US Threat Assessment

February 2024

Please see the Annual Threat Assessment of the U.S. Intelligence Community (PDF) and excerpts below, evidence of the cyber threat facing the U.S. and the world.

Technology
China seeks to become a world S&T superpower and to use this technological superiority for economic, political, and military gain. Beijing is implementing a whole-of-government effort to boost indigenous innovation and promote self-reliance, and is prioritizing advanced power and energy, AI, biotechnology, quantum information science, and semiconductors. Beijing is trying to fast-track its S&T development through investments, intellectual property (IP) acquisition and theft, cyber operations, talent recruitment, scientific and academic collaboration, and illicit procurements.

- In 2023, a key PRC state-owned enterprise has signaled its intention to channel at least $13.7 billion into emerging industries such as AI, advanced semiconductors, biotechnology, and new materials. China also announced its Global AI Governance Initiative to bolster international support for its vision of AI governance.
- China now rivals the United States in DNA-sequencing equipment and some foundational research. Beijing's large volume of genetic data potentially positions it to lead in precision medicine and agricultural biotechnology applications.
- China is making progress in producing advanced chips for cryptocurrency mining and cellular devices at the 7-nanometer (nm) level using existing equipment but will face challenges achieving high-quality, high-volume production of cutting-edge chips without access to extreme ultraviolet lithography tools. By 2025, 40 percent of all 28-nm legacy chips are projected to be produced in China, judging from the number of new factories expected to begin operating during the next two years.

Cyber
China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks. Beijing's cyber espionage pursuits and its industry's export of surveillance, information, and communications technologies increase the threats of aggressive cyber operations against the United States and the suppression of the free flow of information in cyberspace.

- PRC operations discovered by the U.S. private sector probably were intended to pre-position cyber-attacks against infrastructure in Guam and to enable disrupting communications between the United States and Asia.
- If Beijing believed that a major conflict with the United States were imminent, it would consider aggressive cyber operations against U.S. critical infrastructure and military assets. Such a strike would be designed to deter U.S. military action by impeding U.S. decision-making, inducing societal panic, and interfering with the deployment of U.S. forces.
- China leads the world in applying surveillance and censorship to monitor its population and repress dissent. Beijing conducts cyber intrusions targeted to affect U.S. and non-U.S. citizens beyond its borders—including journalists, dissidents, and individuals it views as threats—to counter views it considers critical of CCP narratives, policies, and actions.

Moscow will continue to employ all applicable sources of national power to advance its interests and try to undermine the United States and its allies, but it faces a number of challenges, such as severance from Western markets and technology and flight of human capital, in doing so. This will range from using energy to try to coerce cooperation and weaken Western unity on Ukraine, to military and security intimidation, malign influence, cyber operations, espionage, and subterfuge.

Russia will pose an enduring global cyber threat even as it prioritizes cyber operations for the Ukrainian war. Moscow views cyber disruptions as a foreign policy lever to shape other countries' decisions and continuously refines and employs its espionage, influence, and attack capabilities against a variety of targets.

- Russia maintains its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States as well as in allied and partner countries.

Cyber and Malign Influence Operations

Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied and partner networks and data. Tehran's opportunistic approach to cyber-attacks puts U.S. infrastructure at risk for being targeted, particularly as its previous attacks against Israeli targets show that Iran is willing to target countries with stronger cyber capabilities than itself. Iran will continue to conduct malign influence operations in the Middle East and in other regions, including trying to undermine U.S. political processes and amplify discord.

Ahead of the U.S. election in 2024, Iran may attempt to conduct influence operations aimed at U.S. interests, including targeting U.S. elections, having demonstrated a willingness and capability to do so in the past.

- During the U.S. election cycle in 2020, Iranian cyber actors obtained or attempted to obtain U.S. voter information, sent threatening emails to voters, and disseminated disinformation about the election. The same Iranian actors have evolved their activities and developed a new set of techniques, combining cyber and influence capabilities, that Iran could deploy during the U.S. election cycle in 2024.

North Korean leader Kim Jong Un will continue to pursue nuclear and conventional military capabilities that threaten the United States and its allies, which will enable periodic aggressive actions as he tries to reshape the regional security environment in his favor. North Korea has emerged from its deepest period of isolation driven by a combination of nearly two decades of severe UN sanctions and its self-imposed COVID-19 lockdown. Today, it is pursuing stronger ties with China and Russia with the goal of increasing financial gains, diplomatic support, and defense cooperation. Kim almost certainly has no intentions of negotiating away his nuclear program, which he perceives to be a guarantor of regime security and national pride. In addition, Kim probably hopes that he can use his bourgeoning defense ties with Russia to pursue his goal of achieving international acceptance as a nuclear power.

- North Korea increasingly will engage in illicit activities, including cyber theft labor deployments and the import and export of UN-proscribed commodities, to fund regime priorities such as the WMD program.

North Korea's cyber program will pose a sophisticated and agile espionage, cybercrime, and attack threat. Pyongyang's cyber forces have matured and are fully capable of achieving a variety of strategic objectives against diverse targets, including a wider target set in the United States and South Korea. North Korea will continue its ongoing cyber campaign, particularly cryptocurrency heists; seek a broad variety of approaches to launder and cash out stolen cryptocurrency; and maintain a program of IT workers serving abroad to earn additional funds.

Cyber Crime

Transnational organized criminals involved in ransomware operations are improving their attacks, extorting funds, disrupting critical services, and exposing sensitive data. Important U.S. services and critical infrastructure such as health care, schools, and manufacturing continue to experience ransomware attacks; however, weak cyber defenses, coupled with efforts to digitize economies, have made low-income countries’ networks also attractive targets.

- The emergence of inexpensive and anonymizing online infrastructure combined with the growing profitability of ransomware has led to the proliferation, decentralization, and specialization of cyber criminal activity. This interconnected system has improved the efficiency and sophistication of ransomware attacks while also lowering the technical bar for entry for new actors.
- Transnational organized criminals sometimes cease operations temporarily in response to high-profile attention, law enforcement action, or disruption of infrastructure, although group members also find ways to rebrand, reconstitute, or renew their activities.
- Absent cooperative law enforcement from Russia or other countries that provide cyber criminals a safe haven or permissive environment, mitigation efforts will remain limited.