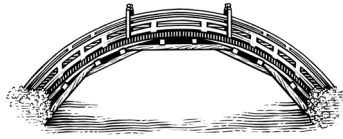


ROUNDTABLE

The Future of Cybersecurity across the Asia-Pacific



*Adam Segal*

*Valeriy Akimenko and Keir Giles*

*Daniel A. Pinkston*

*James A. Lewis*

*Benjamin Bartlett*

*Hsini Huang*

*Elina Noor*

## Introduction

Conventional security and warfare have been thoroughly mutated in the information age, and Asian nations are at the forefront of the technological developments that are driving these changes. China is investing heavily in technologies such as artificial intelligence (AI) and 5G and exporting many of its technological products regionally and globally, while limiting the cyber capabilities of foreign countries and companies within its borders. In the recent presidential elections in the United States and Taiwan, coercive tactics involving cyberattacks and information warfare were prevalent. As a result, many countries have recognized the need for new cybersecurity measures to protect the integrity of the democratic electoral process. Securing digital markets and other interests is also a priority. The Association of Southeast Asian Nations (ASEAN), for example, held a cybersecurity summit in 2018, and Singapore launched the ASEAN-Singapore Cybersecurity Centre of Excellence in October 2019 to conduct research and train personnel for responding to cybersecurity threats.

This roundtable examines the cyber policies of the United States and its key adversaries and partners in Asia from a variety of perspectives, including their offensive and defensive cyber capabilities and the military applications of these tools. Adam Segal opens the roundtable by discussing China's cyber capabilities as well as its vulnerabilities. Though Beijing can be expected to escalate its cyberattacks over the next five years, Segal notes that "CCP leaders are likely cognizant that China is vulnerable to similar attacks." He argues that this equity between strength and weakness will limit China's use of cyberattacks to military targets for fear of retaliation. For now, China presents a threat and serious challenge in the Asia-Pacific region.


Another cyberpower, Russia, has demonstrated offensive capabilities in several areas. Valeriy Akimenko and Keir Giles provide a thorough analysis of Russia's cyber activities, both offensive and defensive, as part of the country's comprehensive information warfare campaign. Most importantly, they claim that Western approaches to cybersecurity are suitable for responding to more traditional cyberthreats but insufficient "for the wider and more holistic tactics like the ones adopted by Russia." Moscow has woven cyber capabilities into the fabric of its information warfare, circumventing the defenses of its rivals with subversion and disinformation and limiting the effectiveness of countries focused on more traditional cyberdefenses.

Daniel A. Pinkston analyzes North Korea's offensive cyber capabilities. Though the country is normally considered technologically backward, Pyongyang's highly skilled hackers can produce sophisticated and

destructive cyberattacks, including bank robberies and ransomware attacks. Pinkston notes that the “methods to discover the sources of attacks are improving,” but that due to the country’s opaque nature, “attribution still takes considerable time,” which allows North Korea to strengthen its own computer network defenses. He argues that such attacks are likely to continue as long as the Kim dynasty remains in control.

James A. Lewis discusses U.S. cyber policy and the United States’ failure to keep up with the continuously morphing cybersecurity challenges that have emerged after the Cold War. Although Washington was “originally a pioneer in the use of cyber techniques,” Lewis asserts that it “now lags behind as the domain evolves beyond conventional military and espionage activities.” Across the Pacific, U.S. ally Japan is challenged by its own constitutionally imposed restrictions in the face of heightened regional threats. Benjamin Bartlett discusses Japan’s efforts to strengthen both its defensive and offensive cyber capabilities. The latter are important for disrupting adversarial attacks. Though the country’s national security policy “does not necessarily preclude further development of offensive cyber capabilities,” Bartlett contends that “it is unlikely that Japan will develop them in the near future.”

The final two essays cover the cyber policies of Taiwan and ASEAN, respectively. Hsini Huang provides an account of the administration and infrastructure governing cyber policy in Taiwan amid increasingly tense cross-strait relations. Taiwan has “chosen to play the role of regional cybersecurity facilitator in exchange for more cross-country information sharing and cooperation with its regional friends” rather than independently develop cyber capabilities. In a similarly nonconfrontational manner, ASEAN has also opted for cooperation and multilateralism in pursuit of international security. Elina Noor concludes that “ASEAN’s approach is to consolidate centrality while continuing to engage—if not, enmesh—its larger dialogue partners in cooperative efforts.” As member states will likely remain targets of cyberattacks, ASEAN will need to build collective cyber capacity at all levels.

In the near future, Russia and China will continue to pose the largest cybersecurity threats to the United States and other democracies, while North Korea also remains a menace in this domain. The asymmetric nature of cyberwarfare, as well as the range of capabilities that countries can employ, provides unique challenges to the United States and its friends and allies. “As digital technologies become central to social and commercial activity,” Lewis observes, “U.S. priorities in cyberspace will need to adjust.” Cyber policies going forward must be more comprehensive and holistic to defend the wide range of areas threatened. 

## China's Pursuit of Cyberpower

*Adam Segal*

China is one of the most active cyberspace players in the Asia-Pacific, developing and deploying cyber capacities in pursuit of its economic, political, and strategic objectives. Chinese computer network operations are conducted to strengthen the competitiveness of China's economy, accelerate the modernization of the People's Liberation Army (PLA), weaken opponents of the Chinese Communist Party (CCP), resist international pressure and foreign ideas, and offset U.S. dominance in conventional military capabilities.<sup>1</sup> Beijing is also aggressively supporting the indigenous innovation of emerging technologies that will give it new capabilities in cyberspace, especially 5G, artificial intelligence, and quantum information systems.

Although Western governments often dismiss comments from Chinese foreign ministry officials declaring China the world's biggest victim in cyberspace as distractions and diversions, Chinese officials do in fact see their cybersecurity as weak relative to the degree of threat and the capabilities they perceive from potential adversaries, the United States in particular.<sup>2</sup> As the July 2019 defense white paper puts it, "Cybersecurity remains a global challenge and poses a severe threat to China."<sup>3</sup> Perhaps the clearest evidence that the leadership sees China's situation as precarious is the speed with which it has addressed what it sees as two major sources of weakness: an underdeveloped cybersecurity regulatory framework and widespread dependence on foreign technology in critical networks. Over the last five years, China has rapidly developed new cybersecurity institutions, laws, guidelines, and standards and has moved to replace foreign suppliers with domestic counterparts.

---

ADAM SEGAL is the Ira A. Lipman Chair in Emerging Technologies and National Security and Director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations (United States). He can be reached at <asegal@cfcr.org>.

<sup>1</sup> Adam Segal, "How China Is Preparing for Cyberwar," *Christian Science Monitor*, Passcode, March 20, 2017 ~ <https://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0320/How-China-is-preparing-for-cyberwar>.

<sup>2</sup> See, for example, "Foreign Minister Geng Shuang's Daily Briefing Online on February 11, 2020," Ministry of Foreign Affairs of the People's Republic of China (PRC), February 11, 2020 ~ [https://www.fmprc.gov.cn/mfa\\_eng/xwfw\\_665399/s2510\\_665401/t1743480.shtml](https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1743480.shtml).

<sup>3</sup> State Council Information Office (PRC), *China's National Defense in the New Era* (Beijing, July 2019).

Both Chinese capabilities and vulnerabilities are likely to increase in the next five years. This combination of strengths and weaknesses means that China is primarily a cyberespionage threat to the Asia-Pacific. While the potential for Beijing to use more disruptive or destructive cyberattacks against an adversary in a regional conflict is high, especially against command-and-control systems, CCP leaders are likely cognizant that China is vulnerable to similar attacks.

This essay introduces the range of Chinese cyberoperations and the organizational structure that supports and conducts them. It also highlights significant weaknesses in Chinese cyberdefenses, such as an underdeveloped cybersecurity industry and lack of investment and expertise. The essay concludes that the combination of the Chinese economy becoming more reliant on information and communications technologies and the PLA becoming more dependent on digital systems has resulted in Chinese leaders becoming more sensitive to China's vulnerability to cyberattacks.

### *China's Cyberattacks*

The vast majority of computer attacks originating from China have targeted private-sector companies in an effort to steal intellectual property, trade secrets, and other information that could help China become more economically competitive. President Xi Jinping set a goal for China to become a "world-leading" science and technology power by 2049, and the country has significantly ramped up spending on research and development; expanded enrollment in science, technology, engineering, and mathematic disciplines at universities; and pushed specialized industrial strategies in emerging technologies, such as artificial intelligence, semiconductors, quantum research, and next-generation communication technologies.

China has also, however, directed cyber industrial espionage at high-technology and advanced manufacturing companies in the United States, Europe, Japan, and Southeast Asia.<sup>4</sup> Hackers have reportedly targeted the negotiation strategies and financial information of firms in the energy, banking, law, and pharmaceutical sectors. In an operation known as Cloud

---

<sup>4</sup> CrowdStrike Global Intelligence Team, "Putter Panda," CrowdStrike Intelligence Report, May 2, 2014 <https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf>; Mandiant, "APT 1: Exposing One of China's Cyber Espionage Units," February 19, 2013 <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report>; "What Is the Path to Checking Enemies and Achieving Victory in Informationized Wars?" *PLA Daily*, May 6, 2016 [http://www.81.cn/jmywyl/2016-05/06/content\\_7037878.htm.pdf](http://www.81.cn/jmywyl/2016-05/06/content_7037878.htm.pdf); and "Project CameraShy: Closing the Aperture on China's Unit 78020," ThreatConnect, 2015 <https://www.threatconnect.com/camerashy>.

Hopper, Chinese hackers, allegedly from the Ministry of State Security, breached at least a dozen cloud providers over several years, which allowed them access to data from hundreds of companies.<sup>5</sup> The damage this theft inflicted on the victims' economies, or, conversely, how much it helped China's economy, is unknown. The Office of the Director of National Intelligence estimated in November 2015, however, that all cyber-enabled economic espionage, not just Chinese activity, costs the U.S. economy \$400 billion per year.<sup>6</sup>

State-supported hackers also use cyberattacks to steal military secrets to accelerate the PLA's modernization and gather political information on agencies, institutions, and individuals that might have an impact on Beijing's foreign policy or threaten domestic stability. While Andrea and Marco Gilli have argued that the complexity of modern weapon systems makes it difficult to close the technological gap through cybertheft, Chinese hackers have stolen information from over two dozen U.S. Defense Department programs, including the MIM-104 Patriot surface-to-air missile system and the F-35.<sup>7</sup> Hackers recently targeted more than two dozen universities in the United States, Canada, and Southeast Asia to steal research about maritime technologies being developed for military use.<sup>8</sup>

In addition, Chinese hackers allegedly breached firms that hold large amounts of personal information, such as Anthem, Equifax, and Marriott, to allow Chinese intelligence agencies to exploit financial problems, health issues, and travel information in their attempts to recruit individuals to spy for China and to conduct counterintelligence against U.S. spies.<sup>9</sup>

---

<sup>5</sup> Rob Barry and Dustin Volz, "Ghosts in the Clouds: Inside China's Major Corporate Hack," *Wall Street Journal*, December 30, 2019 ~ <https://www.wsj.com/articles/ghosts-in-the-clouds-inside-chinas-major-corporate-hack-11577729061>.

<sup>6</sup> Commission on the Theft of American Intellectual Property, "Update to the IP Commission Report: The Theft of American Intellectual Property—Reassessments of the Challenge and United States Policy," National Bureau of Asian Research, 2017, 1 ~ [http://www.ipcommission.org/report/IP\\_Commission\\_Report\\_Update\\_2017.pdf](http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf).

<sup>7</sup> Andrea Gilli and Mauro Gilli, "Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage," *International Security* 43, no. 3 (2019): 141–89; and Matthew Pennington, "Intel Chief Warns U.S. Tech Threatened by China Cyber Theft," *Military Times*, February 3, 2015 ~ <http://www.militarytimes.com/story/military/tech/2015/02/03/intel-chief-warns-us-tech-threatened-by-china-cyber-theft/22810269>.

<sup>8</sup> Dustin Volz, "Chinese Hackers Target Universities in Pursuit of Maritime Military Secrets," *Wall Street Journal*, March 5, 2019 ~ <https://www.wsj.com/articles/chinese-hackers-target-universities-in-pursuit-of-maritime-military-secrets-11551781800>.

<sup>9</sup> David Sanger et al., "Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing," *New York Times*, December 11, 2018 ~ <https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html>; Eric Geller, "Chinese Nationals Charged for Anthem Hack, 'One of the Worst Data Breaches in History,'" *Politico*, May 9, 2019 ~ <https://www.politico.com/story/2019/05/09/chinese-hackers-anthem-data-breach-1421341>; and "Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax," U.S. Department of Justice, Press Release, February 10, 2020 ~ <https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking>.

Embassies, foreign ministries, and other government offices in Germany, India, Indonesia, Romania, South Korea, Taiwan, and other countries have been targeted, as have journalists and Tibetan and Uighur activists. Government hackers, for example, broke into telecommunications operators in Turkey, Kazakhstan, India, Thailand, and Malaysia to track Uighurs traveling in Central and Southeast Asia.<sup>10</sup>

Responsibility for conducting cyberoperations is distributed across Chinese intelligence agencies and the PLA. In December 2015, Beijing established the Strategic Support Force, whose duties include electronic warfare, cyberoffense and cyberdefense, and psychological warfare.<sup>11</sup> Industrial espionage using cyber methods has primarily shifted to hacking groups connected to the Ministry of State Security.<sup>12</sup> While PLA cyberforces spread across the Third and Fourth Departments will still conduct some espionage operations (with the Third Department of the General Staff managing at least twelve operational bureaus and three research institutes), the purpose of the Strategic Support Forces is in part to allow them to concentrate on cyberoperations in support of military goals.

Cyberattacks appear to be an important part of Chinese planning for any regional conflict. PLA military analysts often write of using cyberattacks against command-and-control computers, as well as satellite and communication networks, in a conflict's beginning stages to seize information dominance.<sup>13</sup> For example, *The Science of Military Strategy*, a generally authoritative study of the PLA's strategic thought published by the Chinese Academy of Military Science, argues that "the side holding network warfare superiority can adopt network warfare to cause dysfunction in the adversary's command system, loss of control over his operational forces and activities, and incapacitation or failure of weapons and equipment—and thus seize the initiative within military confrontation."<sup>14</sup>

---

<sup>10</sup> Jack Stubbs, "China Hacked Asian Telcos to Spy on Uighur Travelers," Reuters, September 5, 2019 ~ <https://www.reuters.com/article/us-china-cyber-ughurs/china-hacked-asian-telcos-to-spy-on-ughur-travelers-sources-idUSKCN1VQ1A5>.

<sup>11</sup> John Costello, "China's Strategic Support Force: A Force for a New Era," testimony to the U.S.-China Economic and Security Review Commission, Washington, D.C., February 15, 2018 ~ [http://www.uscc.gov/sites/default/files/Costello\\_Written%20Testimony.pdf](http://www.uscc.gov/sites/default/files/Costello_Written%20Testimony.pdf).

<sup>12</sup> Catalin Cimpanu, "APT-Doxing Group Exposes APT17 as Jinan Bureau of China's Security Ministry," ZDNet, July 24, 2019 ~ <https://www.zdnet.com/article/apt-doxing-group-expose-apt17-as-jinan-bureau-of-chinas-security-ministry>.

<sup>13</sup> "What Is the Path to Checking Enemies and Achieving Victory in Informationized Wars?"

<sup>14</sup> Peng Guangqian, ed., *The Science of Military Strategy*, 3rd ed. (Beijing: Military Science Press, 2013), 189.

Chinese military writings also suggest that cyberattacks can have a strategic deterrent effect given the United States' dependence on banking, telecommunications, and other critical networks.<sup>15</sup> A highly disruptive or destructive attack on these networks might reduce the possibility that the United States will become involved in a regional conflict. Some Chinese intrusions into critical infrastructure may intentionally leave evidence behind to act as a warning that the U.S. homeland might not be immune to attack in the case of a conflict over Taiwan or the South China Sea.

### *Chinese Cyberdefense*

While its cyber operators are very active in the networks of others, Chinese military analysts are clearly worried that China itself could be the victim of cyberattacks. Previously, the PLA, dependent on landline and sea-based fiber optics and mainland-based servers, routers, and transmission switches, appeared relatively insulated from cyberattacks.<sup>16</sup> But as the PLA modernizes it has become more reliant on information technology in its military operations. Around 2010, top military and civilian leaders recognized that China's exposure to cyberattacks had substantially increased, and a 2015 RAND study noted that China's integrated air-defense systems; maritime intelligence, surveillance, and reconnaissance systems; and dual-use networks would be "obvious targets" for cyberoperations in the event of a conflict.<sup>17</sup>

Chinese policymakers' concerns about cybersecurity are driven both by the increasing dependence of the economy on information technology and by significant technological and regulatory vulnerabilities. China's digital economy is now the largest in the world, reaching 31.3 trillion yuan (approximately \$4.6 trillion) and accounting for 35% of GDP in 2018.

