*

30 *ibid*

31 Ibid.

32 Mark A. Stokes, Jenny Lin, L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance

Infrastructure," *Project 2049 Institute* (November 11, 2011), https://project2049.net/2011/11/11/the-chinese-peoples-liberation-army-signals-intelligence-and-cyber-reconnaissance-infrastructure/

33 Dean Cheng, "*Cyber Dragon: Inside China's Information Warfare and Cyber Operations,"* [Westport, CT: Praeger Publishing, November 14, 2016], 182

34 Mark A. Stokes, Jenny Lin, L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," *Project 2049 Institute* (November 11, 2011), https://project2049.net/2011/11/11/the-chinese-peoples-liberation-army-signals-intelligence-and-cyber-reconnaissance-infrastructure/

35 *ibid*

36 Nicole Perlroth, "2nd China Army Unit Implicated in Online Spying," *New York Times,* June 9, 2014. Crowdstrike, *Crowdstrike Intelligence Report* (Sunnyvale, CA: Crowdstrike, 2014)

37 U.S.-China Economic and Security Review Commission, *Chinese Intelligence Services and Espionage Threats to the United States,* (USCC 2016 Annual Report to Congress, USCC: November 16, 2016)

38 Peter Mattis, "The Analytic Challenge of Understanding Chinese Intelligence Services," *Studies in Intelligence* vol.56, no.3 (September 2012) https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-56-no.-3/pdfs/Mattis-Understanding%20Chinese%20Intel.pdf

39 National Counterintelligence and Security Center, *Foreign Economic Espionage in Cyberspace 2018* (Washington, D.C.: National Counterintelligence and Security Center, July 26, 2018)

40 Insikt Group, " Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3," *Record Future,* May 17, 2017, https://www.recordedfuture.com/chinese-mss-behind-apt3/

41 Insikt Group, "China's Cybersecurity Law Gives the Ministry of State Security Unprecedented New Powers Over Foreign Technology" *Record Future,* August 31, 2017; https://www.recordedfuture.com/china-cybersecurity-law/

42 Priscilla Moriuchi and Ladd Bill, "China Altered Public Vulnerability Data to Conceal MSS Influence," *Record Future,* March 9, 2018 https://www.recordedfuture.com/chinese-vulnerability-data-altered/

43 Global Security, "Ministry of Public Security, " Global Security, [No date given] https://www.globalsecurity.org/intell/world/china/mps.htm; Federation of American Scientist, "China Intelligence Resource Program," (November 26,1997):https://fas.org/irp/world/china/mps/org.htm

44 Covington; "China Seeks Public Comments for Draft Regulations on Cybersecurity Multi-level Protection Scheme to Implement the Cybersecurity," Law, Covington & Burlington LLP, July 5, 2018; https://www.cov.com/-/media/files/corporate/publications/2018/07/china-seeks-public-comments-for-draft-regulations-on-cybersecurity-multilevel-protection-scheme-to-implement-the-cybersecurity-law.pdf

45 Ministry of Industry Information and Technology (中华人民共和国工业和信息化部); http://www.miit.gov.cn/n1146322/n4426653/index.html

46 Robert Sheldon, Joe McReynolds, *Civil-Military Integration and Cybersecurity*," China and Cybersecurity: Espionage, Strategy, and Politics and in the Digital Domain(Oxford, UK; Oxford University Press, 2015, pp.190-200)

47 U.S. House of Representatives Permanent Select Committee on Intelligence, Investigative Report on the U.S. National Security Issues Posed by Chinese

Telecommunications Companies Huawei and ZTE, October 8th, 2012

48 Raymond Zhong, "China's Huawei Is at Center of Fight Over 5G's Future," *New York Times*, March 7, 2018.

49 *ibid*

50 US-China Economic and Security and Review Commission, Hearing on China, the United States, and Next-Generation Connectivity (March 8 , 2018)

51 Eric Bangeman, "Lenovo laptop deal draws scrutiny from government agency," *Ars Technica*, March 28, 2006

52 U.S.- China Economic and Security Review Commission, Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications technology (April 19, 2018)

53 *ibid*

54 U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*, (Washington, D.C.,: May 16, 2018)

55 军事科学院·军事理论著作 (Military Academic Works , Academy of Military Science) https://fas.org/nuke/guide/china/sms-2013.pdf

56 http://www.cae.cn/cae/html/files/2015-10/29/20151029105822561730637.pdf

57 Lorand Laskai,"Why Does Everyone Hate Made in China 2025?," Council on Foreign Relations, March 28, 2018

58 Munish Sharma, "Decrypting China's Quantum Leap," *The China Journal*, no. 80 (July 2018): 24-45.; Dominique Barton, Johnathan Woetzel, Jeongmin, Seong, Qinzheng Tian, "Artificial Intelligence: Implications for China,"(presented, 2017 China Development Forum, April 2017) ; Robert Warren Button, "Artificial Intelligence in the Military", *RAND Corporation,* September 7, 2017, https://www.rand.org/blog/2017/09/artificial-intelligence-and-the-military.html; Bloomberg, " Is China Winning Race with U.S. to Develop Quantum Computers?," *The South China Morning Post*, April 9, 2018

