Eroding Global Stability: The Cybersecurity Strategies Of China, Russia, North Korea, And Iran

Description

Editorâ??s note: This article is part of Project Cyber, which explores and characterizes the myriad threats facing the United States and its allies in cyberspace, the information environment, and conventional and irregular spaces. Please contact us if you would like to propose an article, podcast, or event environment. We invite you to contribute to the discussion, explore the difficult questions, and help.

In recent years, declarations like â??no-limits partnership,â?• â??comprehensive agreement,â?• and â??security partnershipâ?• between the United Statesâ?? adversaries have become increasingly common. On May 16, 2024, Russian President Vladimir Putin and Chinese Communist Party Leader Xi Jinping reaffirmed their comprehensive partnership during their historic 43rd meeting. Since Russia invaded Ukraine on February 24, 2022, Russian-Iranian collaboration has reached new levels, with Iranian drones becoming a familiar site over the battlefields. North Korea too, has upped its cooperation with Russia, working closely on schemes to avoid Western sanctions and even signing a mutual defense pact on June 19, 2024. The extent to which Americaâ??s adversaries cooperate on cybersecurity remains less understood but is a growing concern.

However, as unified Western actions against rogue and adversarial states have increased (e.g., sanctions, public shaming, etc.) and hot wars roil Ukraine and Israel, the agreements and cooperation among China, Russia, North Korea, and Iran have similarly grown stronger and more unified. In this context, the cybersecurity strategies of China, Russia, North Korea, and Iran have emerged as significant and irregular threats to global stability, threatening the contemporary geopolitical landscape. Furthermore, each nation has developed sophisticated cyber capabilities designed to asymmetrically attack the international security frameworks established by NATO (North Atlantic Treaty Organization) and Western powers. It is, therefore, important to assess how US adversaries collaborate in cyberspace and are using asymmetric and irregular tactics to undermine the liberal world order.

https://irregularwarfareinsider.podbean.com/e/eroding-global-stability-the-cybersecurity-strategies-of-china-russia-north-korea-and-iran/

Strategic Cybersecurity Alliances

State-sponsored malicious cyber actors from China, Russia, North Korea, and Iran increasingly dominate the cyber threat landscape and are driven by geopolitical, economic, and military objectives. Moreover, adversaries develop capabilities for strategic ends, blurring the line between irregular and conventional warfare in cyberspace. Importantly, their efforts are not strictly unilateral, as evidence increasingly points toward formal and informal collaboration among rogue states in cyberspace. For example, Chinese and Russian cyber actors have been known to share malware and exploit kits, enabling more sophisticated attacks. Additionally, joint operations, like coordinated disinformation campaigns, have been observed, highlighting our adversariesâ?? willingness to coordinate influence operations.

Furthermore, China, Russia, North Korea, and Iran also leverage emerging technologies, like artificial intelligence (AI) and generative AI, to enhance their cyber capabilities. Disruptive technologies can enhance already sophisticated cyber operations and allow for automated attacks, deep-fakes, and advanced social engineering tactics. AI in cyber operations poses new challenges for cybersecurity defenders as it increases the complexity, scale, and pace of potential attacks. How these nations use cyber capabilities, and leverage asymmetric advantages for strategic ends, underscores the need for greater international cooperation and more robust policy coordination to counter these irregular threats.

Peopleâ??s Republic of China

Chinaâ??s journey toward becoming a cyber power began in the early 2000s. At the helm is the Central Commission for Cybersecurity and Informatization (CCCI), chaired by President Xi Jinping, as well as the Ministry of State Security, the Ministry of Public Security, and the Cyberspace Administration of China. The â??Great Firewall of Chinaâ?• exemplifies Chinaâ??s commitment to information control, both domestically and internationally, and allows government control over the internet and information. By limiting domestic information access, the government controls the populationâ??s understanding of other nations and restricts external access to Chinese-focused content, sites, etc.

A key component of Chinaâ??s cyber strategy is the concept of military-civil fusion, which encourages collaboration between the private sector and military and integrates resources. The fusion is evident in the activities of major Chinese tech firms like Huawei, Alibaba, and Tencent, which play significant roles in advancing Chinaâ??s cyber ambitions and provide irregular approaches to securing technological control over an increasing percentage of the worldâ??s telecommunications and digital infrastructure outside China.

