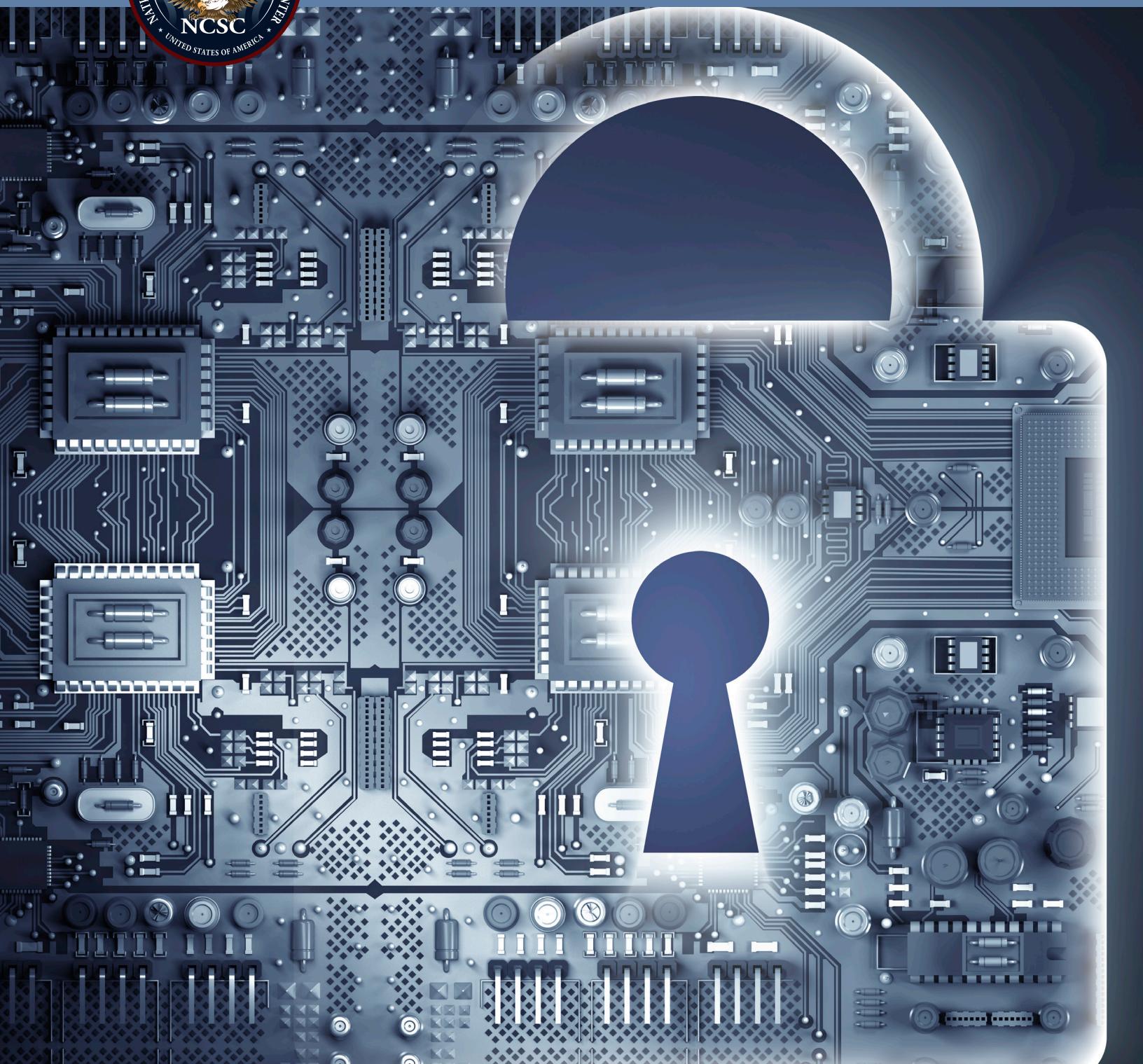
# Foreign Economic Espionage in Cyberspace

2018

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER




NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER
NCSC
UNITED STATES OF AMERICA

# Contents

# Executive Summary

In the 2011 report to Congress on *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace*, the Office of the National Counterintelligence Executive provided a baseline assessment of the many dangers facing the U.S. research, development, and manufacturing sectors when operating in cyberspace, the pervasive threats posed by foreign intelligence services and other threat actors, and the industries and technologies most likely at risk of espionage. The 2018 report provides additional insight into the most pervasive nation-state threats, and it includes a detailed breakout of the industrial sectors and technologies judged to be of highest interest to threat actors. It also discusses several potentially disruptive threat trends that warrant close attention.