---

<sup>15</sup> Jia Daojin and Chang Wei, "The Three Development Stages of Informationized Wars," *Study Times*, May 30, 2016 ~ [http://www.cctb.net/llyj/llyj/llwz/201606/t20160601\\_342024.htm](http://www.cctb.net/llyj/llyj/llwz/201606/t20160601_342024.htm).

<sup>16</sup> Adam Segal, "U.S. Offensive Cyber Operations in a China-U.S. Military Confrontation," in *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, ed. Herb Lin and Amy Zegart (Washington, D.C.: Brookings Press, 2019).

<sup>17</sup> Fiona Cunningham, "Maximizing Leverage: Explaining China's Force Postures in Limited Wars" (PhD diss., Massachusetts Institute of Technology, September 2018); and Eric Heginbotham, *U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power 1996-2017* (Santa Monica: RAND Corporation, 2015), 259-83.



The total value of online transactions in China exceeded \$1.5 trillion in 2019, compared to \$600 billion in the United States.<sup>18</sup>

Despite the growing importance of information and communications technologies to the economy, there is a serious lack of cybersecurity investment and expertise. A 2019 report estimates that Chinese companies spend around \$7.3 billion on cybersecurity annually, about nine times less than the U.S. private sector.<sup>19</sup> Moreover, the country faces a talent gap, with estimates of workforce shortfalls reaching 1.4 million by 2020, up from 700,000 in 2019.<sup>20</sup> While the revenue of the domestic cybersecurity industry is growing faster than the global average, Chinese analysts argue that the country's firms lack core technologies and innovation capacity.<sup>21</sup>

Even before National Security Agency contractor Edward Snowden's revelations in 2013 about U.S. intelligence agency activities, Chinese leaders believed that dependence on foreign technology was a security threat. Snowden's revelations re-energized efforts to promote "secure and controllable" technology and encourage its adoption in sensitive sectors to guard against spying by foreign products. In 2019 the CCP's Central Office, for example, ordered every government office and public institution to remove all foreign software and hardware within three years.<sup>22</sup>

The Chinese leadership has also used the intelligence disclosures to consolidate its cyber policy authorities and accelerate policy development. After years of inertia during which cyber policy was fragmented among the Ministry of Industry and Information Technology, the Ministry of State Security, the Ministry of Public Security, the PLA, and others, Xi established a new agency, the Cyberspace Administration of China, and gave it responsibility for controlling online content, bolstering cybersecurity, and developing the digital economy. Xi also now chairs the newly established

---

<sup>18</sup> "China's E-Commerce Trade Volume Reaches 31.63 Trillion Yuan in 2018," Xinhua, May 28, 2019 [~ https://www.chinadaily.com.cn/a/201905/28/WS55cecfadaa3104842260be4b1.html](https://www.chinadaily.com.cn/a/201905/28/WS55cecfadaa3104842260be4b1.html); Lambert Bu et al., "China Digital Consumer Trends 2019: Discovering the Next Wave of Growth," McKinsey Digital, September 2019 [~ https://www.mckinsey.com/~media/mckinsey/featured%20insights/china/china%20digital%20consumer%20trends%20in%202019/china-digital-consumer-trends-in-2019.ashx](https://www.mckinsey.com/~media/mckinsey/featured%20insights/china/china%20digital%20consumer%20trends%20in%202019/china-digital-consumer-trends-in-2019.ashx).

<sup>19</sup> Liane Ferreira, "Cybersecurity in China Is a Business Worth \$8.9 Billion," CGTN, September 19, 2019 [~ https://news.cgtn.com/news/2019-09-19/Cybersecurity-in-China-is-a-business-worth-8-9-billion-K6RRVvwmGU/index.html](https://news.cgtn.com/news/2019-09-19/Cybersecurity-in-China-is-a-business-worth-8-9-billion-K6RRVvwmGU/index.html).

<sup>20</sup> "China's Cyberspace Security Talent Gap Is Large," Xinhua, September 18, 2019 [~ http://www.chinanews.com/gn/2019/09-18/8959259.shtml](http://www.chinanews.com/gn/2019/09-18/8959259.shtml).

<sup>21</sup> "China's Cybersecurity Market to Expand 20% in 2019," *China Daily*, December 10, 2019 [~ https://www.chinadaily.com.cn/a/201912/10/WS55def5812a310cf3e3557d39e.html](https://www.chinadaily.com.cn/a/201912/10/WS55def5812a310cf3e3557d39e.html).

<sup>22</sup> Yuan Yang and Nian Liu, "Beijing Orders State Offices to Replace Foreign PCs and Software," *Financial Times*, December 8, 2019 [~ https://www.ft.com/content/b55fc6ee-1787-11ea-8d73-6303645ac406](https://www.ft.com/content/b55fc6ee-1787-11ea-8d73-6303645ac406).

Central Commission for Cybersecurity and Informatization to drive policy from the top. Additionally, over the last five years the Chinese government has developed an interlocking framework of laws, regulations, and standards designed to increase cybersecurity and data integrity.<sup>23</sup> In particular, the National Security Law, Counterterrorism Law, Multi-Level Protection System, and Cybersecurity Law include provisions for online content management, the protection of critical information infrastructure, security reviews for network products and services, and measures that require data localization.

### *Conclusion*

In February 2014, President Xi Jinping declared that there is “no national security without cybersecurity,” and since then cybersecurity has been a national priority for China.<sup>24</sup> Despite Beijing’s active use of computer network operations to achieve its economic, political, and strategic goals, Chinese leaders recognize that they remain vulnerable to the same types of attacks. Over the last five years, they thus have dedicated significant attention to bolstering both cyberoffense and cyberdefense, while also funding large-scale investments in artificial intelligence and quantum information systems that will give China new abilities to project power in cyberspace.

This balance of strengths and weaknesses might convince the CCP to exercise restraint in a conflict, limiting attacks to military targets. There are real risks, however, that even limited cyberattacks could cause an incident to escalate rapidly and spill over into physical conflict. For the Asia-Pacific, China will remain a significant power in cyberspace, posing a serious intelligence and military challenge. ◆

---

<sup>23</sup> Paul Triolo et al., “China’s Cybersecurity Law One Year On,” *New America*, November 30, 2017 ~ <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year>.

<sup>24</sup> “Xi Jinping: China Must Evolve from a Large Internet Nation to a Powerful Internet Nation,” *Xinhua*, February 27, 2014.

## Russia's Cyber and Information Warfare

*Valeriy Akimenko and Keir Giles*

Russia's exercise of cyberpower forms an integral part of the far broader concept known as information warfare. The key principle of the Russian approach to information warfare, including cyber activities, is that information is the most important object of operations, independent of the channel through which it is transmitted. The aim is to control—or weaponize—information in whatever form it takes. Thus, “cyber” in particular is just a technical representation of information. In short, in Russia's comprehensive approach to the information domain, cyber is not a stand-alone discipline.

This principle underpins all Russian efforts to extract, exfiltrate, manipulate, distort, or insert information. Alongside cyber activities, the channels available for doing this are as diverse as using fake or real news media to plant disinformation, trolling campaigns, issuing official government statements, giving speeches at rallies or demonstrations, posting defamatory online videos, and sending direct text messages. Russian information activities are not limited to cyberspace. Rather than using the term “cyberspace,” Russian officials refer to “information space,” which includes both computer and human information processing.<sup>1</sup>

This essay starts with an explanation of the terminological, doctrinal, and practical distinguishing features of Russian cyber activities as part of information warfare. It goes on to look at a number of Russia's agencies and capabilities involved in the prosecution of cyber activities, both offensive and defensive. In conclusion, the essay emphasizes the main implication of this distinctive approach: the need for nations to prepare a broad range of defenses against Russia's holistic approach to offensive cyber, information warfare, and other forms of hostile online activity.

---

**VALERIY AKIMENKO** is a Senior Research Associate at the Conflict Studies Research Centre (United Kingdom). He can be reached at <valeriy.akimenko@conflictstudies.org.uk>.

**KEIR GILES** is Director of the Conflict Studies Research Centre and a Senior Consulting Fellow of the Russia and Eurasia Programme at Chatham House (United Kingdom). He can be reached at <keir.giles@conflictstudies.org.uk>.

<sup>1</sup> Keir Giles, “Handbook of Russian Information Warfare,” NATO Defense College, Fellowship Monograph Series, no. 9, November 2016, 69.

## *Terminology, Strategy, and Doctrine*

Russia's approach to defining a doctrine for computer network operations is determined by the core concept of "information confrontation" (or "information war") and includes all hostile activities using information as a tool, target, or domain of operations. The concept implies computer network operations alongside disciplines such as psychological operations, strategic communications, influence, intelligence, *maskirovka* (military deception), disinformation, electronic warfare, debilitation of communications, degradation of navigation support, and destruction of enemy computer capabilities. The aim is "to influence the perception and behavior of the enemy, population, and international community."<sup>2</sup>

Russia sees superiority in this broad application of information warfare as a key enabler for victory in current and future conflicts:

Wars will be resolved by a skillful combination of military, nonmilitary, and special nonviolent measures that will be put through by a variety of forms and methods and a blend of political, economic, informational, technological, and environmental measures, primarily by taking advantage of information superiority. Information warfare in the new conditions will be the starting point of every action now called the new type of warfare, or hybrid war, in which broad use will be made of the mass media and, where feasible, global computer networks (blogs, various social networks, and other resources).<sup>3</sup>

*Russian cyber terminology.* "Cyber" as a separate function or domain is not a Russian concept.<sup>4</sup> The delineation of activities in the cyber domain from other activities processing, attacking, disrupting, or stealing information is seen as artificial. The phrase "cyber warfare" in Russian writing is used to describe foreign concepts and activities. The closest that Russian thinking comes to separating out computer network operations from other activities is the division between the information-technological and information-psychological domains, the two main strands of information warfare.<sup>5</sup>

---

<sup>2</sup> A.J.C. Selhorst, "Russia's Perception Warfare," *Militaire Spectator* 185, no. 4 (2016): 151.

<sup>3</sup> S.G. Chekinov and S.A. Bogdanov, "Prognozirovaniye kharaktera i soderzhaniya voyn budushchego: Problemy i suzhdeniya" [Forecasting the Nature and Content of Wars of the Future: Problems and Assessments], *Voennaya mysl*, no. 10 (2015): 44–45.

<sup>4</sup> T.L. Thomas, "Information Security Thinking: A Comparison of U.S., Russian, and Chinese Concepts," Foreign Military Studies Office, July 2001 ~ <http://fmso.leavenworth.army.mil/documents/infosecu.htm>.

<sup>5</sup> V. Kvachkov, "Spetsnaz Rossii" [Russia's Special Operations Forces], *Voyennaya literatura*, 2004 ~ [http://militera.lib.ru/science/kvachkov\\_vv/index.html](http://militera.lib.ru/science/kvachkov_vv/index.html).

Cyber activities, however, do not map directly to the information-technological domain: as an integral part of information warfare overall, they are also inherent in information-psychological operations. Importantly, moreover, information-psychological operations are undertaken “permanently”—regardless of the notional state of cooperation or hostility between the opposing sides. Multiple senior Russian officials have emphasized that open conflict need not have been declared for hostile activity in the information space to begin.<sup>6</sup>

*Information security doctrine.* It follows that Russia does not have publicly released national strategies relating specifically to its cyber activities. The closest approximation is the Information Security Doctrine. The most recent iteration of this document, approved in December 2016, follows a line adopted in previous strategic documents that portrays Russia as under constant information attack. Rhetorically, the text resembles the National Security Strategy adopted in December 2015, which signaled a heightened sense of threat toward Russia. The information space in this document is defined more broadly than in the previous version of the same doctrine from 2000. “Informatization” is a key term, which refers to social, economic, and technical processes for adopting and expanding information technology nationwide and securing access to information resources. This change indicates recognition of the information domain’s role in technological development and, most importantly, regards this domain as a tool to change the fabric of society. The Information Security Doctrine describes how this tool is used in the interests of Russia’s national security and calls for an increased role for internet and information security management as well as for the domestic production of information technology.<sup>7</sup>

### *Agencies, Capabilities, and Control*

*Opaque chain of command.* The structures and organizations involved in prosecuting information warfare and thus cyber activities from within Russia are highly opaque. Little open-source information about them is reliable.

---

<sup>6</sup> See, for example, comments by deputy chief of the General Staff Lieutenant General Aleksandr Burutin, interviewed by Interfax-AVN, January 31, 2008.

<sup>7</sup> Katri Pynnöniemi and Martti J. Kari, “Russia’s New Information Security Doctrine: Guarding a Besieged Cyber Fortress,” Finnish Institute of International Affairs (FIIA), FIIA Comment, December 2016 ≈ [https://www.fiaa.fi/wp-content/uploads/2017/04/comment26\\_russia\\_s\\_new\\_information\\_security\\_doctrine.pdf](https://www.fiaa.fi/wp-content/uploads/2017/04/comment26_russia_s_new_information_security_doctrine.pdf).

Information warfare efforts appear to be duplicated through parallel structures, such as the Federal Security Service (FSB) and the Russian military intelligence service (known as GU or GRU). It is the GRU, however, that has rapidly emerged as the prime suspect in the conduct of cyberattacks (and psychological operations over the internet). These have ranged from hacking Democratic Party IT systems in the U.S. presidential election in 2016, to deploying a highly disruptive computer virus dubbed NotPetya in 2017, to the Sandworm cyberattack against Ukraine in 2014.<sup>8</sup> The United Kingdom's National Cyber Security Centre has attributed at least ten cyber campaigns to the GRU between 2015 and 2018.<sup>9</sup> In addition to governments, the targets included various international authorities over inquiries politically detrimental to Russian interests. Operations involved the deployment of teams in the field to gain access to hard-target computers, accounts, and systems.<sup>10</sup> Information leaked into the public domain through proxies (such as Guccifer 2.0) or like-minded external parties (such as WikiLeaks) has been amplified by mainstream media, both from Russia (via outlets such as RT and Sputnik) and even from target nations.<sup>11</sup>

*Information Operations Troops.* Russia's Information Operations Troops (Voyska Informatsionnykh Operatsiy or VIO) were announced as part of its order of battle in February 2017. Their role has been widely misinterpreted in Western media as providing primarily cyberforce capabilities. Instead, their purpose appears to be in keeping with the broad Russian definition of information activities. There is little information publicly available on their operating model, size, or equipment. It is thought, however, that their main function is to apply a combination of traditional propaganda, electronic warfare, disinformation, psychological manipulation, and strategic communications.<sup>12</sup>

---

<sup>8</sup> Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Doubleday, 2019).

<sup>9</sup> "UK Exposes Russian Cyber Attacks," UK Government, Press Release, October 4, 2018 ~ <https://www.gov.uk/government/news/uk-exposes-russian-cyber-attacks>.

<sup>10</sup> "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations," U.S. Department of Justice, Press Release, October 4, 2018 ~ <https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and>.

<sup>11</sup> U.S. Department of Justice, "GRU Indictment," July 13, 2018 ~ <https://www.justice.gov/file/1080281/download>.

<sup>12</sup> Lionel N Beehner et al., "The Fog of Russian Information Warfare," in *Perceptions Are Reality: Historical Case Studies of Information Operations in Large-Scale Combat Operations*, ed. Mark D. Vertuli and Bradley S. Loudon (Fort Leavenworth: Army University Press, 2018), 40–43 ~ <https://www.armyupress.army.mil/Portals/7/combats-studies-institute/csi-books/perceptions-are-reality-lsco-volume-7.pdf>.

*Cyber: State, nonstate, or criminal?* In cyberoperations, as in the physical domain of warfare, Russia benefits from deliberate blurring of the lines between state and nonstate actors. In addition to its own cyber experts, evidence shows that the FSB recruits hackers externally, including from the criminal world. For at least the last decade, the Kremlin has sourced technology and even intelligence information from cybercrime groups to enhance Russia's cyber capabilities. In addition to organized groups, an individual's technical proficiency in cybercrime attracts the attention of the Russian intelligence services, which may then induce or coerce the individual to work for the state.<sup>13</sup>

### *National Resilience and Cybersecurity*

*Russian views on cyberspace.* Russian views on the nature, potential, and use of cyberspace differ significantly from the Western consensus. In particular, in keeping with its historical suspicion of information and opinions from abroad, the Russian state has deep concerns about the principle of uncontrolled information exchange in cyberspace and the presumption that national borders are of limited relevance in that space. The circulation of information that poses a perceived threat to society or the state and sovereignty of the "national internet" is a key security concern for Russia. For example, the authorities consider that Russian political protests, such as over the results of parliamentary and presidential elections, arise at least in part because of a cyber or information warfare campaign against Russia.