Chinaâ??s cyber strategy is also characterized by its use of state-sponsored hacking groups to conduct widespread and far-reaching cyber espionage and sabotage campaigns. The discovery of Volt

Typhoon, a Chinese state-sponsored hacking group, and its activities underscores Chinaâ??s focus on gaining asymmetric advantage over the US and its allies by gaining persistent access to their critical infrastructure. The group uses the unconventional and irregular warfare tactic of â??living off the land ,â?• utilizing existing resources in the operating system of the targeted devices and systems rather than introducing new files that could trigger cybersecurity sensors or be more easily detected through forensic analysis. Volt Typhoonâ??s objective appears to be long-term persistence within the target environment, or pre-positioning, giving China the placement and access to conduct future acts of sabotage and disruption.

Russian Federation

Russiaâ??s evolution as a cyber power began in the late 1990s and early 2000s and is encapsulated in initiatives like, the Information Security Doctrine of the Russian Federation. Moreover, Russiaâ??s cyber strategy is deeply rooted in the concept of political warfare and its understanding of cyberspace as a theater of military operations akin to land, sea, air, and space. However, political warfare for Russia includes a cognitive dimension that influences how they leverage cyberspace to achieve political outcomes. Russiaâ??s approach to cyberspace, therefore, differs from the concepts espoused by US and other NATO-aligned nations and is characterized by a decentralized and asymmetric approach to cyber operations.

The Russian government views cyberspace as a critical domain for exerting influence and achieving geopolitical goals and their cyber ecosystem is a complicated tangle of state and non-state actors. The Federal Security Service, the Foreign Intelligence Service, and the Main Directorate of the General Staff of the Armed Forces of the Russian Federation all have cyber units that conduct operations domestically and internationally. These agencies also recruit cybercriminals to carry out operations on their behalf, providing them with legal protection and resources in exchange for their services.

A key component of Russiaâ??s cyber strategy is the concept of information confrontation, an approach that integrates cyber operations, psychological operations, electronic warfare, and traditional military operations to achieve strategic objectives. Russia has been implicated in numerous cyber espionage and disruptive activities targeting both governmental and private sector entities worldwide. For instance, Russian cyber actors have been implicated in attacks on US election systems, energy grid, water systems, and other critical sectors. The operations are designed to foster instability, leveraging cyber operations, cyber espionage, influence campaigns, and other asymmetric tactics as force multipliers in geopolitical conflicts.

Furthermore, Russia has a long history of integrating cyber operations into its broader military strategy, relying on cyber capabilities during conflicts, like its ongoing invasion of Ukraine. The integration of cyber operations into Russiaâ??s broader political warfare framework, reminiscent of Soviet-era â??active measures,â?• further complicates attribution and response measures. Importantly, Russiaâ??s approach to leveraging cyber operations and capabilities to disrupt critical infrastructure, spread disinformation, and conduct espionage underscores its asymmetric and irregular approach to confrontation with Western powers.

Democratic Peopleâ??s Republic of Korea

North Koreaâ??s growth as a cyber power also began in the early 2000s and is largely focused on leveraging its cyber capabilities to circumvent economic sanctions and finance its regime through illicit means. Directing North Koreaâ??s cyber activity is its Reconnaissance General Bureau, with â??Bureau 121â?• being responsible for conducting cyber espionage, financial theft, and disruptive cyberattacks. However, North Koreaâ??s cyber capabilities are divided among several units, including the now-infamous Lazarus Group, Kimsuky, and APT37, known for their sophisticated cyber operations.

North Koreaâ??s cyber strategy seeks to develop defensive and offensive capabilities. On the defensive side, North Korea has invested heavily in protecting its critical infrastructure and sensitive data from cyberattacks. On the offensive side, North Korea has developed various capabilities to conduct cyber espionage, disinformation campaigns, and disruptive cyberattacks.

North Korea has been implicated in numerous cyber espionage and disruptive activities targeting both governmental and private sector entities worldwide. One of the most notable North Korean cyber operations is the 2014 Sony Pictures hack but the most significant is likely the 2017 WannaCry ransomware. WannaCry ransomware infected more than 200,000 computers in over 150 countries, causing widespread disruption by encrypting files on infected computers and demanding ransom payments in cryptocurrency. The attack is an example of North Koreaâ??s ability to conduct large-scale disruptive cyber operations and the regimeâ??s willingness to engage in asymmetric and irregular attacks to fund its government.