## This report focuses on the following issues

***Foreign economic and industrial espionage against the United States continues to represent a significant threat to America's prosperity, security, and competitive advantage.*** Cyberspace remains a preferred operational domain for a wide range of industrial espionage threat actors, from adversarial nation-states, to commercial enterprises operating under state influence, to sponsored activities conducted by proxy hacker groups. Next-generation technologies, such as Artificial Intelligence (AI) and the Internet-of-Things (IoT) will introduce new vulnerabilities to U.S. networks for which the cybersecurity community remains largely unprepared. Building an effective response will require understanding economic espionage as a worldwide, multi-vector threat to the integrity of the U.S. economy and global trade.

***Foreign intelligence services—and threat actors working on their behalf—continue to represent the most persistent and pervasive cyber intelligence threat.*** China, Russia, and Iran stand out as three of the most capable and active cyber actors tied to economic espionage and the potential theft of U.S. trade secrets and proprietary information. Countries with closer ties to the United States also have conducted cyber espionage to obtain U.S. technology. Despite advances in cybersecurity, cyber espionage continues to offer threat actors a relatively low-cost, high-yield avenue of approach to a wide spectrum of intellectual property.

***A range of potentially disruptive threat trends warrant attention.*** Software supply chain infiltration already threatens the critical infrastructure sector and is poised to threaten other sectors. Meanwhile, new foreign laws and increased risks posed by foreign technology companies due to their ties to host governments, may present U.S. companies with previously unforeseen threats.

Cyber economic espionage *is but one facet* of the much larger, global economic espionage challenge. We look forward to engaging in the larger public discourse on mitigating the national economic harm caused by these threats.

# Scope Note

This report is submitted in compliance with the National Defense Authorization Act for Fiscal Year 2015, Section 1637, which requires that the President annually submit to Congress a report on foreign economic espionage and industrial espionage in cyberspace during the 12-month period preceding the submission of the report.