*The "sovereign RuNet" campaign.* The most dramatic and high-profile expression of Russia's focus on national resilience has been efforts to enable the Russian internet (known domestically as RuNet) to function independently from the rest of the world in what is referred to as the "sovereign RuNet." In December 2019 the Russian government claimed to have successfully tested disconnection of the RuNet from the global internet. The government stated that it had tested several disconnection scenarios, including a simulation of a state-backed cyberattack and a

---

<sup>13</sup> Cory Bennett, "Kremlin's Ties to Russian Cyber Gangs Sow U.S. Concerns," *Hill*, October 11, 2015 <http://thehill.com/policy/cybersecurity/256573-kremlins-ties-russian-cyber-gangs-sow-us-concerns>; and Mike Eckel, "More Glimpses of How Russian Intelligence Utilized Hackers Revealed in U.S. Trial," *Radio Free Europe/Radio Liberty*, March 16, 2020 <https://www.rferl.org/a/more-glimpses-of-how-russian-intelligence-utilized-hackers-revealed-in-u-s-trial/30491223.html>.

response described as “combat mode.”<sup>14</sup> The tests involved both government agencies and telecommunications companies, including local internet service providers (ISPs). The scenarios were designed to check that Russian internet services could continue to function when isolated from the global internet infrastructure, which would essentially turn the RuNet into a vast intranet. Over half of the simulated cyberattacks, however, successfully penetrated Russia’s cyberdefenses.<sup>15</sup>

The tests were a culmination of concerted efforts, carried out over years, toward sovereign RuNet capability. This capability includes mechanisms to re-route traffic through exchange points exclusively managed or approved by the Russian telecommunications regulator so that no traffic is routed outside the country where it could be vulnerable to interception.

Critics argue that in addition to its cybersecurity aims, the legislation could facilitate greater surveillance and censorship. For example, the government has reportedly stepped up efforts to apply deep packet inspection (put simply, the ability to read internet traffic in detail), partly in response to repeated—and largely unsuccessful—efforts to ban the use of encrypted communications systems such as the messaging app Telegram.<sup>16</sup> Other regulatory efforts pursue this as well, such as the data localization requirement for corporations (like Apple, for example) and social media platforms to store Russian users’ data within Russia’s borders.

While the sovereign RuNet concept symbolizes the Russian government’s commitment to technological independence, especially from the West, its practical goal is straightforward: a controllable, isolatable, defensible, domestic internet.

*SORM and other surveillance.* Online activity within Russia is monitored by default by the Sistema Operativno-Rozysknykh Meropriyatiy (Operational Investigative Measures System, or SORM). SORM is a well-documented overt system for recording internet use through Russian ISPs and enabling access to this monitoring to a range of Russian

---

<sup>14</sup> Justin Sherman, “Russia’s Domestic Internet Is a Threat to the Global Internet,” Slate, October 24, 2019 ~ <https://slate.com/technology/2019/10/russia-runet-disconnection-domestic-internet.html>.

<sup>15</sup> Angelina Krechetova and Ekaterina Kinyakina, “Minkomsvyazi podvelo itogi pervykh ucheniy po zakonu o ‘suverennom RuNete’” [Communications Ministry Sums Up the Results of the First Exercise in Line with the Law on the “Sovereign RuNet”], *Vedomosti*, December 23, 2019 ~ <https://www.vedomosti.ru/technology/news/2019/12/23/819484-suverennom-runete>.

<sup>16</sup> “Russia Starts Rolling Out DPI Filtration Tech That Might Finally Block Telegram,” Meduza, September 27, 2019 ~ <https://meduza.io/en/news/2019/09/27/russia-starts-rolling-out-dpi-filtration-tech-that-might-finally-block-telegram>.



law-enforcement bodies.<sup>17</sup> The system captures metadata and content from mobile and landline calls (SORM-1), internet traffic (SORM-2), and all other media (SORM-3). In theory, the retrieval of intercepted data requires a court order, but in practice this requirement is unlikely to inconvenience the security services.

The Russian state's surveillance powers have been further enhanced in recent years by progressively more stringent laws and measures ostensibly aimed at data protection and counterterrorism. Laws now in force oblige ISPs to store all user transactions for up to six months and the relevant metadata for up to three years. Captured user information includes the text of all written communications and an archive of all video and audio communications; the user's exact home address and passport details; lists of relatives, friends, and contacts; related social media accounts; languages spoken; and records of all e-payments. This information, along with encryption codes, must be provided to the security services on demand.

*Anti-cybercrime agencies.* In order to protect their online communications, Russian state officials are instructed to use a closed government network, RSNet. Each employee has his or her own secure work email account that can only be accessed from a special IP address using a designated computer, though rollout of the system is reportedly patchy.<sup>18</sup> A range of government agencies are assigned cybersecurity tasks: for example, Department K (Upravleniye K), which operates under the Ministry of the Interior, is responsible for generic computer crime.<sup>19</sup> The FSB has been tasked with defense against attacks on government systems and, in particular, critical national infrastructure. In January 2013, President Vladimir Putin ordered the FSB to create a state system to detect, provide early warning, and deal with the aftermath of computer attacks. Known as GosSOPKA (Gosudarstvennaya Sistema Obnaruzheniya, Preduprezhdeniya i Likvidatsii Posledstviy Kompyuternykh Atak),<sup>20</sup> the intent of the system is to shield all government information resources within a single system

---

<sup>17</sup> Keir Giles and Kim Hartmann, "Socio-Political Effects of Active Cyber Defence Measures," in *6th International Conference on Cyber Conflict: Proceedings*, ed. P. Brangetto, M. Maybaum, and J. Stinissen (Tallinn: NATO CCD COE Publications, 2014), 23–38.

<sup>18</sup> Daniil Turovsky, "Moscow's Cyber-Defense: How the Russian Government Plans to Protect the Country from the Coming Cyberwar," *Meduza*, July 19, 2017 ~ <https://meduza.io/en/feature/2017/07/19/moscow-s-cyber-defense>.

<sup>19</sup> Kimberly Lukin, "Russian Cyberwarfare Taxonomy and Cybersecurity Contradictions between Russia and the EU: An Analysis of Management, Strategies, Standards and Legal Aspects," in *National Security: Breakthroughs in Research and Practice*, vol. 1 (Hershey: IGI Global, 2019), 408–42.

<sup>20</sup> Dmitriy Kuznetsov, "GosSOPKA: Chto takoye, zachem nuzhna i kak ustroyena" [GosSOPKA: What Is It, Why Is It Needed and How Is It Arranged], *Anti-Malware.ru*, April 2, 2019 ~ [https://www.anti-malware.ru/analytics/Technology\\_Analysis/gossopka-what-is-it-how-it-works](https://www.anti-malware.ru/analytics/Technology_Analysis/gossopka-what-is-it-how-it-works).

that has a constantly monitored perimeter and to extend this to all critical infrastructure. It is described as a public-private partnership with a concentration of prevention and response competencies.

A range of computer emergency response teams are nominally operational in Russia to react to cyber incidents in both government and the private sector. State research institutes and commercial companies are also involved in work on cyberdefense. It has been officially stated, however, that cyber fraud in particular “goes virtually unsolved” in Russia.<sup>21</sup>

### *Offensive Cyber: A Holistic Approach*

The Western approach to cyberdefense has typically focused on technical responses to technical threats. This approach is entirely apt for persistent or background threats, but is not always sufficient for the wider and more holistic tactics like the ones adopted by Russia. In other words, Russia’s counterparts may be prepared to face “pure” cyber challenges, but the capabilities and intentions embraced by Russia show that they also need to be prepared for an information war where these are seamlessly melded with disinformation, subversion, and kinetic and electronic warfare effects, with highly ambitious aims up to and including regime change.


Recent practices indicate that the broad nature of the Russian information warfare concept can include real-world operations designed to create information effects as well as the reverse, with seamless integration of cyber concepts and operations throughout. These activities are augmented by the ubiquitous activities of trolls (online profiles run by humans) and bots (those run by automated processes). For Russia, cyber activities in the broad sense are critical to offensive disinformation campaigns, which have strategic effects even if the cyber component is very limited. The problem of propaganda and disinformation—as subsets of a much broader Russian information campaign—is at least as important as the traditional (if often misguided) “cyber Pearl Harbor” notion of crippling cyberattacks on critical national infrastructure.

Russia’s increasingly overt use of hostile cyber and information campaigning, as exemplified during the 2016 U.S. presidential election,<sup>22</sup> follows a trend observed both in the United States and elsewhere, which


---

<sup>21</sup> Statement by the prosecutor-general Igor Krasnov on Ekho Moskvyy radio (Russian), March 17, 2020 ≈ <https://echo.msk.ru/news/2607440-echo.html>.

<sup>22</sup> “Report on Russian Active Measures,” U.S. Congress House of Representatives, Permanent Select Committee on Intelligence, March 22, 2018 ≈ <https://www.hsdl.org/?abstract&did=809811>.

is that “Russia is assuming a more assertive cyber posture based on its willingness to target critical infrastructure systems and conduct espionage operations even when detected and under increased public scrutiny.”<sup>23</sup> Russia thus has the capability in place to operate in all dimensions of cyberspace—from physical infrastructure to the sociocultural layer, and from the electromagnetic spectrum to the arena of public opinion both at home and abroad. The result of this holistic approach to information confrontation, including cyber, has also been clearly demonstrated in campaigns against the United States, not limited to attacks on its democratic system. Any nation that constructs its defenses only against “pure cyber” hostile activities, neglecting the threat of other forms of information campaigns, is entirely unprepared for the forms of attack that Russia is ready to deploy. 

---

<sup>23</sup> James R. Clapper, “Worldwide Threat Assessment of the US Intelligence Community,” statement to the U.S. Senate Armed Services Committee, Washington, D.C., February 9, 2016  [http://www.armed-services.senate.gov/imo/media/doc/Clapper\\_02-09-16.pdf](http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf).

## North Korea's Objectives and Activities in Cyberspace

*Daniel A. Pinkston*

The Democratic People's Republic of Korea (DPRK, or North Korea) is a centralized, authoritarian, personalistic dictatorship under the third generation of the Kim dynasty. Despite having suffered a terrible famine and long-term economic deprivation, North Korea has developed its cyber capabilities into a significant and persistent threat and gained notoriety for its past hacking activities, most remarkably the attacks against Sony Pictures Entertainment, cryptocurrency and bank heists, and ransomware attacks. Pyongyang has seriously cultivated its cyber capabilities since the mid-1990s and now possesses the full range of capabilities to conduct computer network operations, including computer network attack, computer network exploitation, computer network defense, influence operations (military information support operations, information operations, and propaganda), cybercrime, cyberterrorism, and probably physical cyberweapons.<sup>1</sup>

Kim Jong-il recognized the value of cyber capabilities in the 1990s, which gave North Korea ample time to recruit and train human resources and invest in institutions to develop and sustain the country's assets in cyberspace.<sup>2</sup> North Korea's priorities in the realm of information and communications technology (ICT) are embedded in the leadership's national strategy, which is composed of two main parts: national security and economic development. This is no different from any other state, except that the type of regime, division of the two Koreas, and external environment present a number of threats, challenges, and opportunities that affect North Korea's cyber posture and activities.

This essay seeks to put North Korea's cyber activities in the context of the leadership's political goals and the country's science and technology policy.

---

**DANIEL A. PINKSTON** is a Lecturer in International Relations with Troy University (at U.S. military installations in South Korea and Japan). Previously he was the Northeast Asia deputy project director for the International Crisis Group in Seoul. He can be reached at <dapinkston@troy.edu>.

<sup>1</sup> For further background on these capabilities, see Daniel A. Pinkston, "North Korean Cyber Threats," in *Confronting an "Axis of Cyber"?* ed. Fabio Rugge (Milano: Ledizioni LediPublishing, 2018), 89–119.

<sup>2</sup> Even before succeeding his father in 1994, Kim Jong-il had referenced science and technology as a pillar of ideology and as a means to raise economic productivity. See Kim Jong-il, *On the Juche Idea: Treatise Sent to the National Seminar on the Juche Idea Held to Mark the 70th Birthday of the Great Leader Comrade Kim Il Sung, 31 March 1982* (Pyongyang: Foreign Languages Publishing House, 1982); and Kim Jong-il, "Let Us Firmly Equip Ourselves with the Theory of Juche-Oriented Socialist Economic Management," letter, July 1, 1991.

After explaining Pyongyang's national strategy and the role of cyber, this essay will turn to the regime's demand for hard currency and the persistent attraction of cybercrime. While North Korean hackers successfully have demonstrated their skills, they also present a dilemma for the leadership. Who is to monitor these expert technicians? To help mitigate this problem, the regime has replicated its "coup-proofing" institutional design found in the security apparatus and the military. Finally, the essay speculates that in the future North Korea might try to employ its cyber capabilities more extensively in the realm of influence operations.

### *Cyber Capabilities in North Korean Strategy*

When North Korea's cyber infrastructure took off in the mid-1990s, the country's survival was at stake. The economic shock and famine in the wake of the Soviet Union's collapse and the death of founding leader Kim Il-sung led Kim Jong-il to adopt military-first politics that served as a type of public administration and crisis management system for regime survival.<sup>3</sup> Kim Jong-il emphasized national security and military affairs with the aim of achieving a strong and prosperous country.<sup>4</sup> To accomplish this goal, Kim Jong-il envisioned North Korea being strong in three dimensions: ideology and politics, military power, and the economy. He stated that "science and technology is a strong impetus for building a strong and prosperous country," while emphasizing "science as an important part of his strategic line to build a powerful socialist state."<sup>5</sup>

Kim Jong-un has continued his father's emphasis on science and technology. Under his rule, North Korea has been following the *pyongjin* line, which seeks the simultaneous development of nuclear technology (both military and civilian) and the economy. After Kim declared in his 2018 New Year's address that North Korea had "perfected the national nuclear forces," Pyongyang—at least nominally—shifted its emphasis to the economic portion of *pyongjin*.<sup>6</sup> Science and technology, including ICT, are considered critical foundations in the leadership's effort to boost economic

<sup>3</sup> Kim Chol-u, *Songun Politics of Kim Jong Il* (Pyongyang: Foreign Languages Publishing House, 2008); and Kim Hui-bong, *Songunjongch'i mundap* [Military-First Politics: Questions and Answers] (Pyongyang: Pyongyang Publishing Company, 2008).

<sup>4</sup> Kim Jae-ho, *Kim Jong-il kangsongdaeguk konsolchollyak* [Kim Jong-il's Strategy to Build a Strong and Prosperous State] (Pyongyang: Pyongyang Publishing Company, 2000); and Ko Kyong-min, *Pukhan'ui IT chollyak* [North Korea's IT Strategy] (Seoul: Communication Books, 2004), 27–36.

<sup>5</sup> Ko, *Pukhan'ui IT chollyak*, 31.

<sup>6</sup> "Kim Jong Un Makes New Year Address," Korean Central News Agency (KCNA), January 1, 2018 ∞ <https://kcnawatch.org/newstream/1546586950-531763259/kim-jong-un-makes-new-year-address>.

output and efficiency.<sup>7</sup> In his report to the 7th Party Congress in May 2016, Kim called for breakthroughs in advanced technologies such as information technology, nanotechnology, biotechnology, new materials technology, new energy technology, and space technology.<sup>8</sup> North Korea's current five-year economic plan (2016–20) calls on science and information technology as instruments to normalize production in strategic industries.<sup>9</sup> To foster the development of human resources in ICT, North Korean schools now introduce ICT into the curriculum in the fourth grade of elementary school.<sup>10</sup> Kim Il-sung University and Kim Chaek University of Technology are the top universities for training computer scientists and technicians. In 2010 the latter began a distance learning program, and now several other colleges and universities offer similar services.<sup>11</sup>

### *The Role of Cybercrime*

While North Korea's ICT advancements have made economic production more efficient, they have also increased efficiencies in other areas such as politics and national defense. North Korean hackers have been responsible for a number of cybercrimes, including bank robberies that have reportedly brought in as much as \$2 billion and possibly over \$500 million in cryptocurrencies.<sup>12</sup> The 2016 attack against the Bangladesh Central Bank through the Society for Worldwide Interbank Financial Telecommunication (SWIFT) system indicates the sophistication and brazenness of North Korean hackers.<sup>13</sup>

Three main factors are behind the regime's demand for hard currency that drive it to take bold risks and commit cybercrimes. First, despite

<sup>7</sup> So So-yong, "Pukhan ICT chongjaektonghyang mit sisajom" [The Status of North Korea's ICT Policy and Implications], *Information Communication Broadcast Policy* 30, no. 18 (2018).

<sup>8</sup> Chong Sunno, *Kwahakkisullo paljŏnh'a'nun Choson* [Korea Developing with Science and Technology] (Pyongyang: Foreign Language Publishing House, 2019), 6.

<sup>9</sup> These industries include electric power, coal, metals, rail transport, agriculture, fisheries, foreign trade, and joint-venture economic development zones. Institute for Unification Education, *2019 Pukhan ihae* [Understanding North Korea 2019] (Seoul: Nul'um Plus, December 2018), 120.

<sup>10</sup> *Ibid.*, 184–85.

<sup>11</sup> By April 2019, 690 students had graduated from Kim Chaek University of Technology's online education programs, which include master's and doctorate programs. Chong, *Kwahakkisullo paljŏnh'a'nun Choson*, 74–75.

<sup>12</sup> Kate O'Flaherty, "North Korean Hackers' \$2 Billion Heist Is 'Funding WMD Programs,'" *Forbes*, August 7, 2019 ~ <https://www.forbes.com/sites/kateoflahertyuk/2019/08/07/north-korean-hackers-2-billion-heist-is-funding-wmd-programs>.