Islamic Republic of Iran

Iranâ??s cyber proliferation began after the Stuxnet attack in 2010, an attack that targeted Iranâ??s nuclear enrichment facilities. Stuxnet highlighted the vulnerability of Iranâ??s critical infrastructure to foreign intervention and pushed the regime to invest heavily in developing cyber capabilities. As a result, Iranâ??s cyber strategy has been focused on retaliatory cyber capabilities and driven by its perception that it is engaged in an ongoing conflict with the West over its nuclear program and other geopolitical issues. Unlike China and Russia, which primarily engage in cyber espionage, or North

Korea, which engages in cybercrime and theft, Iranâ??s regime views cyber operations as a means of retaliating against sanctions and other forms of pressure from the international community.

Similar to North Korea, Iranâ??s cyber strategy focuses on the development of defensive and offensive capabilities. On the defensive side, Iran has invested in protecting its critical infrastructure and sensitive data from cyberattacks and crafted defensive cyber doctrine to guide how the regime repels and mitigates cyberattacks against Iran. Offensively, Iran has developed various capabilities to conduct cyber espionage, disinformation campaigns, and disruptive cyberattacks.

Iranâ??s focus on retaliatory capabilities makes them a particularly volatile cyber actor, that is willing and able to launch disruptive attacks with little warning. For example, a significant Iranian cyber operation was Operation Ababil, which disrupted services at US financial institutions through a series of distributed denial-of-service attacks between 2011 and 2013. The Iranian hacking collective, Izz ad-Din al-Qassam Cyber Fighters, carried out the attacks and is believed to be state-sponsored. The operation was designed to impact major US banks and is understood as the regimeâ??s retaliation against economic sanctions.

To date, Iran has been implicated in numerous cyber espionage and disruptive activities targeting both governmental and private sector entities worldwide. The Shamoon attack, which targeted Saudi Aramco in 2012, is among the most notable Iranian cyber operations. The attack used malware to cause irreparable damage to thousands of computers, rendering them useless by overwriting the master boot record, partition tables, and most files with random data. Shamoon demonstrated Iranâ??s ability to conduct large-scale destructive cyberattacks and highlighted its willingness to use asymmetric attacks to achieve strategic goals.

Implications for Global Security

Chinaâ??s, Russiaâ??s, North Koreaâ??s, and Iranâ??s collaborative and individual cyber strategies have significant implications for global security. Their activities undermine the stability provided by NATO and Western powers, posing complex, asymmetric, and irregular challenges to international norms and, more broadly, cybersecurity. State-sponsored cyber operations, like state-sponsored terrorism or political violence, are sophisticated attempts to erode trust in digital infrastructure and government or institutional functions by disrupting the integrity, availability or confidentiality of data, services, and other aspects of online and physical security. For example, Chinaâ??s cyber activities, including Volt Typhoon, have heightened tensions with the US, particularly over Taiwan. Similarly, Russian cyber operations have exacerbated conflicts in the former Soviet Bloc nations and strained relations with Western nations.

The cyber collaboration between China, Russia, North Korea, and Iran varies in scope; however, its aim always aligns with political goals that negatively impact the existing rules-based world order. For example, Russia leverages malware to attack Ukraine, which was developed by Scarab, a Chinese government-linked cyber group, and shares techniques on how best to leverage AI for attacking targets and â??living off the landâ?• persistence to avoid detection by cyber defenders.

Moreover, the cyber strategiesâ?? collaborative and sophisticated characteristics pose significant challenges for cybersecurity defenders. Traditional cybersecurity measures are often insufficient to counter the advanced tactics used by state-sponsored actors. NATO and Western powers must adopt a comprehensive approach that includes enhancing defensive capabilities, leveraging advanced technologies, fostering international cooperation, and developing offensive cyber strategies to effectively counter these threats. By doing so, they can safeguard the stability and security that have been our worldâ??s cornerstone since World War IIâ??s end.

Evan Morgan is the Founder of Cyber Defense Army, a cybersecurity consultancy and services firm that incorporates geopolitical risk in their cybersecurity practices for clients. He is a United States Air Force veteran.

The views expressed are those of the author(s) and do not reflect the official position of the Irregular Warfare Initiative, Princeton Universityâ??s Empirical Studies of Conflict Project, the Modern War Institute at West Point, or the United States Government.

Main Image: Capt. Taiwan Veney, cyber warfare operations officer, watches members of the 175th Cyberspace Operations Group in the Hunterâ??s Den at Warfield Air National Guard Base, Middle River, MD, June 3, 2017. (U.S. Air Force photo by J.M. Eddins Jr.)

If you value reading the Irregular Warfare Initiative, please consider supporting our work. And for the best gear, check out the IWI store for mugs, coasters, apparel, and other items.

Date Created
2024/08/01