## Definitions of Key Terms

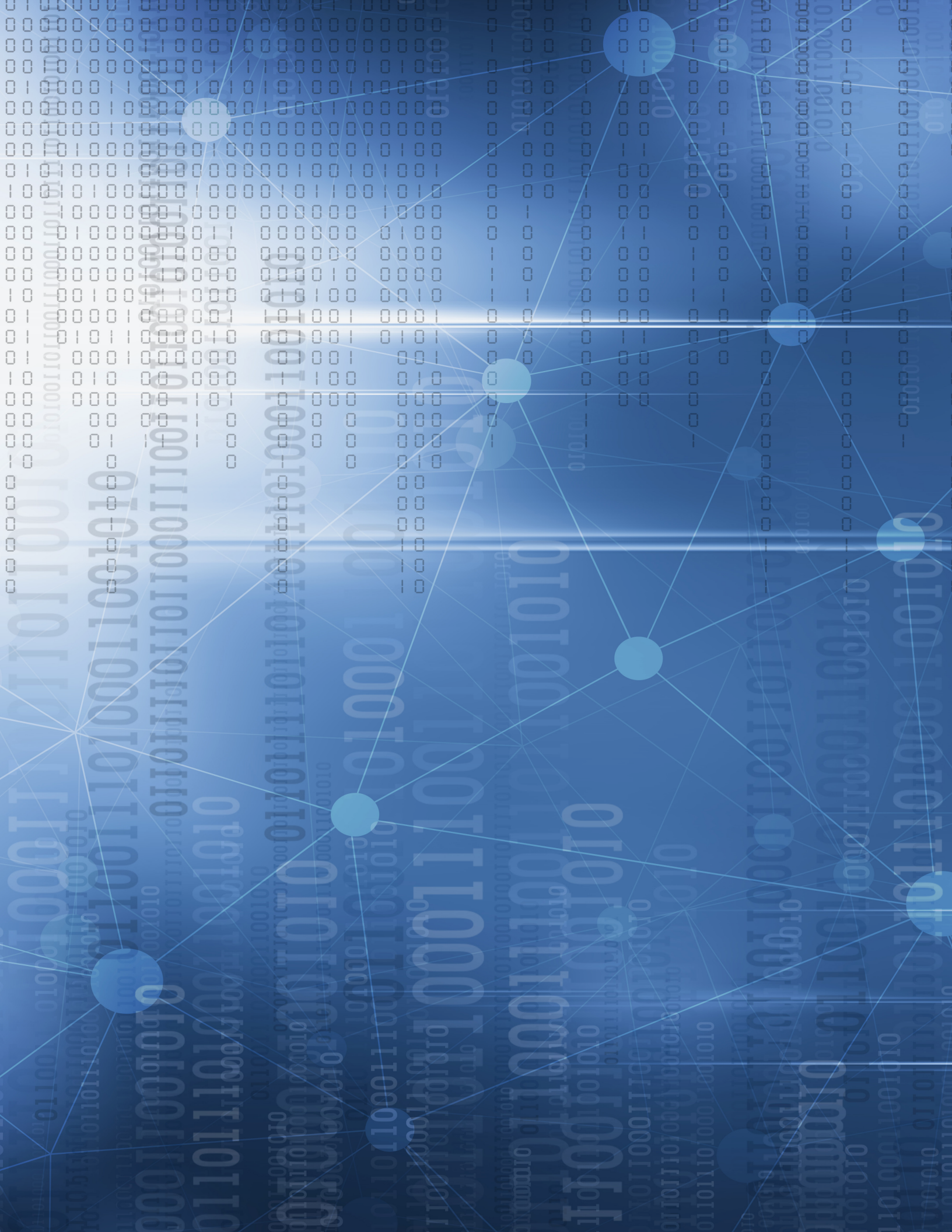
For the purpose of this report, key terms were defined according to definitions provided in Section 1637 of the National Defense Authorization Act for Fiscal Year 2015.

***Economic or Industrial Espionage*** means (a) stealing a trade secret or proprietary information or appropriating, taking, carrying away, or concealing, or by fraud, artifice, or deception obtaining, a trade secret or proprietary information without the authorization of the owner of the trade secret or proprietary information; (b) copying, duplicating, downloading, uploading, destroying, transmitting, delivering, sending, communicating, or conveying a trade secret or proprietary information without the authorization of the owner of the trade secret or proprietary information; or (c) knowingly receiving, buying, or possessing a trade secret or proprietary information that has been stolen or appropriated, obtained, or converted without the authorization of the owner of the trade secret or proprietary information.

***Cyberspace*** means (a) the interdependent network of information technology infrastructures; and (b) includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

## Contributors

The National Counterintelligence and Security Center (NCSC) compiled this report, with close support from the Cyber Threat Intelligence Integration Center (CTIIC), and with input and coordination from many U.S. Government organizations, including the Central Intelligence Agency (CIA), Defense Cyber Crime Center (DC3), Defense Intelligence Agency (DIA), Defense Security Service (DSS), Department of Energy (DoE), Department of Defense (DoD), Department of Homeland Security (DHS), Department of State (DoS), Department of Treasury (Treasury), Federal Bureau of Investigation (FBI), National Cyber Investigative Joint Task Force (NCIJTF), National Geospatial-Intelligence Agency (NGA), National Reconnaissance Office (NRO), National Security Agency (NSA), and Office of the Director of National Intelligence (ODNI).



# I. The Strategic Threat of Cyber Economic Espionage

Foreign economic and industrial espionage against the United States continues to represent a significant threat to America's prosperity, security, and competitive advantage. Cyberspace remains a preferred operational domain for a wide range of industrial espionage threat actors, from adversarial nation-states, to commercial enterprises operating under state influence, to sponsored activities conducted by proxy hacker groups. Next-generation technologies such as Artificial Intelligence (AI) and the Internet-of-Things (IoT) will introduce new vulnerabilities to U.S. networks for which the cybersecurity community remains largely unprepared. Building an effective response demands understanding economic espionage as a worldwide, multi-vector threat to the integrity of the U.S. economy and global trade.