<sup>13</sup> The hackers tried to steal \$850 million but only took about \$81 million before the theft was discovered. Ben Buchanan, "How North Korean Hackers Rob Banks around the World," *Wired*, February 28, 2020 ~ <https://www.wired.com/story/how-north-korea-robs-banks-around-world>.

“marketization from below” following the formal economy’s breakdown after the 1990s famine, Pyongyang has not fully embraced market reforms. In sum, the North Korean economy can be described as a hybrid economy, with the formal state sector preserving the attributes of a centrally planned economy and its “insatiable desire for investment.”<sup>14</sup> Bank robberies and other crimes using cyber techniques help balance North Korea’s chronic trade deficit and circumvent economic sanctions.

The second factor pushing North Korea toward cybercrime is the economic sanctions imposed on Pyongyang due to its WMD and missile development programs. Some scholars argue that authoritarian dictators are motivated to acquire WMDs to deter foreign adversaries while they “coup proof” their domestic system against the military and internal security forces. North Korea is no exception in this regard. The DPRK’s Korean People’s Army (KPA), although organized as a joint force, is highly politicized.<sup>15</sup> Military officers are promoted based on their loyalty to the supreme leader, and politically the KPA is weak, being under the control of the Korean Workers’ Party (KWP) and three command-and-control channels. This institutional design prevents coups d’état but also reduces the military’s efficiency against external enemies. Thus, the KPA’s conventional weakness is a strong motivation for the North Korean leadership to pursue cyber and other asymmetric capabilities.

The third motivating factor behind Pyongyang’s hacking for hard currency is the need to provide private goods to the Kim regime selectorate—the winning coalition that keeps Kim Jong-un and the KWP elite in power. The KWP dominates information within North Korea, and it allocates a tremendous number of resources to ideology and indoctrination. Nevertheless, dictators must provide material rewards in exchange for loyalty. In a nutshell, the security forces will not provide the services to repress society or intimidate potential political challengers unless they receive material benefits.<sup>16</sup>

---

<sup>14</sup> János Kornai, *The Socialist System: The Political Economy of Communism* (Princeton: Princeton University Press, 1992), 163.

<sup>15</sup> See Jongseok Woo, “Songun Politics and the Political Weakness of the Military in North Korea: An Institutional Account,” *Problems of Post-Communism: Political Institutions and Authoritarian Drift* 63, no. 4 (2016): 253–62.

<sup>16</sup> See Ronald Wintrobe, *The Political Economy of Dictatorship* (Cambridge: Cambridge University Press, 1998); and Bruce Bueno de Mesquita and Alastair Smith, *The Dictator’s Handbook: Why Bad Behavior Is Almost Always Good Politics* (New York: PublicAffairs, 2011).

## Organization and Regime Security

North Korea's ICT advancements have security service applications. Authoritarian dictators need instruments of surveillance and repression to remain in power, and Pyongyang's security apparatus is quite advanced. The Kim family regime has a number of instruments that have become more efficient with its growing ICT infrastructure.<sup>17</sup> Digitalization and ICT make it easier for the KWP's Organization and Guidance Department, the Ministry of State Security, the Ministry of People's Security, the General Political Bureau, the Military Security Bureau, and other surveillance and reporting institutions to communicate, keep records, and maintain social control.

In terms of institutional design, North Korea is replicating the redundancy and competitive arrangement of its military and security institutions in its cyber institutions. Some of the institutional arrangements are based on a division of labor for technical efficiency, but in the cyber realm the dictator faces the same problem as in the military and security forces: who guards the guards? Mapping the institutional landscape is complicated because North Korean leadership has an incentive to conceal its cyber capabilities and institutions. It becomes more confusing because private cybersecurity firms create names for cyber actors based on forensic analysis, usually with little regard or understanding of North Korea's official names and organizational hierarchies.

North Korea's hacking activities are generally divided between the KPA General Staff and the Reconnaissance General Bureau, which is tasked with intelligence collection and covert actions against South Korea. Both organizations have subordinate entities that design software, maintain networks, and engage in computer network operations against adversaries. Cybersecurity firms that analyze North Korean hacking activities have created names for these groups such as the Lazarus Group, Bluenoroff, Andariel, Stardust Chollima, Labyrinth Chollima, Ricochet Chollima, and Silent Chollima.<sup>18</sup> It is uncertain what role, if any, the KPA General Staff

<sup>17</sup> For an overview of the Kim family regime's instruments of control, see Daniel Byman and Jennifer Lind, "Pyongyang's Survival Strategy: Tools of Authoritarian Control in North Korea," *International Security* 35, no. 1 (2010): 44–74.

<sup>18</sup> "Kaspersky Lab Helps to Disrupt the Activity of the Lazarus Group Responsible for Multiple Devastating Cyber-Attacks," Kaspersky Labs, February 25, 2016 ~ <https://web.archive.org/web/20160901174007/http://www.kaspersky.com/about/news/virus/2016/Kaspersky-Lab-helps-to-disrupt-activity-of-Lazarus-Group-responsible-for-multiple-devastating-cyber-attacks>; Michael Mimoso, "Lazarus APT Spinoff Linked to Banking Hacks," Threatpost, April 3, 2017 ~ <https://threatpost.com/lazarus-apt-spinoff-linked-to-banking-hacks/124746/>; and Adam Meyers, "Meet CrowdStrike's Adversary of the Month for April: Stardust Chollima," CrowdStrike, April 6, 2018 ~ <https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-april-stardust-chollima>.



and the Reconnaissance General Bureau play in monitoring domestic internet traffic. However, the Ministry of State Security almost certainly is responsible for some surveillance, given Group 109's task of monitoring and preventing the spread of South Korean videos, dramas, and music in the North.<sup>19</sup> Furthermore, the Ministry of State Security has reportedly hacked into the electronic devices of foreign visitors.<sup>20</sup>

The Central Information Agency for Science and Technology maintains the Kwangmyong network, North Korea's domestic intranet that links research institutes, academic institutions, libraries, enterprises, and elite citizens.<sup>21</sup> The agency was established in August 1963 to collect scientific information from abroad, maintain databases, and disseminate information domestically, all of which require computer network security. Recently, North Korea has completed construction of a facility for the Internet Communications Bureau in Pyongyang. The scope of its tasks and responsibilities is not fully clear but probably includes providing internet services and managing internet traffic in accordance with party security guidance.<sup>22</sup>

North Korea's foreign priorities in cyberspace include developing the following:

- Cyberweapons that can be integrated with electronic warfare and other asymmetric capabilities
- Cyber tools for espionage in military security, industrial technology, and diplomatic information

---

<sup>19</sup> Rachel Vandenbrink, "Internet Enemies' China, Vietnam, North Korea Tighten Controls," Radio Free Asia, March 12, 2014 ∞ <https://www.rfa.org/english/news/china/internet-enemies-03122014175502.html>; and Ha Yoon Ah, "North Korea's Group 109 Ratchets Up Crackdowns in Ryanggang Province," *Daily NK*, June 18, 2019 ∞ <https://www.dailynk.com/english/north-koreas-group-109-ratchets-up-crackdowns-in-ryanggang-province>.

<sup>20</sup> Roseanne Gerin, "Security Agents in North Korea Step Up Hacks of Foreigners' Digital Devices," Radio Free Asia, June 1, 2017 ∞ <https://www.rfa.org/english/news/korea/security-agents-in-north-korea-step-up-hacks-of-foreigners-digital-devices-06012017162154.html>.

<sup>21</sup> For additional background, see "Chung'anggwahakkisult'ongbosa" [Central Information Agency for Science and Technology], in "Encyclopedia of Korean Culture," Academy of Korean Studies ∞ <http://encykorea.aks.ac.kr/Contents/Item/E0070396>; and Kang Jin-gyu, "Pukhan Chung'anggwahakkisult'ongbosa, tayangan kwahakkisuljaryo pal'gan" [North Korea's Central Information Agency for Science and Technology, Publishing Various Science and Technology Materials], *NK Economy*, March 13, 2019 ∞ <https://www.nkeconomy.com/news/articleView.html?idxno=1204>.

<sup>22</sup> Martyn Williams, "North Korea and the Internet: Building for the Future," North Korea Tech, August 1, 2018 ∞ <https://www.northkoreatech.org/2018/08/01/pyongyang-internet-communication-bureau>; and Mathew J. Schwartz, "How NSA Hacked North Korean Hackers," *BankInfoSecurity*, January 19, 2015 ∞ <https://www.bankinfosecurity.com/report-nsa-hacked-north-korean-hackers-a-7810>.

- Cyber sources of revenue, including legitimate internet commerce (albeit small in scale) and illegitimate or criminal sources of hard currency
- Defenses against cyberespionage and cyberattacks from adversaries, especially from South Korea and the United States
- More sophisticated and extensive information operations

North Korea's computer network defense against foreign intrusion, by contrast, does not receive much external coverage or attention (except from those foreign actors seeking to exploit North Korean vulnerabilities). North Korean society is the world's most isolated from the global internet, but the country is not immune from malware or computer network exploitation. According to the *New York Times*, the National Security Agency was able to infiltrate North Korean hacker systems in 2010. This ability ultimately provided the evidence to conclude with high confidence that North Korea was responsible for the destructive cyberattack against Sony in November 2014.<sup>23</sup> This occurred around the same time that the United States allegedly launched the Stuxnet attack to disable Iran's uranium-enrichment centrifuges. The United States reportedly designed and tried to execute a similar cyberattack against North Korean nuclear facilities but without success.<sup>24</sup> However, the United States is rumored to have succeeded in disrupting North Korean ballistic missile tests. In 2014, President Barack Obama reportedly approved the "left of launch" program to use malware and other non-kinetic means to sabotage North Korean missiles either before launch or shortly after they leave their launchpads. The program is believed to have thwarted several Musudan intermediate-range ballistic missile flight tests before Pyongyang discovered and corrected the problems in late 2016.<sup>25</sup>

---


<sup>23</sup> David E. Sanger and Martin Fackler, "NSA Breached North Korean Networks before Sony Attack, Officials Say," *New York Times*, January 18, 2015 ~ <https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html>.

<sup>24</sup> Joseph Menn, "Exclusive: U.S. Tried Stuxnet-Style Campaign against North Korea but Failed—Sources," Reuters, May 29, 2015 ~ <https://www.reuters.com/article/us-usa-northkorea-stuxnet/exclusive-u-s-tried-stuxnet-style-campaign-against-north-korea-but-failed-sources-idUSKBN0OE2DM20150529>.

<sup>25</sup> David E. Sanger and William J. Broad, "Trump Inherits a Secret Cyberwar against North Korean Missiles," *New York Times*, March 4, 2017 ~ <https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html>; and Riki Ellison, "Left of Launch," Missile Defense Advocacy Alliance, March 16, 2015 ~ <https://missiledefenseadvocacy.org/alert/3132>.

*Future Priorities?*

A future priority for Pyongyang could be greater efforts at information operations in cyberspace, since the North Korean leadership has an incentive to influence public perception and discourse in South Korea and other countries. Pyongyang has a limited presence on social media, but the messaging has been relatively low in volume and sophistication. North Korea has reportedly been active in past South Korean electoral campaigns by posting comments on bulletin boards and websites. While North Korea has the language and cultural skills to operate in the South Korean information space, the messaging is often awkward or clumsy, and South Korea's National Security Law and long-term experience provide the means to counter and censor such information operations. While Pyongyang might desire to influence public opinion on the margins in countries or regions such as the United States, Japan, China, and Europe, doing so would require a long-term and costly investment of human resources with negligible benefits.

Nonetheless, North Korea's offensive cyber capabilities have become more sophisticated and destructive. Initially, its cyberattacks consisted of defacing websites or distributed-denial-of-service attacks against servers. Following the Sony attack in November 2014, however, North Korean hackers have focused on larger crimes such as bank robberies and ransomware to earn hard currency for the regime. Given the attributes of the regime and its need for cash, these efforts should be expected to continue unless there is a fundamental change in the nature of the government. North Korean hackers are highly skilled and not effectively deterred from aggressive cyberattacks. Methods to discover the sources of attacks are improving, but attribution still takes considerable time. This makes retaliation difficult, especially considering that North Korea has few cyber targets for retaliation and its cyberwarriors are learning to strengthen their computer network defenses. 

## A Necessary Contest: An Overview of U.S. Cyber Capabilities

*James A. Lewis*

The U.S. government began to worry about vulnerabilities in the cyber domain and to search for ways to reduce them more than twenty years ago. At the same time, in secret, it began developing and using offensive cyberoperations for military purposes while also ensuring that its intelligence agencies amended their collection activities to accommodate the arrival of the internet. The United States' major strategic opponents—Russia and China—at first lagged in developing these military capabilities but are now considered peers or near-peers in terms of their capabilities. Digital technologies and cyberspace have become a new and central domain of conflict among these powers and others. In this domain, however, the U.S. perspective on cybersecurity is somewhat outdated—still too close to its 1990s focus on protecting critical infrastructure and somehow deterring opponents—and no longer sufficient to manage national interests.<sup>1</sup>

Nonstate actors do not have the ability or interest to launch a truly destructive cyberattack. Although, according to European intelligence sources, some Russian-speaking criminal groups have greater cyber capabilities than all but a handful of states and could carry out disruptive attacks, they have little interest in actions that do not yield financial returns (or these proxy groups may be constrained by the Russian state from offering their services to third parties). Terrorist groups lack the expertise and, in most cases, the interest to launch cyberattacks. The most active groups, Hezbollah and Hamas, act largely as proxy forces for Iran. This makes cyber conflict the domain of nation states, something demonstrated by a simple review of public and nonpublic accounts of cyber actions. It is inaccurate to look solely at “cybersecurity,” as if this activity occurred outside the larger sphere of military and diplomatic relationships.

This essay examines how U.S. cyber policy has evolved in response to the return of great-power competition and the development of offensive cyber capabilities by the United States and other countries. While the 2015 UN General Assembly called on all nations to observe norms and

---

JAMES A. LEWIS is a Senior Vice President and Director of the Technology Policy Program at the Center for Strategic and International Studies (United States). He can be reached at <jalewis@csis.org>.

<sup>1</sup> White House, “National Cyber Strategy,” September 2018. ~> <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.

confidence-building measures to increase stability and reduce the chance for cyber conflict,<sup>2</sup> the behavior of major powers in cyberspace is largely unchanged. Norms are defined by actions, and the United States is adopting a more active approach (both diplomatically and militarily) to advance its cybersecurity interests.

### *Starting with Critical Infrastructure*

In thinking about cyber capabilities, a useful starting point is that almost all unclassified networks are vulnerable to persistent, well-financed, and skilled opponents. Pervasive vulnerability shapes cybersecurity. Cyber conflict participants take advantage of these vulnerabilities, in part because defense is still inadequate, and in part because of the lack of agreed rules for how cyber conflict should be conducted. The result is that cyberspace is largely an unconstrained field for conflict. A Russian or Chinese intelligence trawler would never dare sail into a U.S. port—and if it did, it would not go unchallenged—but the speed, ease of access, and relative covertness of cyberoperations means that intrusions by cyberpowers occur almost on a daily basis, sometimes detected, sometimes not, and with the perpetrators often unconcerned when discovered.

The initial U.S. approach to cybersecurity was focused on protecting critical infrastructure from a cyberattack by nonstate actors.<sup>3</sup> This was in many ways an error, as the greatest risks turned out to be from espionage, intellectual property theft, and financial crime.<sup>4</sup> The number of cyberespionage and cybercrime incidents increased dramatically in the first decade after the commercialization of the internet, and it continues to grow. Cybersecurity policy at the time did not consider the risk of political manipulation that blended hacking and social media. In retrospect, the

---

<sup>2</sup> See UN General Assembly Resolution 70/237, “Developments in the Field of Information and Telecommunications in the Context of International Security,” December 2015 ~ <https://undocs.org/A/RES/70/237>.

<sup>3</sup> The very first cyber policy document, Presidential Decision Directive 63, opens by saying, “The United States possesses both the world’s strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems.” White House, “Critical Infrastructure Problem,” May 22, 1998 ~ <https://fas.org/irp/offdocs/pdd/pdd-63.htm>.

<sup>4</sup> “The Economic Impact of Cybercrime and Cyber Espionage,” Center for Strategic and International Studies (CSIS), July 22, 2013 ~ [https://csis-prod.s3.amazonaws.com/s3fs-public/legacy\\_files/files/publication/60396rpt\\_cybercrime-cost\\_0713\\_ph4\\_0.pdf](https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf).

chance of a catastrophic cyberattack on critical infrastructure is remote and the locus of cyber conflict has moved elsewhere.<sup>5</sup>

This first generation of U.S. cyberdefense was somewhat ad hoc. Legal authorities were unclear or lacking, and there was a struggle among agencies over who would lead cyberdefense. For example, the Department of Homeland Security for many years after its creation was uncertain about its mission in cyberspace. Much of this debate was resolved during the Obama administration, which gave the Department of Homeland Security the lead for domestic cybersecurity, issued an executive order to organize the federal government for cyberdefense, and charged the National Institute of Standards and Technology with creating a framework to guide private-sector cybersecurity practices. This mix of sector-specific voluntary and mandatory measures has improved U.S. cybersecurity. As the United States is a continent-sized economy with thousands of companies and political jurisdictions, these defenses remain imperfect. There are still vulnerabilities in key critical infrastructures, but on the whole U.S. cybersecurity is better off than it was twenty years ago.