59 DIME: Diplomatic, information, military, and economic actions.

60 Jess Macy Yu," Chinese Cyber-attacks on Taiwan government becoming harder to detect," *Reuters, June* 15, 2018, https://www.reuters.com/article/us-taiwan-china-cybersecurity/chinese-cyber-attacks-on-taiwan-government-becoming-harder-to-detect-source-idUSKBN1JB17L

61 Sanil Chohan, Winnona DeSombre, Justin Grosfelt, "Chinese Cyberespionage Originating From Tsinghua University Infrastructure," *Record Future,* August 16, 2018 https://www.recordedfuture.com/chinese-cyberespionage-operations/

62 Samantha Hoffman, Peter Mattis,"Managing the Power Within: China's State Security Commission," War on the Rocks, July 18, 2016, https://warontherocks.com/2016/07/managing-the-power-within-chinas-state-security-commission/ ;Juan Andres-Guerrero Saade, Sanil Chohan, "Red Alpha: New Campaigns Discovered Targeting the Tibetan Community," *Record Future*, June 26, 2018 https://www.recordedfuture.com/redalpha-cyber-campaigns/

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

64 The SecDev Group,"Tracking Ghostnet: Investigating a Cyberespionage Network," *The SecDev Group*, March 29, 2009; Andres-Guerrero Saade, Sanil Choban," RedAlpha: New Campaigns Discovered Targeting the Tibetan Community," *Record Future,* June 26, 2018 https://

www.recordedfuture.com/redalpha-cyber-campaigns/

65 Andres-Guerrero Saade, Sanil Choban, "RedAlpha: New Campaigns Discovered Targeting the Tibetan Community," *Recorded Future,* June 26, 2018, https://www.recordedfuture.com/redalpha-cyber-campaigns/

66 Sanil Chohan, Winnona DeSombre, Justin Grosfelt," Chinese Cyberespionage Originating from Tsinghua University Infrastructure," *Recorded Future,* August 16, 2018

67 Alexander Bowe, "China's Overseas United Front Work: Background and Implications for the United States" (Washington, D.C.: U.S.-China Economic and Security Review Commission, August 24, 2018)

68 *ibid*

69 Melanie Lee and Lucy Hornby,"Google attack puts spotlight on China's 'red" hackers," *Reuters*, January 20, 2010 https://www.reuters.com/article/us-google-china-hackers-idUSTRE60J20820100120

70 USCC, Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications technology, April 19 2018, https://docs.house.gov/meetings/IF/IF16/20180516/108301/HHRG-115-IF16-20180516-SD105-U105.pdf U.S. Department of Defense, Annual Report to Congress, "Military and Security Developments Involving the People's Republic of China," May 16, 2018, https://media.defense.gov/2018/Aug/16/2001955282/-1/-1/1/2018-CHINA-MILITARY-POWER-REPORT.PDF

71 Robert Sheldon and Joe McReynolds, "Civil-Military Integration and Cybersecurity" in China and Cybersecurity, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (Oxford, UK: Oxford Scholarship Online, 2015), 190-200.

72 Mandiant, "APT 1: Exposing Once of China's Cyber Espionage Units," (Alexandria, VA, 2013).

73 William C. Hannas, James Mulvenon and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation*,"(New York, NY: Routledge, 2013), 195-206.

74 William C. Hannas, James Mulvenon and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation*,"(New York, NY: Routledge, 2013), 204

75 It is worth noting that in the case of the United States, the practice of "naming and shaming" Chinese operators associated with industrial espionage has been met with some success. For example, the indictment of five PLA cyber operators in connection to industrial espionage operations is widely regarded as contributing to the 2015 US-China Cyber Agreement, which has notionally reduced the aggregate number of industrial espionage attacks targeting US corporations. However, it remains to be seen whether this strategy of naming and shaming can be employed writ large (e.g. in Latin America and the Caribbean).Rollins, John W; U.S.-China Cyber Agreement; *fas.org*; 16 October 2015; https://fas.org/sgp/crs/row/IN10376.pdf AND cfr.org; "indictment of PLA Officers; cfr.org May 2014; https://www.cfr.org/interactive/cyber-operations/indictment-pla-officers