The United States remains a global center for research, development, and innovation across multiple high-technology sectors. Federal research institutions, universities, and corporations are regularly targeted by online actors seeking all manner of proprietary information and the overall long-term trend remains worrisome.

While next generation technologies will introduce a range of qualitative advances in data storage, analytics, and computational capacity, they also present potential vulnerabilities for which the cybersecurity community remains largely unprepared. The solidification of cloud computing over the past decade as a global information industry standard, coupled with the deployment of technologies such as AI and IoT, will introduce unforeseen vulnerabilities to U.S. networks.

- **Cloud networks and IoT infrastructure are rapidly expanding the global online operational space.** Threat actors have already demonstrated how cloud can be used as a platform for cyber exploitation. As IoT and AI applications expand to empower everything from "smart homes" to "smart cities", billions of potentially unsecured network nodes will create an incalculably larger exploitation space for cyber threat actors.

- **Lack of industry standardization during this pivotal first-generation deployment period will likely hamper the development of comprehensive security solutions in the near-term.**

- **Building an effective response demands understanding economic espionage as a worldwide, multi-vector threat to the integrity of both the U.S. economy and global trade.** Whereas cyberspace is a preferred operational domain for economic espionage, it is but one of many. Sophisticated threat actors, such as adversarial nation-states, combine cyber exploitation with supply chain operations, human recruitment, and the acquisition of knowledge by foreign students in U.S. universities, as part of a strategic technology acquisition program.

# II. Threats from Foreign Countries

Foreign intelligence services—and threat actors working on their behalf—continue to represent the most persistent and pervasive cyber intelligence threat. China, Russia, and Iran stand out as three of the most capable and active cyber actors tied to economic espionage and the potential theft of U.S. trade secrets and proprietary information. Countries with closer ties to the United States have also conducted cyber espionage to obtain U.S. technology. Despite advances in cybersecurity, cyber espionage continues to offer threat actors a relatively low-cost, high-yield avenue of approach to a wide spectrum of intellectual property.

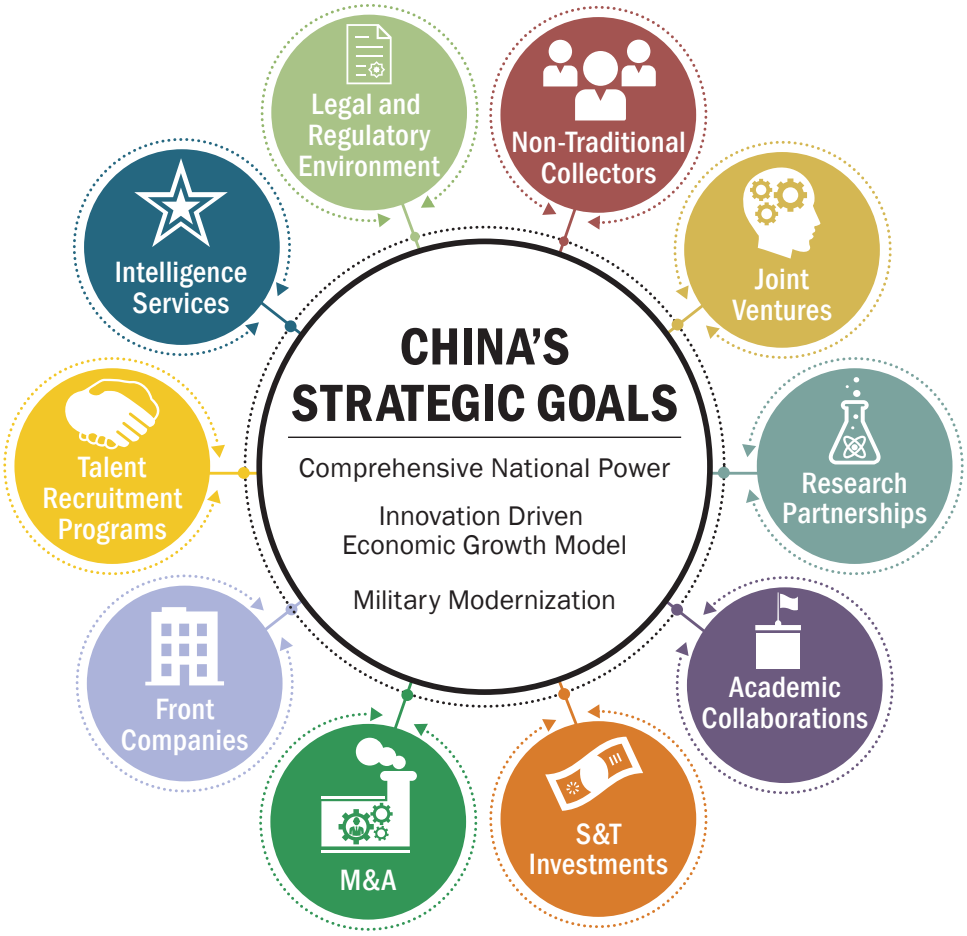
We anticipate that China, Russia, and Iran will remain aggressive and capable collectors of sensitive U.S. economic information and technologies, particularly in cyberspace. All will almost certainly continue to deploy significant resources and a wide array of tactics to acquire intellectual property and proprietary information.