### *Offensive Capabilities*

The Obama administration, building on the work of the George W. Bush administration, also developed doctrines for the use of offensive cyberoperations and in 2010 created the U.S. Cyber Command in response to a dramatic Russian hack of the Department of Defense's classified network, the first military command openly dedicated to cyberwarfare. Many nations have since followed this precedent. The development of offensive capabilities has profound implications for cybersecurity because it offers an opportunity to develop new policies to block opponent action (using cyberforces) and shape opponent behavior. This could prove more effective than the traditional cyberdefense conducted by individual network operators on a reactive, uncoordinated, and ad hoc basis.

This new emphasis on offensive capacities as part of a larger cyberdefense policy reinforces the need to look at cybersecurity as a subsidiary element of national and international security. Undergirding U.S. cyberdefenses is a reasonable concern held by the United States' potential opponents—such

---

<sup>5</sup> See, for example, James A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," CSIS, December 2002 ≈ [https://csis-prod.s3.amazonaws.com/s3fspublic/legacy\\_files/files/media/csis/pubs/021101\\_risks\\_of\\_cyberterror.pdf](https://csis-prod.s3.amazonaws.com/s3fspublic/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf); and James A. Lewis, "Cyber Solarium and the Sunset of Cybersecurity," CSIS, March 13, 2020 ≈ <https://www.csis.org/analysis/cyber-solarium-and-sunset-cybersecurity>.

as China and Russia—that a dramatic cyberattack, such as the proverbial “blacking out the East Coast,” would provoke a damaging U.S. military response. These potential state opponents then believe, correctly, that the United States has unparalleled attribution capabilities, and they take into consideration the risks of attribution, retaliation, and escalation. This means that outside of some potential larger armed conflicts, they have restricted their cyber activities to espionage and coercive actions that fall below the roughly defined use-of-force threshold, which is generally taken to mean cyber actions that produce casualties or destruction.

However, no cyber action has ever produced casualties and very few (less than a dozen) have produced noticeable destruction.<sup>6</sup> This threshold still leaves ample space for U.S. opponents to engage in harmful acts, however, and the United States has found it difficult to develop a counterstrategy. In part, this difficulty reflects the powerful influence of Cold War deterrence planning among U.S. policymakers, when it was sufficient to build a powerful military force, which through its very existence would prevent opponents from taking hostile action. This approach still shapes U.S. thinking, but it has not worked for a decade against new-style conflict that avoids the direct use of force. The United States has not deterred espionage, state-sponsored crime, or cyber coercion. Though nuclear deterrence also had limits during the Cold War, the shortcomings of deterrence in the cyber domain and the opportunities for espionage and coercion provided by digital technology make cyberspace one of the primary venues for conflict between major powers.<sup>7</sup>

### *Responding to Opponent Doctrines and Use*

In wartime, the major powers have developed doctrines and technologies to use cyberoperations to gain military advantage. Cyberattacks offer speed, precision, and an unparalleled ability to expand the fog of war. They inevitably will be used as part of larger military operations to disrupt opponent weapons systems or command and control, and they could provide significant military advantage. But these disruptive capabilities are largely reserved for armed conflict. Russia (as well as, to a lesser extent, China) has developed doctrines and techniques

---

<sup>6</sup> “Significant Cyber Incidents,” CSIS  <https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents>.

<sup>7</sup> Michael S. Rogers, “United States Cyber Command,” statement before the Senate Committee on Armed Services, Washington, D.C., February 27, 2018.

to achieve coercive effect without greatly increasing the risk of armed clashes with the United States.

Espionage, the primary form of hostile cyber action against the United States, is rampant. Espionage from China has reached unprecedented levels in its effort to acquire technology and commercial advantage, and Russia uses a blend of espionage and propaganda activities to create coercive political effects. The United States is no laggard when it comes to spying, as Edward Snowden's revelations attest, but its espionage still follows entirely conventional politico-military channels.<sup>8</sup> In responding to China, traditional counterespionage is of limited value, diplomatic engagement (as in the 2015 U.S.-China Cyber Agreement) has proved tenuous, and countermeasures such as indictments, though politically painful to the Chinese Communist Party, are not sufficient to convince China to stop spying.<sup>9</sup>

Russia has had signal success in what it sometimes calls reflexive operations—online actions intended to create political disruption by combining hacking (to obtain emails or other information) with other digital techniques and social media activities. First used by Russia against domestic political opponents, reflexive operations are now employed as a tool of foreign policy and coercion.<sup>10</sup> The United States, with its focus on critical infrastructure, has not developed adequate defenses against the new Russian information operations. Conventional measures, such as hardening the electoral machinery, are insufficient to block cyber-enabled information operations. The most effective defense techniques, which involve controlling activities on social media, create First Amendment difficulties, given the potential to interfere with protected political speech. Both Russia and China know this and take advantage of it. China has studied Russian operations but has not been as successful outside Asia because it lacks Russia's deep understanding of Western political culture. (Iran also lacks a close understanding of Western political culture.)

Neither Russia nor China has any incentive to stop cyberoperations. Espionage and political coercion do not qualify as an "attack" in the sense commonly used in international law. It is in this gray area between armed conflict and peacetime operations that most cyber actions take place.

---

<sup>8</sup> "Edward Snowden: Leaks that Exposed U.S. Spy Programme," BBC News, January 17, 2014.

<sup>9</sup> David E. Sanger and Steven Lee Myers, "After a Hiatus, China Accelerates Cyberspying Efforts to Obtain U.S. Technology," *New York Times*, November 29, 2018.

<sup>10</sup> Heather A. Conley et al., *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* (Washington, D.C.: CSIS, 2016).



Cybersecurity in the traditional sense does not encompass this political and informational arena of conflict. While it is a mischaracterization to say (as Russia does) that information has become a weapon, information has become a major element of cyber campaigns against the United States and its allies. The use of information for coercive purposes is central to the contest between the major powers in ways that cyberattacks on critical infrastructure are not. In this respect, the U.S. perspective on cybersecurity is still too similar to its 1990s origins.

One consideration for U.S. policymakers is how to refocus the cybersecurity discussion on these informational and political aspects. This is, after all, a conflict that takes place in what the Russians call the “information space.” U.S. government capabilities in this arena are weak and underdeveloped. The United States has not used propaganda or active measures for decades and has relied instead on its own assumed innate superiority and attractiveness as a source of influence in international affairs. There is both a degree of hubris and a degree of truth in this. Few outside China are rushing to buy copies of books on Xi Jinping Thought, and neither Russia’s kleptocracy nor Iran’s theocracy is attractive. A modernized U.S. cybersecurity policy would need to develop authorities, tools, and techniques for political action that would likely fall outside the authority and expertise now possessed by the military. At the moment, however, this discussion of an information strategy is barely on the U.S. policy agenda.

### *Persistent Engagement and Defend Forward*

Despite these limitations, U.S. cybersecurity policy is evolving and developing ways to use improved offensive capabilities for defensive purposes. The creation of the U.S. Cyber Command a decade ago provides the government with opportunities to create a different approach to cybersecurity that does not rely solely on network defense and is more attuned to the changed nature of interstate conflict. This is a difficult process given both the distractions of recent Middle East misadventures and the continued magnetic pull of Cold War strategy.

Two recent operations highlight the United States’ growing skill in this uncertain domain. The first is the work of Joint Task Force (JTF) ARES, a cyber command operation against the Islamic State of Iraq and Syria (ISIS). Though many of the details remain classified, the United States successfully disrupted ISIS support networks, finances, and propaganda. In unclassified comments, the head of U.S. Cyber Command said of JTF ARES that, even

though not everything worked, in overall terms it was a success. The second operation was the effort to prevent Russia's Internet Research Agency from interfering in the 2018 midterm elections by temporarily disabling its internet infrastructure.<sup>11</sup> These two operations may be harbingers of a more assertive U.S. presence in cyberspace.

The phrases used to describe the new U.S. approach to cybersecurity are "defend forward" and "persistent engagement," part of larger and still developing strategies for active defense by the United States and its treaty allies. The key is that actions are taken on an opponent's network rather than on U.S. networks. These are a violation of sovereignty and domestic criminal law, to be sure, but are by no means an armed attack or a use of force causing casualties or physical destruction according to international law. There is ambiguity, since permanently erasing data is considered a form of destruction, but there is no clear international consensus on whether such an action qualifies as force or an armed attack. The United States, like its opponents, has preferred to inhabit this area of ambiguity in its cyberoperations (with the one major exception being Stuxnet, which created physical damage to Iranian centrifuges).<sup>12</sup>

U.S. cyber priorities are still largely defensive even in espionage activities, but they are not perceived as such by the United States' strategic opponents. This mismatch of perceptions is one source escalating conflict; the other is that Russia, China, and Iran believe they can use cyberoperations against the United States in ways that do not create unacceptable risk. This is an unstable environment. While there are ongoing negotiations in the United Nations on norms, none of the three major powers as yet are willing to make any concessions. This mutual recalcitrance has led U.S. cyber policy to take a different avenue.

### *A Framework for Responsible State Behavior in Cyberspace*

Active defense is embedded in the larger U.S. diplomatic strategy for cybersecurity. Since 2010, the United States has pursued the development of a framework for responsible state behavior, defined by agreed norms and reinforced by confidence-building measures. The cornerstone of this definition of responsible state behavior is the 2015 agreement by all

---

<sup>11</sup> Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *Washington Post*, February 27, 2019.

<sup>12</sup> Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, November 3, 2014.

members of the UN General Assembly to eleven norms that dictate how a state should behave in cyberspace to reduce the chances of conflict and preserve stability. The creation of a framework for responsible state behavior has been accompanied by an academic discussion of how to “implement” norms, as if they were an instruction manual for operating in cyberspace. States do not implement norms; rather, they choose to observe norms by undertaking policies and actions that are consistent with them. For cyberspace, these norms are voluntary, and each state has discretion on how to observe them. The agreed norms do not prohibit espionage (although a U.S.-China agreement in 2015 to limit commercial espionage by state actors was endorsed by the G-20), nor do they prohibit attacks on critical infrastructure if these attacks are consistent with a state’s obligations under international law.

The benefit of agreed norms is that a state’s failure to observe them can be used to justify a punitive response, whether this involves countermeasures, in-kind retaliation, or force. At the UN General Assembly in February 2020, the United States and 27 other countries agreed that they would cooperate on imposing punitive measures on those countries that did not observe the 2015 agreement. This provides a justification for the new and more assertive U.S. posture in cyberspace, as well as for working with like-minded allies and partners. The principle area of disagreement is over how existing commitments to international law apply in cyberspace. The obligation to respect sovereignty that is embodied in the UN Charter, such as prohibiting member states from interfering in another country’s political independence, is violated by every nation that engages in espionage. Russia and China would argue that the United States also routinely interferes in their internal affairs, but their definition of interference is different and based in part on a rejection—or at least diminution—of so-called universal values like the Universal Declaration on Human Rights, which they believe infringe on their sovereign authority.

Sovereignty has become a vital issue in the discussion of cybersecurity. The reaction to a cyberspace dominated by U.S. and Chinese tech giants, and the commercial globalization of the 1990s, has led many countries to extend sovereign control into cyberspace through national regulation and law. Their goals are to control national data, improve privacy, and reduce cybersecurity risk. This expansion of national sovereignty is also driven by deep concerns over the failure of internet governance to provide security or privacy; the internet as it is currently structured is seen as a growing source

of risk by many nations. U.S. policy on cybersecurity will need to evolve in light of this.

### *Rethinking Cyber Dogma*

Cyberspace has become an arena for great-power conflict. To quote Abraham Lincoln, “the dogmas of the quiet past are inadequate to the stormy present.”

Cybersecurity and internet governance have until now been treated as distinct issues. Yet in recent years, these areas have started to merge. There has always been a link between data protection and cybersecurity. The beliefs held by authoritarian regimes that an open internet is part of a larger and intrusive political campaign by the United States to inculcate regime change and that the governance structure of the internet is a threat to regime survival have made governance an area of tension and increasing conflict. This is not cybersecurity in the conventional sense. As digital technologies become central to social and commercial activity, U.S. priorities in cyberspace will need to adjust.

The internet was created at a moment of American triumphalism with little attention to security because of assumptions about a harmonious future for international relations. Since then, cyberspace has become central to international conflict. The United States, originally a pioneer in the use of cyber techniques, now lags behind as the domain evolves beyond conventional military and espionage activities. The United States retains impressive capabilities, but its strategy must evolve if it is to make better use of these to advance its national interests in cyberspace. ◆

## Japan: An Exclusively Defense-Oriented Cyber Policy

*Benjamin Bartlett*

There is little question that over the last decade, and particularly since 2014, Japan has been accelerating its efforts to build cyber capabilities. However, unlike some states in the region, Japan's capabilities are almost entirely defensive in nature. Even the limited offensive capabilities now being planned are aimed at preventing potential adversaries from using cyberattacks against the country within the context of a military conflict rather than toward launching cyberattacks against other states.

This essay argues that this pattern is primarily a result of two factors: (1) regional actors' development of offensive cyber capabilities alongside Japan's own growing dependence on information technology that represents an increased threat to its national security, and (2) an "exclusively defense-oriented" national security policy that limits Japan's potential response. It first discusses both of these factors and then turns to the offensive and defensive cyber capabilities that Japan has been developing as a result.

### *Cyberthreats to Japan's National Security*

For Japan, the offensive cyber capabilities of three states in particular are cause for concern: China, Russia, and North Korea. All three have built considerable offensive capabilities and have shown themselves willing to use those capabilities to exploit the cyber domain and, in the case of North Korea and Russia, conduct cyberattacks.<sup>1</sup> An advanced persistent threat, APT10, associated with China, has reportedly stolen information from a number of Japanese public and private organizations.<sup>2</sup> Likewise, North Korea has hacked into and stolen money from Japanese Bitcoin exchanges.<sup>3</sup> Russia does not yet seem to have targeted Japan, but Japan has noted Russia's activities elsewhere, including its use of hybrid warfare. Japan has

---

**BENJAMIN BARTLETT** is an Assistant Professor in the Department of Political Science at Miami University in Ohio (United States). He can be reached at <bartlebg@miamioh.edu>.

<sup>1</sup> "Cyber exploitation" refers to using cyber tools to exfiltrate data, while "cyberattack" refers to using cyber tools either to interfere with the workings of a system or to cause physical damage.

<sup>2</sup> Tatsuya Sudo, "Chinese Hackers May Have Struck Keidanren System in 2016," *Asahi shimbun*, January 13, 2019 ~ <http://www.asahi.com/ajw/articles/AJ201901130021.html>.

<sup>3</sup> Julian Ryall, "North Korea Hits Out at Japan as Cyber Arms Race Heats Up," *Telegraph*, May 23, 2019 ~ <https://www.telegraph.co.uk/news/2019/05/23/north-korea-hits-japan-cyber-arms-race-heats>.

significant territorial disputes with both China and Russia, while North Korea continues to be a challenge to overall regional stability.<sup>4</sup>

Two factors make Japan particularly vulnerable to threats in cyberspace. First, Japan's plans for future economic growth and competitiveness are centered on technologies such as the Internet of Things and artificial intelligence. These technologies will open up more of its society and economy to cyberattacks.<sup>5</sup> Second, the Japan Self-Defense Forces (JSDF) rely heavily on advanced technology, including a number of recent upgrades to its command, control, communications, and intelligence equipment.<sup>6</sup> While this has obvious advantages, it also makes the JSDF potentially vulnerable to cyberattacks. Moreover, the JSDF is having difficulty recruiting, meaning it may become more reliant on these technologies to make up for a lack of manpower.<sup>7</sup>

In short, a few regional actors present major cyberthreats to Japan's national security. The two key scenarios Japan has to worry about in this context are (1) the use of cyberattacks to disrupt the operations of the JSDF as part of an attack against Japan, or perhaps to prevent the JSDF from coming to the aid of another military, and (2) attacks against critical infrastructure. To understand how Japan is responding to these threats, however, it is important to contextualize the country's overall defense policy and how it is shaped by Japan's constitution, which prohibits warmaking potential.

### *A Defense-Oriented Offense*

Article 9 of Japan's constitution prohibits warmaking potential or the use of force, or even the threat of force, as a political instrument.<sup>8</sup> However, as long interpreted by the Japanese government, it does not deny the inherent right of self-defense. Instead, the government interprets the article

---

<sup>4</sup> Ministry of Defense (Japan), *Defense of Japan 2019* (Tokyo, 2019), 44–45, 167–68.

<sup>5</sup> Cabinet (Japan), "The 5th Science and Technology Basic Plan (Provisional Translation)," January 22, 2016 ≈ <http://www8.cao.go.jp/cstp/english/basic/5thbasicplan.pdf>.