76 Kvachkov, Vladimir. 2004. "Спецназ России (Russia's Special Forces)." Часть третья. Теория специальных операций (Part 3: Theory of Special Operations). 3.1. Специальный метод ведения войны. Формы геополитического противоборства (Section 3.1 Special Methods of Warfare. Forms of Geopolitical Conflict). *Военная литература* (*Military Literature*). http://militera.lib.ru/science/kvachkov_vv/index.html

77 Thomas Boghardt," Active Measures: The Russian Art of Disinformation," *International Spy Museum*, October 2006 https://spy-

museum.s3.amazonaws.com/files/back_active-measures.pdf

78 Thomas Rid, Disinformation a primer in Russian active measures and influence campaigns (Washington, DC; Select Committee on Intelligence United States Senate, 2017)

79 Valeriy Gerasimov, "The Value of Science in Prediction," *VPK*. 27 Feb 2013, http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf

80 Quote translated from original Russian. See: Valeriy Gerasimov, "The Value of Science in Prediction," *VPK*. 27 Feb 2013, http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf

81 Bartles, Charles K; "Getting Gerasimov Right." *Mi litary Review*. 28 Feb 2016.

82 Quote translated from original Russian. See: Gerasimov, Valeriy; "The Value of Science in Prediction." *VPK*. 27 Feb 2013. p. 2.

83 Mark Galeotti,"Putin's Hydra: Inside Russia's Intelligence Service," *European Council on Foreign Relations; no date* https://www.ecfr.eu/page/-/ECFR_169_ _PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf

84 *ibid*

85 Interview with the author.

86 U.S. District Court for the District of Columbia, Indictment; USA v. Russian Officials, U.S. District Court for the District of Columbia, July 13, 2018, https://www.justice.gov/file/1080281/download

87 Mark Galeotti,"Putin's Hydra: Inside Russia's Intelligence Service," *European Council on Foreign Relations; no date* https://www.ecfr.eu/page/-/ECFR_169_ _PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf

88 Quinta Jurecic, "Government Indicts FSB Officers and Two Others in Yahoo Hacking Case" *lawfareblog.com*, March 15, 2017, https://www.lawfareblog.com/government-indicts-fsb-officers-and-two-others-yahoo-hacking-case

89 Interview with the author.

90 Interview with the author. Also, see: HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group

91 Andy Greenberg, "Your Guide to Russia's Infrastructure Hacking Teams," *wired.com*, July 17, 2017, https://www.wired.com/story/russian-hacking-teams-infrastructure/

92 ibid

93 ibid

94 Andy Greenberg, "Petya Ransomware Epidemic May Be Spillover From Cyberwar." *Wired,* June, 28, 2017, https://www.wired.com/story/petya-ransomware-ukraine/

95 Andy Greenberg, "The White House Blames Russia for NotPetya, the Most Costly Cyberattack in History," *wired.com*, February 25, 2018, https://www.wired.com/story/white-house-russia-notpetya-attribution/

96 Jason Healy, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks," *Atlantic Council*, January 2012, http://www.atlanticcouncil.org/publications/issue-briefs/beyond-attribution-seeking-national-responsibility-in-cyberspace.

97 The report does not appear in the public domain in either English or Russian. Coverage of the report is available at: Pravda. 2017. "Official: Russia has one of the five world's most powerful cyber armies." *Pravda.ru*. 10 Jan.

98 US-CERT; ALERT (TA18-074A) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors; US-CERT; https://www.us-cert.gov/ncas/alerts/TA18-074A

99 Kim Zettter,"A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever, *wired.com*, January 8, 2015, https://www.wired.com/2015/01/german-steel-mill-hack-destruction/

100 Aaron F. Brantly, Nerea M. Cal and Devlin P. Winkelstein, "Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW," *Army Cyber Institute at West Point*, 2017, from https://cyberdefensereview.army.mil/Portals/6/Documents/UA%20Report%20Final%20AB.pdf

101 "China's Influence & American Interests: Promoting Constructive Vigilance," *Hoover Institution*, November 29, 2018, https://www.hoover.org/research/chinas-influence-american-interests-promoting-constructive-vigilance.

102 Carin Zissis, "Central America Caught in China-Taiwan Diplomatic Tussle, Americas Society Council of the Americas," September 11, 2018, https://www.as-coa.org/articles/central-america-caught-china-taiwan-diplomatic-tussle

103 Prasad, Binay, "A Latin American Battle: China vs. Taiwan," The Diplomat, August 19, 2017, https://thediplomat.com/2017/08/a-latin-american-battle-china-vs-taiwan/.

104 "Panama cuts ties with Taiwan in favor of China," *British Broadcasting Corporation*, June 13, 2017

105 Josh Horwitz,"Taiwan now had diplomatic relations with fewer than 20 countries," *Quartz,* May 1, 2018

106 Chris Horton, "El Salvador Recognizes China in Blow to Taiwan," *New York Times,* August 21, 2018

107 Steven Lee Myers and Chris Horton, "China tries to erase Taiwan One Ally (and Website) at a Time," *N ew York Time,* May 25, 2018

108 ibid

109 Mingjiang Li, "Rising from Within: China's Search for a Multilateral World and Its Implications for Sino-US Relations," *Global Governance* 17, no. 3 (2011): 331-51. http://www.jstor.org/stable/23033751.