Countries with closer ties to the United States have conducted cyber espionage and other forms of intelligence collection to obtain U.S. technology, intellectual property, trade secrets, and proprietary information. U.S. allies or partners often take advantage of the access they enjoy to collect sensitive military and civilian technologies and to acquire know-how in priority sectors.

## China: Persistent Cyber Activities

China has expansive efforts in place to acquire U.S. technology to include sensitive trade secrets and proprietary information. It continues to use cyber espionage to support its strategic development goals—science and technology advancement, military modernization, and economic policy objectives. China's cyberspace operations are part of a complex, multipronged technology development strategy that uses licit and illicit methods to achieve its goals. Chinese companies and individuals often acquire U.S. technology for commercial and scientific purposes. At the same time, the Chinese government seeks to enhance its collection of U.S. technology by enlisting the support of a broad range of actors spread throughout its government and industrial base.

## China's Strategic Goals




| | |
|---|---|
| Non-Traditional Collectors | China uses individuals for whom science or business is their primary profession to target and acquire US technology. |
| Joint Ventures (JV) | China uses JVs to acquire technology and technical know-how. |
| Research partnerships | China actively seeks partnerships with government laboratories-such as the Department of Energy labs-to learn about and acquire specific technology, and the soft skills necessary to run such facilities. |
| Academic Collaborations | China uses collaborations and relationships with universities to acquire specific research and gain access to high-end research equipment. Its policies state it should exploit the openness of academia to fill China's strategic gaps. |
| S&T Investments | China has sustained, long-term state investments in its S&T infrastructure. |
| M&A | China seeks to buy companies that have technology, facilities and people. These sometimes end up as Committee on Foreign Investment in the United States (CFIUS) cases. |
| Front Companies | China uses front companies to obscure the hand of the Chinese government and acquire export controlled technology. |
| Talent Recruitment Programs | China uses its talent recruitment programs to find foreign experts to return to China and work on key strategic programs. |
| Intelligence Services | The Ministry of State Security (MSS), and military intelligence offices are used in China's technology acquisition efforts. |
| Legal and Regulatory Environment | China uses its laws and regulations to disadvantage foreign companies and advantage its own companies. |

The Intelligence Community and private sector security experts continue to identify ongoing Chinese cyber activity, although at lower volumes than existed before the bilateral September 2015 U.S.-China cyber commitments. Most Chinese cyber operations against U.S. private industry that have been detected are focused on cleared defense contractors or IT and communications firms whose products and services support government and private sector networks worldwide. Examples of identified ongoing Chinese cyber activity include the following:

- According to several cyber intelligence companies, in 2017 the China-associated cyber espionage group APT10 continued widespread operations to target engineering, telecommunications, and aerospace industries. APT10 targeted companies across the globe, including the United States, using its exploitation of managed IT service providers as a means to conduct such operations.

- Cybersecurity researchers have found links between Chinese cyber actors and a back door in the popular CCleaner application that allowed the actors to target U.S. companies, including Google, Microsoft, Intel, and VMware.

- In November 2017, PricewaterhouseCoopers (PWC) reported that the China-based APT, known as KeyBoy, was shifting its focus to target Western organizations. According to PWC, the targeting likely was for corporate espionage purposes. KeyBoy previously focused on Asian targets, according to commercial cybersecurity reporting.