<sup>6</sup> Ryo Hinata-Yamaguchi, "Japan's Defense Readiness: Prospects and Issues in Operationalizing Air and Maritime Supremacy," *Naval War College Review* 71, no. 3 (2018): 41–60.

<sup>7</sup> Tara Copp, "How Will Japan Defend Itself, If It Can't Get Its Youth to Serve?" *Military Times*, January 30, 2019 ≈ <https://www.militarytimes.com/news/your-military/2019/01/30/how-will-japan-defend-against-china-if-it-cant-get-its-youth-to-serve>.

<sup>8</sup> "The Constitution of Japan," art. 9, Prime Minister of Japan and His Cabinet, November 3, 1946 ≈ [https://japan.kantei.go.jp/constitution\\_and\\_government\\_of\\_japan/constitution\\_e.html](https://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html).

as a requirement to have the minimal armed forces necessary to exercise this right.<sup>9</sup>

Though it is widely recognized, at least beginning with the Koizumi administration and possibly accelerated during the current Abe administration, that Japan has moved away from an antimilitaristic stance toward a more pragmatic approach to national security,<sup>10</sup> Tokyo still maintains what it refers to as an “exclusively defense-oriented policy.” This means that defensive force is used only in the event of an attack,<sup>11</sup> and that force and defense capabilities possessed and maintained are limited to the minimum necessary for self-defense.<sup>12</sup> Important for any discussion of cyber capabilities, the use of force is notably not confined to the boundaries of Japan, its territorial waters, or its airspace.<sup>13</sup> However, there has been little public consideration by the government as to what shape cyberoperations beyond Japan’s borders might take.

Thus, while Japan’s defense policy allows for some offensive cyber capabilities, there are limits as to what is acceptable. Moreover, there are two other factors that militate against Japan’s building strong offensive cyber capabilities. First is the long-standing policy of limiting Japan’s defense spending to no more than 1% of GDP, which means that the Ministry of Defense (MOD) and the JSDF must make hard decisions on investing in capabilities.<sup>14</sup> The combination of real threats to its cybersecurity and its exclusively defense-oriented policy have led Japan to invest heavily in defensive rather than offensive cyber capabilities. Second, if Japan were to become involved in a militarized conflict, its ally, the United States, has a considerable cyber arsenal that would also likely be brought to bear.<sup>15</sup>

---

<sup>9</sup> Ministry of Defense (Japan), *Defense of Japan 2019*, 198.

<sup>10</sup> See, for example, Michael J. Green, *Japan’s Reluctant Realism: Foreign Policy Challenges in an Era of Uncertain Power* (New York: Palgrave Macmillan, 2003); Richard J. Samuels, *Securing Japan: Tokyo’s Grand Strategy and the Future of East Asia* (Ithaca: Cornell University Press, 2007); Andrew L. Oros, *Normalizing Japan: Politics, Identity, and the Evolution of Security Practice* (Stanford: Stanford University Press, 2008); Amy Catalinac, *Electoral Reform and National Security in Japan: From Pork to Foreign Policy* (Cambridge: Cambridge University Press, 2016); Andrew L. Oros, *Japan’s Security Renaissance: New Policies and Politics for the Twenty-First Century* (New York: Columbia University Press, 2017); and Sheila A. Smith, *Japan Rearmed: The Politics of Military Power* (Cambridge: Harvard University Press, 2019).

<sup>11</sup> Until recently, this meant “an attack against Japan,” but in 2014 a Cabinet decision expanded this to include an armed attack against a foreign country that is in a close relationship with Japan, if that attack would also threaten Japan’s survival. See Ministry of Defense (Japan), *Defense of Japan 2019*, 198.

<sup>12</sup> *Ibid.*, 200.

<sup>13</sup> *Ibid.*, 199.

<sup>14</sup> Crystal Pryor and Tom Le, “Looking Beyond 1 Percent: Japan’s Security Expenditures,” *Diplomat*, April 3, 2018 <https://thediplomat.com/2018/04/looking-beyond-1-percent-japans-security-expenditures>.

<sup>15</sup> Paul Kallender and Christopher W. Hughes, “Japan’s Emerging Trajectory as a ‘Cyber Power’: From Securitization to Militarization of Cyberspace,” *Journal of Strategic Studies* 40, nos. 1–2 (2017): 133–37.

Japan is, however, in the process of developing limited offensive capabilities, though these too are mainly for defensive purposes. There are plans to create a joint cyber unit directly under the MOD with limited offensive capabilities, although its primary duty will be to protect the MOD and JSDF networks. Specifically, this unit will have the capacity to disrupt an opponent's use of cyberspace for launching cyberattacks. In this it will differ from the current Cyber Defense Unit, which has only defensive capabilities. This new unit will be established by 2023.<sup>16</sup> The nature of its offensive capabilities will be quite limited, however. These are capabilities meant to disrupt an adversary's use of cyberspace as a weapon—that is, capabilities aimed at disrupting networks and computer systems—rather than capabilities to cause harm to physical systems.<sup>17</sup> In short, even these offensive capabilities are being built for defensive purposes to help prevent cyberattacks against Japan in a conflict scenario; and they pose little threat outside of this scenario. This is in line with Japan's exclusively defense-oriented policy.

### *Japan's Cyberdefense Capabilities and Critical Sectors*

While Japan's defense policy and priorities may limit its offensive capabilities, in recognizing the national security threats that the country faces from potential cyberattacks the government began building defensive capabilities at the end of the 1990s and has accelerated its efforts over the last decade. Its overall cybersecurity budget increased from 26.70 billion yen in fiscal year 2004 to 71.29 billion yen in fiscal year 2019.<sup>18</sup>

Recognizing that cyberattacks against the JSDF, the government, and critical infrastructure pose the highest threat to national security, the government has made efforts to strengthen Japan's cybersecurity capabilities in all three areas. In particular, two trends are apparent across all three areas: increasing centralization of responsibility and increasing coordination and communication among relevant actors.

---

<sup>16</sup> Ministry of Defense (Japan), *Defense of Japan 2019*, 229.

<sup>17</sup> *Ibid.*, 219.

<sup>18</sup> National Center of Incident Readiness and Strategy for Cybersecurity (NISC) (Japan), "2006 nendo no jouhou sekyuriti taisaku no hyouka nado: 'Shin no sekyuriti sanshin kuni' wo mezasu torikumi no ichinenme no hyouka [Evaluation of FY 2006 Information Security Measures: Evaluation of the First Year of Efforts Aiming at "A Country Advancing True Information Security"]", April 23, 2007, appendix 23 ~ [https://www.nisc.go.jp/active/kihon/pdf/sjeval\\_2006.pdf](https://www.nisc.go.jp/active/kihon/pdf/sjeval_2006.pdf); and Cybersecurity Strategic Headquarters (Japan), "Saibaasekyuriti 2019" [Cybersecurity 2019], May 23, 2019, 238 ~ <https://www.nisc.go.jp/active/kihon/pdf/cs2019.pdf>.



*The Japan Self-Defense Forces.* The JSDF's earliest efforts to build cyber capabilities occurred early in the new millennium when first the Air Self-Defense Force, and then the Ground Self-Defense Force and Maritime Self-Defense Force, set up their own cybersurveillance units. At this point, each service was essentially in charge of its own cybersecurity; there was no coordination between them. In 2007 the MOD improved on this by establishing a combined command, the Defense Information Infrastructure, and it followed up a year later with the establishment of the Command Control Communication Computers Systems Command (C4SC). This was a step forward, as C4SC acted as a coordinator between the cybersecurity units of the Air Self-Defense Force, Ground Self-Defense Force, and Maritime Self-Defense Force, but each service was still largely responsible for its own efforts.<sup>19</sup>

The JSDF's capabilities were finally centralized in 2014, when the MOD established the joint Cyber Defense Unit under the C4SC. Though at present the unit only consists of around 220 personnel (up from around 90 when it was created), its creation placed responsibility for the monitoring and defense of the MOD and JSDF networks within a single, centralized unit.<sup>20</sup> As mentioned above, the government plans to create a new joint cyber unit responsible for protecting the JSDF's networks by 2023. This new unit will be placed directly under the MOD's authority, further centralizing control and responsibility.<sup>21</sup>

Cooperation between Japanese and U.S. forces in the cyber domain is recent but growing. In 2019 the JSDF and the U.S. military held a multiday exercise to simulate a joint response to a cyberattack.<sup>22</sup> In 2020 the Ground Self-Defense Force hosted the first joint cyberdefense seminar with the U.S. military.<sup>23</sup> Given the centrality of the U.S.-Japan alliance to Japan's defense, this trend will no doubt continue.

---

<sup>19</sup> Kallender and Hughes, "Japan's Emerging Trajectory as a 'Cyber Power,'" 129–31.

<sup>20</sup> Ministry of Defense (Japan), "Establishment of the Cyber Defense Unit," *Japan Defense Focus*, no. 52 (2014)  $\approx$  [http://www.mod.go.jp/e/jdf/sp/no52/sp\\_activities.html#article03](http://www.mod.go.jp/e/jdf/sp/no52/sp_activities.html#article03); Franz-Stefan Gady, "Japan: The Reluctant Cyberpower," *Asie Visions*, no. 24 (2017); and Ministry of Defense (Japan), "Defense Programs and Budget of Japan," 2019, 6–7  $\approx$  [https://www.mod.go.jp/e/d\\_budget/pdf/310118.pdf](https://www.mod.go.jp/e/d_budget/pdf/310118.pdf).

<sup>21</sup> Ministry of Defense (Japan), *Defense of Japan 2019*, 229.

<sup>22</sup> "Tai saibaakougeki nichibei de" [U.S.-Japan Cyberattack Response], *Nihon keizai shimbun*, December 10, 2019  $\approx$  <https://www.nikkei.com/article/DGXMZO53113880Z01C19A2PP8000>.

<sup>23</sup> "Rikuji, beigun tonoshiba boei semina wo hatsu kaisai" [GSDF Opens First Cyber Defense Seminar with U.S. Military], *Sankei shimbun*, February 26, 2020  $\approx$  <https://www.sankei.com/politics/news/200226/pl2002260026-n1.html>.

*Government.* As with the JSDF, Japan's efforts toward protecting the government as a whole have followed a similar pattern of increasing coordination and centralization, particularly within two Cabinet bodies: the Cybersecurity Strategic Headquarters, which is directly under the authority of the prime minister, and its secretariat, the National Center of Incident Readiness and Strategy for Cybersecurity (NISC). The former consists of ministers, along with members of the private sector and academia, and meets a few times a year to set overall policy. The latter contains bureaucrats seconded from the MOD; the Ministry of Economy, Trade and Industry; the Ministry of Internal Affairs and Communications; and the National Police Agency. Together with helping to implement overall policy, the NISC handles much of the day-to-day affairs of government cybersecurity.<sup>24</sup>

The Cybersecurity Strategic Headquarters and the NISC both had predecessors established in 2005; however, they were located lower in the hierarchy of the Cabinet Office and had limited authority over other parts of government. The 2014 Basic Law on Cybersecurity, which established these new organizations, changed this and gave them the authority both to request information from other government bodies on cybersecurity issues and to ask for cooperation in implementing policy. A later amendment expanded this authority to include incorporated administrative agencies, such as the Japan Pension Service.<sup>25</sup>

Within NISC there are two bodies of technical staff, one proactive and the other reactive. The proactive body, Government Security Operation Coordination Team Number 1 (GSOC1), monitors government networks, analyzes malware, collects information about cyberthreats, and distributes this information to the various ministries and agencies. The reactive body, the Cyber Incident Mobile Assistance Team, provides technical support and advice when a ministry or agency has been hit by a cyberattack. Incorporated administrative agencies are monitored by a separate body of technical staff, Government Security Operation Coordination Team Number 2 (GSOC2), located under the Information-technology Promotion Agency, itself an incorporated administrative agency.<sup>26</sup> Thus, the monitoring of government cybersecurity is not entirely centralized but

---

<sup>24</sup> Motohiro Tsuchiya, "Cyber Security Governance in Japan: Two Strategies and a Basic Law," in *Information Governance in Japan: Towards a New Comparative Paradigm*, ed. Kenji E. Kushida, Yuko Kasuya, and Eiji Kawabata (Stanford: Silicon Valley New Japan Project, 2016).

<sup>25</sup> *Ibid.*

<sup>26</sup> Cybersecurity Strategic Headquarters (Japan), "Saibaasekyuriti 2019," 29.

instead split between GSOC1 and GSOC2. Nevertheless, the pattern over time has been one of increasing centralization and clearer authority for the NISC.

*Critical infrastructure.* Because critical infrastructure is primarily in the hands of private firms, it is impossible to centralize authority as it occurs in the government. However, the government has nevertheless worked to improve coordination by building lines of communication both between critical infrastructure firms and between those firms and the government.<sup>27</sup> The government classifies thirteen infrastructure sectors as critical: telecommunications, finance, aviation, rail, electricity, gas, government/administrative services, medical services, water, transport, chemicals, credit, and oil.

For each sector, the government has created an organization called Capability for Engineering of Protection, Technical Operation, and Response (CEPTOAR), which is responsible for sharing information about cyberthreats and cyberattacks between relevant firms and the Cabinet secretariat via the ministry responsible for that sector. It has also created a CEPTOAR Council, which shares information across sectors. To help encourage firms to share information with the government, information given by a firm to the CEPTOAR secretariat is anonymized before being passed on to the government.<sup>28</sup>

### *Conclusion*

While Japan has recently accelerated its efforts to strengthen its cyber capabilities in response to an increasingly threatening digital environment, these efforts have been almost entirely defensive in nature. To the degree that it is developing offensive capabilities, they are aimed at disrupting an adversary's ability to carry out cyberattacks against Japan.

It is important to note that Japan's defense-oriented national security policy does not necessarily preclude further development of offensive cyber capabilities. For example, offensive capabilities developed specifically for limited military targets, such as disrupting targeting

---

<sup>27</sup> NISC (Japan), "Saibaasekyuriti taisaku no kyouka ni muketa taiou ni tsuite" [About Responses toward Strengthening Cybersecurity Measures], November 9, 2016, 10 ~ [http://www.kantei.go.jp/jp/singi/keizaisaisei/miraitoshikaigi/4th\\_sangyokakumei\\_dai2/siryou9.pdf](http://www.kantei.go.jp/jp/singi/keizaisaisei/miraitoshikaigi/4th_sangyokakumei_dai2/siryou9.pdf).

<sup>28</sup> NISC (Japan), "Action Plan on Information Security Measures for Critical Infrastructures," December 13, 2005 ~ [http://www.nisc.go.jp/eng/pdf/actionplan\\_ci\\_eng.pdf](http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf); and Cybersecurity Strategic Headquarters (Japan), "The Cybersecurity Policy for Critical Infrastructure Protection (4th Edition)," April 18, 2017 ~ [http://www.nisc.go.jp/eng/pdf/cs\\_policy\\_cip\\_eng\\_v4.pdf](http://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4.pdf).

systems, during an attack against Japan would seem to fall within the boundaries of what is acceptable under Japanese policy. Given the practical difficulties and expense of developing these capabilities, it is unlikely that Japan will develop them in the near future. Because the threat to Japan's cybersecurity is only increasing, however, we can expect that investments in defensive capabilities will continue to grow. ◆

## A Collaborative Battle in Cybersecurity? Threats and Opportunities for Taiwan

*Hsini Huang*

According to the World Economic Forum's 2020 Global Risks Report, cyberattacks rank as one of the top ten hazards in terms of likelihood and impacts, following environmental dangers such as extreme weather or natural disaster.<sup>1</sup> The development of an increasingly digitized economy, the Internet of Things, and other fourth industrial revolution technologies have raised concerns about cybersecurity risks in daily life, business, critical infrastructure, and public domains.<sup>2</sup>

Despite the threat and potential harm to Taiwan's economy, President Tsai Ing-wen's defense policy has emphasized that cybersecurity is national security. In the past twenty years, Taiwan (the Republic of China, or ROC), with its long history of complicated cross-strait relations, has witnessed a constant and increasing threat from the rising conflicts in cyberspace. According to an interview with Vice Premier Chen Chi-mai of the Executive Yuan (Taiwan's executive branch), Taiwan perceived a total of 3 billion scans by hackers for potential vulnerabilities and 30 million attacks in 2019. Unsurprisingly, most attacks on government sites and services were from mainland China (the People's Republic of China, or PRC) or launched by Chinese network forces,<sup>3</sup> including various advanced persistent threats to secretly penetrate both public and private systems.<sup>4</sup> For example, in June 2019, Taiwan's Ministry of Civil Services reported a serious data leak of civil servants' personal information. In 2014, Taiwan's *Apple Daily* was

---

**HSINI HUANG** is an Associate Professor in the Graduate Institute of Public Affairs and Department of Political Science at the National Taiwan University (Taiwan). She can be reached at <hsinihuang@ntu.edu.tw>.

<sup>1</sup> "The Global Risks Report 2020," World Economic Forum  $\approx$  <https://www.weforum.org/reports/the-global-risks-report-2020>.

<sup>2</sup> Fourth industrial revolution technologies include cloud computing, autonomous cars, precision medicine, and drones.