110 "An Updated Draft of the Code of Conduct Distributed in the United Nations- What's New," *The NATO Cooperative Cyber Defense Centre of Excellence;*"Unpacking The Competing Russian and U.S. Cyberspace Resolutions at the United Nations," Council on Foreign Relations, October 29, 2018 United Nations, United Nations General Assembly, 73th session, 1st committee, October 22, 2018

111 The State Council, The People's Republic of China, "China's Policy Paper on Latin America and the Caribbean," November 2008, http://www.gov.cn/english/official/2008-11/05/content_1140347.htm.

112 Capt. George Gurrola, "China-Latin America Arms Sales Antagonizing the United States in the Western Hemisphere," *Military Review,* July – August 2018

113 See, for example: "Indictment of PLA Officers," *Council on Foreign Affairs,* May 2014

114 Adam Segal, Samantha Hoffman, Fergus Hanson and Tom Uren, "Hacking for Cash," Australian Strategic Policy Institute, September 25, 2018.

115 David E Sanger and Katie Benner,"U.S. Accuses Chinese Nationals of Infiltrating Corporate and Government Technology," *New York Times*, December 20, 2018, https://www.nytimes.com/2018/12/20/us/politics/us-and-other-nations-to-announce-china-crackdown.html

116 "Will the Russians Meddle in Latin American Elections?,"*Center for Strategic and International*

Studies, March 26, 2018, https://www.csis.org/events/will-russians-meddle-latin-american-elections.html

117 See, for example: https://medium.com/dfrlab/how-the-so-called-left-wing-nazis-story-spread-in-brazil-b29da8ffc77a and https://medium.com/dfrlab/electionwatch-as-colombia-votes-again-misinformation-flows-67ba41b656af

118 See, for example: https://medium.com/dfrlab/rt-and-sputnik-spin-narrative-on-guaid%C3%B3s-attempt-to-take-power-in-venezuela-cde0dc23ccd0

119 Julia Gurganus,"Russia: Playing a Geopolitical Game in Latin America," *Carnegie Endowment for International Peace*, https://carnegieendowment.org/2018/05/03/russia-playing-geopolitical-game-in-latin-america-pub-76228.

120 "APT28: New Espionage Operations Target Military and Government Organizations," *Symantec Corporation*, October 4, 2018,https://www.symantec.com/blogs/election-security/apt28-espionage-military-government

121 Robert Morgus, Jocelyn Woolbright, and Justin Sherman, "The Digital Deciders" *New America*, October 23, 2018, https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/

122 Robert Morgus, "Russia Gains and Upper Hands in the Cyber Norms Debate," *Council on Foreign Relations*, December 5, 2016, https://www.cfr.org/blog/russia-gains-upper-hand-cyber-norms-debate

123 White propaganda refers to propaganda where the artist of the propaganda is not hidden.

124 Grey propaganda refers to propaganda where the artist of the propaganda is intentionally and meticulously obfuscated so that the origin of the information is difficult to decipher.

125 Black propaganda refers to propaganda where the artist of the propaganda presents false or misleading information and purports to be on one side of the conflict, but is actually from the opposite side.

126 William Booth, "Witch Hunt," *Washington Post*, May 17, 1994, https://www.washingtonpost.com/archive/lifestyle/1994/05/17/witch-hunt/d2663dda-139e-4e3d-8e81-eb48b09f02be/?utm_term=.d26885ea3634

127 Boon Yew Ng, "Emerging from the Shadows," June 2017, https://www.accaglobal.com/content/dam/ACCA_Global/Technical/Future/pi-shadow-economy.pdf

128 Julia Gurganus,"Russia; Playing a Geopolitical Game in Latin America" *Carnegie Endowment for International Peace*, May 3, 2018, https://carnegieendowment.org/2018/05/03/russia-playing-geopolitical-game-in-latin-america-pub-76228

129 ibid

130 Boon Yew Ng, "Emerging from the Shadows," June 2017, https://www.accaglobal.com/content/dam/ACCA_Global/Technical/Future/pi-shadow-economy.pdf

131 Mark Galeotti,"Transitional Aspects of Russian Organized Crime," *Chatham House*, July 17, 2012

132 Blank, Stephen, "Cyber War and Information War á la Russe," *Carnegie Endowment for International Peace,* October 16, 2017, https://carnegieendowment.org/2017/10/16/cyber-war-and-information-war-la-russe-pub-73399

NEW AMERICA