- According to FireEye, in 2017 TEMP.Periscope continued targeting the maritime industry as well as engineering-focused entities including research institutes, academic organizations, and private firms in the United States. FireEye has detected sharp increases in targeting in early 2018 as well.

### Recent Unsealed U.S. Indictment With a Link to China

In November 2017, Wu Yingzhuo, Dong Hao and Xia Lei, Chinese nationals and residents of China, were charged with computer hacking, theft of trade secrets, conspiracy, and identity theft. These efforts were directed at U.S. and foreign employees and the computers of three corporations that were victims in the financial, engineering, and technology industries between 2011 and May 2017.

We believe that China will continue to be a threat to U.S. proprietary technology and intellectual property through cyber-enabled means or other methods. If this threat is not addressed, it could erode America's long-term competitive economic advantage.

## Russia: A Sophisticated Adversary

The threat to U.S. technology from Russia will continue over the coming years as Moscow attempts to bolster an economy struggling with endemic corruption, state control, and a loss of talent departing for jobs abroad. Moscow's military modernization efforts also likely will be a motivating factor for Russia to steal U.S. intellectual property. An aggressive and capable collector of sensitive U.S. technologies, Russia uses cyberspace as one of many methods for obtaining the necessary know-how and technology to grow and modernize its economy. Other methods include the following:

- Use of Russian commercial and academic enterprises that interact with the West;
- Recruitment of Russian immigrants with advanced technical skills by the Russian intelligence services; and
- Russian intelligence penetration of public and private enterprises, which enable the government to obtain sensitive technical information from industry.

Russia uses cyber operations as an instrument of intelligence collection to inform its decision-making and benefit its economic interests. Experts contend that Russia needs to enact structural reforms, including economic diversification into sectors such as technology, to achieve the higher rate of gross domestic product growth publicly called for by Russian President Putin. In support of that goal, Russian intelligence services have conducted sophisticated and large-scale hacking operations to collect sensitive U.S. business and technology information. In addition, Moscow uses a range of other intelligence collection operations to steal valuable economic data:

- In 2016, the hacker "Eas7" confided to Western press that she had collaborated with the Russian Federal Security Service (FSB) on economic espionage missions. She estimated that "among the good hackers, at least half works (sic) for government structures," suggesting Moscow employs cyber criminals as a way to make such operations plausibly deniable.
- Moscow has used cyber operations to collect intellectual property data from U.S. energy, healthcare, and technology companies. For example, Russian Government hackers last year compromised dozens of U.S. energy firms, including their operational networks. This activity could be driven by multiple objectives, including collecting intelligence, developing accesses for disruptive purposes, and providing sensitive U.S. intellectual property to Russian companies.
- Since at least 2007, the Russian state-sponsored cyber program APT28 has routinely collected intelligence on defense and geopolitical issues, including those relating to the United States and Western Europe. Obtaining sensitive U.S. defense industry data could provide Moscow with economic (e.g. in foreign military sales) and security advantages as Russia continues to strengthen and modernize its military forces.

### Recent Unsealed U.S. Indictment with a Link to Russia

In March 2017, the United States Department of Justice indicted two FSB officials and their Russian cybercriminal conspirators on computer hacking and conspiracy charges related to the collection of emails of U.S. and European employees of transportation and financial services firms. The charges included conspiring to engage in economic espionage and theft of trade secrets.

We believe that Russia will continue to conduct aggressive cyber operations during the next year against the United States and its allies as part of a global intelligence collection program focused on furthering its security interests. Although cyber operations are just one element of Russia's multipronged approach to information collection, they give Russia's intelligence services a more agile and cost-efficient tool to accomplish Moscow's objectives. Indeed, Russian cyber actors are continuing to develop their cyber tradecraft—such as using open-source hacking tools that minimize forensic connections to Russia.