<sup>3</sup> Hsin-fang Lee and Jonathan Chin, "Chinese Hackers Getting Sophisticated," *Taipei Times*, April 5, 2018  $\approx$  <http://www.taipeitimes.com/News/front/archives/2018/04/05/2003690700>; and Sophia Yang, "200 Million Cyber Attacks Hit Taiwan's Military Networks in 2017," *Taiwan News*, May 28, 2018  $\approx$  <https://www.taiwannews.com.tw/en/news/3441894>.

<sup>4</sup> Philip Hsu, "Chinese Hacking Against Taiwan: A Blessing for the United States?" *Diplomat*, January 23, 2018  $\approx$  <https://thediplomat.com/2018/01/chinese-hacking-against-taiwan-a-blessing-for-the-united-states>.

subjected to serious cyberattacks from China because of its reports about the Sunflower Movement and Hong Kong's Occupy Central Movement.<sup>5</sup>

Cybersecurity cannot be built independently from cyberdefense. As the director of the National Center for Cyber Security Technology (NCCST), Chien Hung-wei, responded in a magazine interview: "Cybersecurity is not only about advancing security technologies, but also about intelligence, information, and cognition. We need to understand our opponents to prepare for the next steps."<sup>6</sup> According to Chien, although Taiwan has been the target of massive and numerous cyberattacks, this is actually the best time to use Taiwan as a testing ground for training talent and developing the domestic cybersecurity capacity.

This essay begins by describing the change of government strategies since 1999 in dealing with cybersecurity issues in Taiwan. It then addresses the more recent development of cybersecurity policies under the Tsai administration, including the formation of a cybersecurity strategy triangle between the National Security Council, the Ministry of Defense, and the Executive Yuan. The essay concludes by arguing for the importance of a collaborative alliance with regional friends to build a cybersecurity network through information sharing and communication to protect the regional security altogether.

### *The Shift in Taiwan's Cybersecurity Strategies*

Although Taiwan has experienced cyberthreats from China since 1999,<sup>7</sup> there was initially a clear distinction between Taiwan's two main political parties, the Kuomintang (KMT) and the Democratic Progressive Party, on Taiwan's cybersecurity strategy. Shortly after President Li Teng-hui announced that Taipei and Beijing had a "special state-to-state" relationship in 1999, many ROC government websites were hacked and left with unauthorized digital graffiti (i.e., website defacement).<sup>8</sup> People then became aware of the damages and cognitive impacts that could be carried out through cyberattacks. In response, in 2001 the government formed the National Information and Communication Security Taskforce (NICST) and

<sup>5</sup> Yang Yuan-ting and Jake Chung, "Apple Daily Slams Hack Attack," *Taipei Times*, June 19, 2014. ~ <https://www.taipetimes.com/News/front/archives/2014/06/19/2003593115>.

<sup>6</sup> "Zhi jianshangdefang weizhan" [A Defensive War on Fingertips], *Business Today*, July 31, 2019.

<sup>7</sup> Bonnie S. Glaser and Matthew P. Funaiolo, "Perspectives on Taiwan: Insights from the 2018 Taiwan-U.S. Policy Program," March 28, 2018 ~ <https://www.csis.org/analysis/perspectives-taiwan-0>.

<sup>8</sup> Xiao-He Luo, "Benyue Shangxun duan haike qi qian yu ci laixi" [More than 7,000 Chinese Hacker Attacks This Month], *United Daily News*, August 17, 1999.

the NCCST to improve information security. The NICST focuses on the management of interagency communication, and the NCCST concentrates on the technical services providing cybersecurity. During the administration of President Ma Ying-jeou in 2015, the government established a new cyberintelligence division within the National Security Bureau. But on the military side, Taiwan seemed to focus more on “establishing capability of force preservation” and continuing the KMT’s policies of not provoking the relationship and maintaining sustainable ties with the PRC.<sup>9</sup>

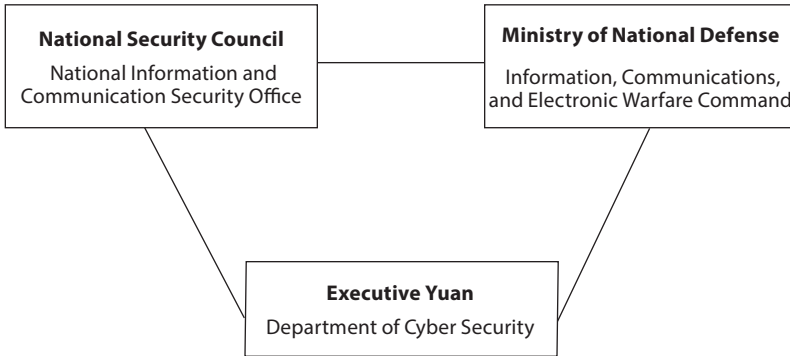
By contrast, given the rising number of advanced persistent threats and other forms of cyberespionage toward government systems, President Tsai Ing-wen’s administration began a series of proactive actions from different angles, starting with the establishment of the National Information and Communication Security Office in August 2016. The office is listed under the National Security Council, a principal advisory forum to the president. In the same month, the Executive Yuan also launched the Department of Cyber Security to administer the nation’s cybersecurity. In June 2017 the Ministry of National Defense announced the launch of the Information, Communication, and Electronic Force Command to prepare for cyberthreats from abroad. The purpose of this “fourth military service” is to defend the ROC’s digital territory as well as to work on developing fundamental cybersecurity technologies and infrastructure domestically. At the operational and managerial level, in May 2018, legislators passed the Information and Communication Management Act, which provides the basic guidelines and standard operating procedures for how the public and private sectors should regularly report cybersecurity activities and issues to the governing authorities. Following that, to delineate cybersecurity as a new part of national security, in June 2019 an amendment bill of the National Security Act was passed to include cyberspace as well as physical space within Taiwan’s defensible territory. However, many argue that cyberspace is not a single space but rather a complicated technical, territorial, and transborder concept. The definition and boundary of cyberspace remain vague and difficult to clarify.

In sum, after 2016 the role of the government in cybersecurity significantly intensified. As depicted in **Figure 1**, the Tsai administration is building a cybersecurity strategy triangle linking the National Security

---

<sup>9</sup> Ministry of National Defense (Taiwan), *National Defense Report 2015* (Taipei, November 2015) ~ <https://china.usc.edu/sites/default/files/article/attachments/taiwan-2015-national-defense-report.pdf>; and Hon-Min Yau, “Explaining Taiwan’s Cybersecurity Policy Prior to 2016: Effects of Norms and Identities,” *Issues and Studies* 54, no. 2 (2018): 1–30.

FIGURE 1

*Taiwan's Cybersecurity Strategy Triangle*

Council, the Ministry of National Defense, and the Department of Cyber Security within the Executive Yuan together. By integrating the responsible authorities, the aim is to defend and manage the rising risk of cyberthreats, as well as increase offensive technological capabilities and military soft power. However, this strategic move has raised some concerns. Scholars of critical security studies have argued that defense might be more important than offense for Taiwan, since it is difficult to assess the payoffs and consequences of cyberweapon development or elevated cross-strait conflicts due to militarized cybersecurity.<sup>10</sup> Additionally, the ROC government is also keen to develop and promote the domestic cybersecurity industry, pushing for the upgrade of cybersecurity infrastructure in Taiwan.

Compared to previous administrations, President Tsai has a stronger ambition to achieve cyber autonomy and strengthen Taiwan's cybersecurity capabilities. The Information and Communication Management Act aims to achieve two goals: one is to enhance the overall national cybersecurity and defensive capabilities, and the other is to create a demand-driven industrial environment for cybersecurity companies.<sup>11</sup> Many believe that the focus on fostering a new industry is good for Taiwan's economy because of its strong foundation and technological capacities in information

<sup>10</sup> Hon-Min Yau, "A Critical Strategy for Taiwan's Cybersecurity: A Perspective from Critical Security Studies," *Journal of Cyber Policy* 4, no. 1 (2019): 35–55.

<sup>11</sup> Hsini Huang and Tien-Shen Li, "A Centralised Cybersecurity Strategy for Taiwan," *Journal of Cyber Policy* 3, no. 3 (2018): 344–62.



technology industries. More specifically, in its national cybersecurity strategy plan, the government is focusing on the following four missions:<sup>12</sup>

- Complete the cybersecurity infrastructure to facilitate government agencies' maturity in cybersecurity governance.
- Construct a national united defense system in cybersecurity to construct a hierarchical cross-agency management scheme and united cybersecurity system.
- Increase self-development capacity to create a thousand-person response team in government agencies in order to prepare national cybersecurity manpower to protect the ROC as a digital country.
- Nurture talent in the field of cybersecurity by providing specialized cybersecurity courses and programs in universities, relaxing requirements for foreign professionals to acquire work permits, and achieving a domestic cybersecurity industries market value of NT\$55 billion.

Furthermore, to advance and complete its national cybersecurity network, a new version of the information security national plan for 2021–24 will likely be proposed in 2020. Many believe that the above-mentioned missions will be emphasized.

### *Collective Security in Response to Cybersecurity*

In cybersecurity, there is no choice but to recognize that cyberspace transcends boundaries and represents a different kind of territory than physical geography. Taiwan faces not only cyberattacks from the PRC but also cyberthreats to financial and other critical systems from Russia and North Korea. Taiwan's abundant experience dealing with cyberattacks can be shared with countries that hold similar beliefs to its own. Given the worsening global threat of cyberattacks, it must be acknowledged that countries will share risks. The ROC government believes that it is in Taiwan's best interest to participate in a regional network where actors can counter this threat and provide collective security.

One of President Tsai's most important foreign policies is the New Southbound Policy. Since May 2016, this initiative has increased Taiwan's economic and social engagements in the Indo-Pacific, including with the ten countries in the Association of Southeast Asian Nations (ASEAN),

---

<sup>12</sup> National Center for Cyber Security Technology (Taiwan), *National Cyber Security Program of Taiwan (2017 to 2020)* (Taipei, November 2017)  $\approx$  <https://nicst ey.gov.tw/File/3BF304D39EA91236>.

six countries in South Asia, Australia, and New Zealand. In April 2019, at the opening of the Indo-Pacific Security Dialogue—and coincident with the 40th anniversary of the Taiwan Relations Act—President Tsai remarked that “Taiwan is ready, willing and able to work with the U.S. and other like-minded partners in promoting a free, open, and prosperous Indo-Pacific.”<sup>13</sup> One month later in May 2019 the Indo-Pacific Cyber Security Dialogue and Inauguration of the Indo-Pacific Cybersecurity Alliance Symposium was held by legislator Hsu Yu-Jen and the American Institute in Taiwan.<sup>14</sup> The symposium aimed to create Taiwan-U.S. cooperation and a potential regional alliance that would connect and benefit countries in the Indo-Pacific by sharing Taiwan’s experience with regional partners and building a cybersecurity information-sharing platform. Ideally, this would boost the development of the cybersecurity industry in the region, as well as cultivate and recruit skilled talent. Moreover, the Department of Cyber Security and the American Institute in Taiwan co-hosted and organized the November 2019 Cyber Offensive and Defensive Exercise, which set a new milestone for bilateral collaboration in cybersecurity and exhibiting the ROC’s cyberdefense capabilities.<sup>15</sup>

Overall, Taiwan’s cybersecurity challenges are an ongoing battle. The complex cross-strait political situation impedes the ROC’s ability to engage in international cybersecurity cooperation. Since 2019 the government’s many collaborations and demonstrations of its technological ability to defend against cyberattacks and organized advanced persistent threats have focused attention on Taiwan. Through the Tsai administration’s efforts, Taiwan has chosen to play the role of regional cybersecurity facilitator in exchange for more cross-country information sharing and cooperation with its regional friends. ◆

---

<sup>13</sup> “Tsai Reiterates Taiwan’s Commitment to Free, Open Indo-Pacific,” *Taiwan Today*, April 17, 2019 ~ <https://taiwantoday.tw/news.php?unit=2,6,10,15,18&post=153285>.

<sup>14</sup> Zheng Ling, “Yintaizianlian mengcheng li, AIT: Zianbu zhishizheng zhiyi ti” [The Set Up of the Indo-Pacific Cybersecurity Alliance, AIT: Cybersecurity Is More than a Political Issue], *Radio Taiwan International*, May 30, 2019 ~ <https://www.rti.org.tw/news/view/id/2022452>.

<sup>15</sup> “U.S. and Taiwan Hold First Joint Cyber-War Exercise,” *BBC*, November 4, 2019 ~ <https://www.bbc.com/news/technology-50289974>.

## Positioning ASEAN in Cyberspace

*Elina Noor*

The Association of Southeast Asian Nations (ASEAN) has long been a target of cyber campaigns. Networks and systems within the ASEAN Secretariat, as well as among its member states, have been compromised by sophisticated tactics, techniques, and procedures that point to advanced persistent threat (APT) actors sponsored by states. These attacks are hardly surprising given the strategic value of the ASEAN region. Nevertheless, despite ASEAN’s pledge in its charter to “respond effectively...to all forms of threats, transnational crimes, and transboundary challenges,” the regional grouping has never responded to these cyberattacks in any explicit or direct manner.<sup>1</sup>

This essay argues that ASEAN has instead chosen to manage international security in cyberspace in a more comprehensive manner, true to its pragmatic, nonconfrontational, and accommodating character. The essay is divided into three parts. First, it discusses how ASEAN’s priorities in the digital space have evolved since the 1990s in line with the region’s own needs and interests, as well as in response to the external environment. The second section outlines ASEAN’s cyberthreat landscape from a geopolitical perspective, offering brief case studies of state-sponsored cyberespionage and providing insight into why ASEAN’s response has been muted despite the serious implications of the sustained cyber campaigns against it. The final part examines ASEAN’s preference for multilateralism and capacity building when managing the threat of international cyberspace insecurity.

### *Priorities, Platforms, and Programs*

Having carved a long arc of efforts to leverage the internet’s economic potential, ASEAN is no newcomer to the digital space. In 1996, ASEAN, then a group of seven member states, gathered to discuss the opportunities

---

ELINA NOOR is an Associate Professor at the Daniel K. Inouye Asia-Pacific Center for Security Studies in Hawaii (United States). She can be reached at <noore@apcss.org>.

NOTE ~ The views expressed here are those of the author and do not necessarily reflect those of the institutions the author is affiliated with.

<sup>1</sup> Association of Southeast Asian Nations (ASEAN), *The ASEAN Charter* (Jakarta, November 2007), art. 1 (8) ~ <https://asean.org/wp-content/uploads/images/archive/publications/ASEAN-Charter.pdf>.

and challenges of the internet. Even in those dial-up years of the World Wide Web, the meeting participants foresaw the internet's "great potential for business, information and cultural exchange."<sup>2</sup> In the decades since, ASEAN has been both proactive and reactive to cyber-related events. Although the grouping has maintained a steady effort to prepare its citizens for the digital world through initiatives like the e-ASEAN framework agreement and information and communications technology (ICT) capacity building,<sup>3</sup> ASEAN has also been forced to respond to a rise in cybercrime,<sup>4</sup> terrorist use of the internet,<sup>5</sup> and, more recently, the dissemination of disinformation and misinformation.<sup>6</sup>

These issues, however, are subsumed by the larger priority of creating access to human resource and infrastructure capacity for ASEAN's combined population of over 600 million to capitalize on the promises of the internet. With Southeast Asia's internet economy hitting \$100 billion in 2019, and 90% of the region's 360 million internet users connecting primarily through their mobile devices, the economics and governance of cyberspace will only grow more important for ASEAN.<sup>7</sup> Despite disparities in the maturity of the member states in the cyber domain, the aspiration of a technologically enabled region is evident in the grouping's many ambitious initiatives. These include the ASEAN ICT Masterplan 2020, the Masterplan on ASEAN Connectivity 2025, and the ASEAN Smart Cities Network. ASEAN's vision, as expressed in these various documents, is the

<sup>2</sup> "Joint Press Release of the ASEAN Forum on Internet," ASEAN, Press Release, September 2–4, 1996 ~ [https://asean.org/?static\\_post=joint-press-release-of-the-asean-forum-on-internet-singapore-2-4-september-1996](https://asean.org/?static_post=joint-press-release-of-the-asean-forum-on-internet-singapore-2-4-september-1996).

<sup>3</sup> ASEAN, "e-ASEAN Framework Agreement," November 2000 ~ [https://asean.org/?static\\_post=e-asean-framework-agreement](https://asean.org/?static_post=e-asean-framework-agreement); and ASEAN, "Brunei Action Plan 'Enhancing ICT Competitiveness: Capacity Building,'" September 2006 ~ <https://asean.org/brunei-action-plan-enhancing-ict-competitiveness-capacity-building>.

<sup>4</sup> See, for example, ASEAN, "Joint Communiqué of the Third ASEAN Ministerial Meeting on Transnational Crime (AMMTC)," October 2001 ~ [https://asean.org/?static\\_post=joint-communicue-of-the-third-asean-ministerial-meeting-on-transnational-crime-ammtc-singapore-11-october-2001](https://asean.org/?static_post=joint-communicue-of-the-third-asean-ministerial-meeting-on-transnational-crime-ammtc-singapore-11-october-2001).

<sup>5</sup> See, for example, ASEAN, "Chairman's Statement of the Thirteenth ASEAN Regional Forum," July 2006 ~ <https://asean.org/chairman-s-statement-of-the-thirteenth-asean-regional-forum-kuala-lumpur>; and ASEAN, "ASEAN Regional Forum (ARF) Statement on Preventing and Countering Terrorism and Violent Extremism Conducive to Terrorism (VECT)," August 2019 ~ [http://aseanregionalforum.asean.org/wp-content/uploads/2019/08/ARF-Statement-on-Counter-Terrorism-and-VECT\\_FINAL.pdf](http://aseanregionalforum.asean.org/wp-content/uploads/2019/08/ARF-Statement-on-Counter-Terrorism-and-VECT_FINAL.pdf).

<sup>6</sup> See, for example, ASEAN, "Framework and Joint Declaration to Minimise the Harmful Effect of Fake News," 14th Conference of the ASEAN Ministers Responsible for Information, May 2018 ~ <https://asean.org/storage/2012/05/Annex-5-Framework-Declr-Fake-News.pdf>.

<sup>7</sup> Google, Temasek, and Bain and Company, "e-Conomy SEA 2019: Swipe Up and to the Right—Southeast Asia's \$100 Billion Internet Economy," October 2019 ~ [https://www.blog.google/documents/47/SEA\\_Internet\\_Economy\\_Report\\_2019.pdf](https://www.blog.google/documents/47/SEA_Internet_Economy_Report_2019.pdf).

consolidation of a connected, innovative, inclusive, integrated, and resilient ASEAN Community that is able to assert its regional identity, unity, and centrality in engaging with the rest of the world.

To be sure, ASEAN has managed these multiple threads as expansively as possible. Within the ASEAN-led architecture at the ministerial level, cyber issues are discussed at the ASEAN Regional Forum, ASEAN Defence Ministers' Meeting, ASEAN Ministerial Meeting on Transnational Crime, ASEAN Digital Ministers' Meeting, and the ASEAN Ministerial Conference on Cybersecurity. These meetings are preceded and replicated by senior officials and in expert working groups at regularly scheduled intervals as well as in intersessional consultations. In the near future, an ASEAN Coordinating Committee on Cybersecurity will be established to strengthen cross-sectoral coordination on cybersecurity in the region.<sup>8</sup> Yet the statements that are issued from these meetings often seem staid, at best, and obtusely deflective of grim realities, at worst.

### *Threat Landscape: Geopolitics and Cyberspace*

In August 2013, two days before the start of the Special ASEAN-China Foreign Ministers' Meeting in Beijing, a computer exploit was planted in an internal document authored by an ASEAN official for the meeting. The implant was designed to communicate with a malicious command-and-control domain to exfiltrate information. That domain itself was registered to an email address very similar to—but different from—one used by a Philippine government official working on ASEAN affairs.<sup>9</sup> ThreatConnect concluded that this example, along with other weaponized documents targeted at commercial, media, and military organizations around Southeast Asia, were “likely the direct operational result of the People’s Republic of China (PRC) government’s interest in gaining intelligence” on the South China Sea dispute.<sup>10</sup>

The next year, following the disappearance of MH370, the Malaysian airliner that disappeared en route to Beijing, there was a marked uptick in cyberoperations targeting nations involved in the search for the plane. Kaspersky Lab attributed these and other linked attacks to the

---

<sup>8</sup> ASEAN, “Advancing Partnership for Sustainability,” Chairman’s Statement of the 35th ASEAN Summit, November 2019 [~ https://asean.org/storage/2019/11/Chairs-Statement-of-the-35th-ASEAN-Summit-FINAL.pdf](https://asean.org/storage/2019/11/Chairs-Statement-of-the-35th-ASEAN-Summit-FINAL.pdf).

<sup>9</sup> “Piercing the Cow’s Tongue: China Targeting South China Seas Nations,” ThreatConnect, May 19, 2014 [~ https://threatconnect.com/blog/piercing-the-cows-tongue-china-targeting-south-china-seas-nations](https://threatconnect.com/blog/piercing-the-cows-tongue-china-targeting-south-china-seas-nations).

<sup>10</sup> *Ibid.*

Chinese-language APT actor Naikon.<sup>11</sup> This group was mostly active in Southeast Asia and Nepal, and particularly targeted the security and military apparatuses of countries in the region. For at least five years prior to the airliner's disappearance, many of Naikon's spear-phishing attempts to collect geopolitical and MH370-related information were successful.<sup>12</sup>

In 2015, as tensions built up around the South China Sea, FireEye reported a similar APT actor: the APT30 threat group.<sup>13</sup> APT30 was responsible for operations that went back to at least 2005, compromising government and commercial targets for "key political, economic, and military information about the region."<sup>14</sup> Of note, APT30 sustained its activities for at least a decade with minimal changes to its *modus operandi*. This suggests not only a lack of discovery and adaptation by APT30's victims, but also the group's confidence in the superiority of its methods to achieve its purpose. FireEye's technical analysis of APT30 led it to conclude that the attacker was state-sponsored, "most likely by the Chinese government."<sup>15</sup> ThreatConnect went a step further and attributed Naikon activities to the People's Liberation Army's Chengdu Military Region Second Technical Reconnaissance Bureau (Military Unit Cover Designator 78020).<sup>16</sup>

Although international law is silent on espionage, in cyberspace the line between information collection and military preparation is much less distinct than in the kinetic space.<sup>17</sup> Cyberspace complements and augments traditional analytical capabilities by enabling quicker and more comprehensive information collection by using the larger sets of data

<sup>11</sup> Costin Raiu and Maxim Golovkin, "The Chronicles of the Helsing APT: The Empire Strikes Back," Kaspersky Securelist, April 15, 2015 ~ <https://securelist.com/the-chronicles-of-the-helsing-apt-the-empire-strikes-back/69567>; Brian Donohue, "Naikon APT Steals Geopolitical Data from the South China Sea," Kaspersky Daily, May 19, 2015 ~ <https://www.kaspersky.com/blog/naikon-apt-south-china-sea/8696>; and Kurt Baumgartner and Maxim Golovkin, "The Naikon APT," Kaspersky Securelist, May 14, 2015 ~ <https://securelist.com/the-naikon-apt/69953>.

<sup>12</sup> Raiu and Golovkin, "The Chronicles of the Helsing APT."

<sup>13</sup> "APT30 and the Mechanics of a Long-Running Cyber Espionage Operation," FireEye, April 2015 ~ <https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/05/20081935/rpt-apt30.pdf>.

<sup>14</sup> *Ibid.*, 3.

<sup>15</sup> *Ibid.*

<sup>16</sup> "Project CameraShy: Closing the Aperture on China's Unit 78020," ThreatConnect, 2015 ~ [http://cdn2.hubspot.net/hubfs/454298/Project\\_CAMERASHY\\_ThreatConnect\\_Copyright\\_2015.pdf?t=1443030820943&submissionGuid=5c3af405-3e95-445f-a1d6-0e106eeb13c6](http://cdn2.hubspot.net/hubfs/454298/Project_CAMERASHY_ThreatConnect_Copyright_2015.pdf?t=1443030820943&submissionGuid=5c3af405-3e95-445f-a1d6-0e106eeb13c6); and "NanHaiShu: RATing the South China Sea," F-Secure Labs, July 2016 ~ [https://www.f-secure.com/documents/996508/1030745/nanhaishu\\_whitepaper.pdf](https://www.f-secure.com/documents/996508/1030745/nanhaishu_whitepaper.pdf).

<sup>17</sup> U.S. military doctrine specifies joint intelligence preparation of the operational environment and intelligence preparation of the battlespace as key analytical tools that directly support command-and-control planning and direction processes. See Joint Chiefs of Staff, *Joint Publication 2-0, Joint Intelligence* (Washington, D.C., 2013) ~ [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2\\_0.pdf](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf).

and resources available. The lag time between information collection, intelligence analysis, and logistical surge in the physical battlespace can thus be shortened through persistent cyber campaigns. This can have significant repercussions in areas such as the territorial disputes in the South China Sea. The discovery of these APTs should therefore be highly disconcerting for ASEAN, especially given the buildup of military installations in the South China Sea over the last decade. Yet neither ASEAN nor any of its individual member states has publicly commented on these cyberoperations.

Diplomatic sensitivities surrounding espionage are an obvious explanation for the absence of response, but there are at least three other reasons: political will, legal uncertainty, and lack of capacity. First, the decision to attribute attacks is ultimately a political call. The reality is that the identified APTs form only a part of Southeast Asia's total threat constellation, and even certain ASEAN member states have been implicated in similar APT activities.<sup>18</sup> While corroborated technical analyses are highly valuable in identifying threat actors in cyberspace, credible attribution requires a thorough assessment involving human, signals, and other intelligence capabilities. Above all, it demands complex political decision-making in an age of global supply chains, connectivity, and interdependence. For ASEAN, an organization of disparate countries grappling with varying levels of development and sometimes conflicting national and regional interests, this political calculus often militates naming and shaming perpetrators.

Second, although the applicability of international law in cyberspace is generally accepted worldwide, the specifics of exactly how it applies are still undecided.<sup>19</sup> There remains vigorous debate about the types of cyber breaches that meet the kinetic threshold of an armed attack, the parameters of the self-defense provision in international law, and the types of recourse available to states affected by cyberattacks, among many other issues. And third, even if cyberattacks contravene national laws, not all ASEAN member states have the requisite legal, technical, or judicial capacity to prosecute cyber-related offences.<sup>20</sup> What is the value of attribution without effective redress, especially taking into account possible retaliation?

---

<sup>18</sup> Jason Thomas, "Cyber Warfare in Vietnam," ASEAN Post, October 4, 2019 [~ https://theaseanpost.com/article/cyber-warfare-vietnam](https://theaseanpost.com/article/cyber-warfare-vietnam).

<sup>19</sup> UN General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security," A/RES/70/237, December 30, 2015 [~ https://undocs.org/A/RES/70/237](https://undocs.org/A/RES/70/237).

<sup>20</sup> See, for example, International Telecommunication Union (ITU), *Global Cybersecurity Index 2018* (Geneva: ITU, 2019) [~ https://www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf).

## *Multilateralism and Capacity Building*

Despite ASEAN's general aversion to tackling complex political-security issues head on, the organization has made laudable progress in keeping pace with international deliberations on the governance architecture of cyberspace. Two years ago, issues such as norms of responsible state behavior and international law in cyberspace were still under the radar in Southeast Asian policy circles. After all, only two Southeast Asian representatives were ever on one of the five iterations between 2004 and 2017 of the UN Group of Governmental Experts (UNGGE) that drafted resolutions on the "Developments in the Field of Information and Telecommunications in the Context of International Security." Malaysia participated in 2004–5 and 2014–15, and Indonesia in 2012–13 and 2016–17.

It was significant, therefore, that in 2018 all ten ASEAN ministers at the ASEAN Ministerial Conference on Cybersecurity agreed to subscribe in principle to the 2015 UNGGE's eleven voluntary, nonbinding norms of responsible state behavior in cyberspace.<sup>21</sup> Only a few months later, the "ASEAN Leaders' Statement on Cybersecurity Cooperation" affirmed this commitment.<sup>22</sup> To be sure, the primarily economic lens through which ASEAN views the digital realm—that is, as an "enabler of economic progress, enhanced, regional connectivity, and the betterment of living standards for all"—was well-reflected in the document's preamble, but the leaders' statement demonstrates that the region is assuredly finding its voice in the evolving debate on responsible state behavior in cyberspace. In acknowledging the need for a common regional understanding of norms, member states have chosen to work multilaterally through ASEAN frameworks, as well as through the United Nations. ASEAN's emphasis on confidence and capacity building for a rules-based cyberspace further accords with its pragmatic, incremental approach to matters of peace and security.

Singapore has largely led the regional charge since its 2018 ASEAN chairmanship, though it began laying the groundwork a few years prior when it launched the ASEAN Cyber Capacity Programme and hosted the first ASEAN Ministerial Conference on Cybersecurity. The program has

---

<sup>21</sup> UN General Assembly, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," Note by the Secretary-General, A/70/174, July 22, 2015 ~ <https://undocs.org/A/70/174>.

<sup>22</sup> ASEAN, "ASEAN Leaders' Statement on Cybersecurity Cooperation," April 27, 2018 ~ <https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf>.



grown from a S\$10 million initiative to the S\$30 million ASEAN-Singapore Cyber Centre of Excellence. The center’s focus on training, research, and information exchange on strategy, policy, legislation, and operations related to cyberspace was deliberately designed to align cyberdiplomacy efforts with operational issues. This, in turn, facilitates regional coordination toward a unified perspective on international platforms.<sup>23</sup> Crucially, the ASEAN-Singapore Cyber Centre of Excellence is ASEAN-centric, open, inclusive, and collaborative. It has been receptive of offers of support from Australia, Canada, the European Union, South Korea, New Zealand, and the United Kingdom. In a similar but separate vein, in 2018, Thailand and Japan launched the ASEAN-Japan Cybersecurity Capacity Building Centre in Bangkok. And additionally, last year ASEAN and the United States held their inaugural Cyber Policy Dialogue to discuss the international cyber environment, joint cooperation, and capacity-building priorities.<sup>24</sup>

When the United States and Russia proposed parallel and potentially competing tracks of discussion at the United Nations on developments in the field of information and telecommunications in the context of international security, most ASEAN member states chose to support both.<sup>25</sup> Singapore argued that both the U.S.-proposed UNGGE and Russian-proposed Open-Ended Working Group (OEWG) “can and should be complementary,” and that it was “important for the major players to work together, in the spirit of consensus, mutual respect, and mutual trust.”<sup>26</sup> Fortunately, the UNGGE and OEWG have been led by collaborative chairs who made clear at the outset that the two tracks would operate complementarily. Indeed, both chairs have frequently appeared together at meetings, and the UNGGE’s smaller quorum has benefited from participating in the OEWG’s larger consultative sessions. Departing from

---

<sup>23</sup> S. Iswaran, “Opening Remarks by Mr. S. Iswaran, Minister for Communications and Information, at the ASEAN Ministerial Conference on Cybersecurity,” Ministry of Communications and Information (Singapore), September 19, 2018 [https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2018/9/opening-remarks-by-mr-s-iswaran-at-the-asean-ministerial-conference-on-cybersecurity?page=1\\_6](https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2018/9/opening-remarks-by-mr-s-iswaran-at-the-asean-ministerial-conference-on-cybersecurity?page=1_6).

<sup>24</sup> “Co-Chairs’ Statement on the Inaugural ASEAN-U.S. Cyber Policy Dialogue,” U.S. Department of State, October 3, 2019 <https://www.state.gov/co-chairs-statement-on-the-inaugural-asean-u-s-cyber-policy-dialogue>.

<sup>25</sup> Myanmar co-sponsored Russia’s proposal of an open-ended working group and abstained from voting on the U.S. proposal for another UNGGE. Cambodia and Laos similarly abstained. See UN General Assembly, “Developments in the Field of Information and Telecommunications in the Context of International Security,” Report of the First Committee, A/73/505, November 19, 2018 <https://undocs.org/A/73/505>.

<sup>26</sup> UN General Assembly, “Developments in the Field of Information and Telecommunications in the Context of International Security,” Report of the Secretary-General, A/74/120, June 24, 2019, 33 <https://undocs.org/A/74/120>.

its more exclusive deliberations—per the OEWG’s example—the current UNGGE has also held its own informal consultative sessions with other UN member states as well as with regional organizations.

In its interaction with the UNGGE, ASEAN members stressed that while states could make a stronger commitment to norms, flexibility would be key in regional implementation. The ASEAN Regional Forum’s work in compiling a point-of-contact directory was highlighted as a concrete example of enhancing confidence-building measures. ASEAN further underscored the importance of capacity building as a “two-way street where both the donor and beneficiary states would learn from each other.”<sup>27</sup>

It is clear that as cyberspace becomes an increasingly contested environment against the backdrop of a sharpening major-power rivalry, ASEAN’s approach is to consolidate centrality while continuing to engage—if not, enmesh<sup>28</sup>—its larger dialogue partners in cooperative efforts. Even as ASEAN will no doubt remain a rich target of geopolitically motivated cyberattacks, it will nonetheless need to focus on building its collective capacity on cyber issues across all fronts to effectively project its perspectives at the international level. As ASEAN forges ahead with its many master plans to plug the region into a digital future, it would do well to remember that the prosperity of the ASEAN Community can only be as robust as the security of its infrastructure. ◆

---

<sup>27</sup> United Nations, “Informal Consultative Meeting of the Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security,” Chair’s Summary, December 5–6, 2019 ≈ <https://www.un.org/disarmament/wp-content/uploads/2019/12/gge-chair-summary-informal-consultative-meeting-5-6-dec-20191.pdf>.

<sup>28</sup> Evelyn Goh, “Great Powers and Hierarchical Order in Southeast Asia: Analyzing Regional Security Strategies,” *International Security* 32, no. 3 (2007/2008): 113–57.