## Iran: An Increasing Cyber Threat

Iranian cyber activities are often focused on Middle Eastern adversaries, such as Saudi Arabia and Israel; however, in 2017 Iran also targeted U.S. networks. A subset of this Iranian cyber activity aggressively targeted U.S. technologies with high value to the Iranian government. The loss of sensitive information and technologies not only presents a significant threat to U.S. national security. It also enables Tehran to develop advanced technologies to boost domestic economic growth, modernize its military forces, and increase its foreign sales. Examples of recent Iranian cyber activities include the following:

- The Iranian hacker group Rocket Kitten consistently targets U.S. defense firms, likely enabling Tehran to improve its already robust missile and space programs with proprietary and sensitive U.S. military technology.
- Iranian hackers target U.S. aerospace and civil aviation firms by using various website exploitation, spearphishing, credential harvesting, and social engineering techniques.
- The OilRig hacker group, which historically focuses on Saudi Arabia, has increased its targeting of U.S. financial institutions and information technology companies.
- The Iranian hacker group APT33 has targeted energy sector companies as part of Iran's national priorities for improving its petrochemical production and technology.
- Iranian hackers have targeted U.S. academic institutions, stealing valuable intellectual property and data.

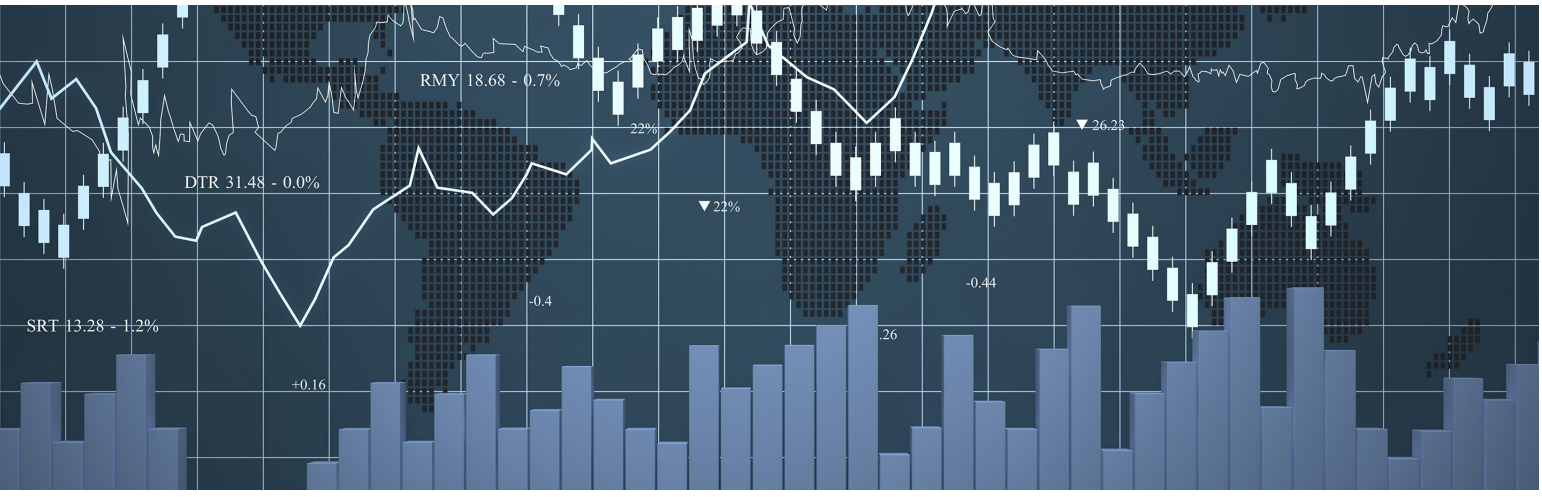
## Recent Unsealed U.S. Indictments with a Link to Iran

In July 2017, Iranian nationals Mohammed Reza Rezakhah and Mohammed Saeed Ajily were charged with hacking into U.S. software companies, stealing their proprietary software, and selling the stolen software to Iranian universities, military and government entities, and other buyers outside of the United States.

In November 2017, Iranian national Behzad Mesri was charged with allegedly hacking HBO's corporate systems, stealing intellectual property and proprietary data, to include scripts and plot summaries for unaired episodes. Mesri had previously hacked computer systems for the Iranian military and has been a member of an Iran-based hacking group called the Turk Black Hat security team.

In March 2018, nine Iranian hackers associated with the Mabna Institute were charged with stealing intellectual property from more than 144 U.S. universities which spent approximately $3.4 billion to procure and access the data. The data was stolen at the behest of Iran's Islamic Revolutionary Guard Corps and used to benefit the government of Iran and other Iranian customers, including Iranian universities. Mabna Institute actors also targeted and compromised 36 U.S. businesses.

We believe that Iran will continue working to penetrate U.S. networks for economic or industrial espionage purposes. Iran's economy—still driven heavily by petroleum revenue—will depend on growth in nonoil industries and we expect Iran will continue to exploit cyberspace to gain advantages in these industries. Iran will remain committed to using its cyber capabilities to attain key economic goals, primarily by continuing to steal intellectual property, in an effort to narrow the science and technology gap between Iran and Western countries.



## Targeted Technologies

Although many aspects of U.S. economic activity and technology are of potential interest to foreign intelligence collectors, we judge that the highest interest is in the following areas:

| Industry | Priority Sectors / Technologies | |
|---|---|---|
| Energy / Alternative Energy | • Advanced pressurized water reactor and high-temperature, gas-cooled nuclear power stations<br>• Biofuels<br>• Energy-efficient industries | • Oil, gas, and coalbed methane development, including fracking<br>• Smart grids<br>• Solar energy technology<br>• Wind turbines |
| Biotechnology | • Advanced medical devices<br>• Biomanufacturing and chemical manufacturing<br>• Biomaterials | • Biopharmaceuticals<br>• Genetically modified organisms<br>• Infectious disease treatment<br>• New vaccines and drugs |
| Defense Technology | • Aerospace & Aeronautic Systems<br>• Armaments | • Marine Systems<br>• Radar<br>• Optics |
| Environmental Protection | • Batteries<br>• Energy-efficient appliances<br>• Green building materials | • Hybrid and electric cars<br>• Waste management<br>• Water/air pollution control |
| High-End Manufacturing | • 3D printing<br>• Advanced robotics<br>• Aircraft engines<br>• Aviation maintenance and service sectors<br>• Civilian aircraft<br>• Electric motors<br>• Foundational manufacturing equipment | • High-end computer numerically controlled machines<br>• High-performance composite materials<br>• High-performance sealing materials<br>• Integrated circuit manufacturing equipment and assembly technology<br>• Space infrastructure and exploration technology<br>• Synthetic rubber |
| Information and Communications Technology | • Artificial intelligence<br>• Big data analysis<br>• Core electronics industries<br>• E-commerce services<br>• Foundational software products<br>• High-end computer chips<br>• Internet of Things | • Network equipment<br>• Next-generation broadband wireless communications networks<br>• Quantum computing and communications<br>• Rare-earth materials |

# III. Emerging Threats

A range of other potentially disruptive threats warrant attention. Software supply chain infiltration has already threatened the critical infrastructure sector and could threaten other sectors as well. Meanwhile, new foreign laws and increased risks posed by foreign technology companies due to their ties to host governments, may present U.S. companies with previously unforeseen threats.

Cyber threats will continue to evolve with technological advances in the global information environment. The following are emerging areas of concern that are likely to disrupt security procedures and expand the opportunities for collection of sensitive U.S. economic and technology information.

## Software Supply Chain Operations

Last year represented a watershed in the reporting of software supply chain operations. In 2017, seven significant events were reported in the public domain compared to only four between 2014 and 2016. As the number of events grows, so too are the potential impacts. Hackers are clearly targeting software supply chains to achieve a range of potential effects to include cyber espionage, organizational disruption, or demonstrable financial impact:

- Floxif infected 2.2 million worldwide CCleaner customers with a backdoor. The hackers specifically targeted 18 companies and infected 40 computers to conduct espionage to gain access to Samsung, Sony, Asus, Intel, VMWare, O2, Singtel, Gauselmann, Dyn, Chunghwa and Fujitsu.

- Hackers corrupted software distributed by the South Korea-based firm Netsarang, which sells enterprise and network management tools. The backdoor enabled downloading of further malware or theft of information from hundreds of companies in energy, financial services, manufacturing, pharmaceuticals, telecommunications, and transportation industries.

- A tweaked version of M.E. Doc was infected with a backdoor to permit the delivery of software from the Ukrainian accounting firm a destructive payload disguised as ransomware. This attack, which was attributed to Russia, paralyzed networks worldwide, shutting down or affecting operations of banks, companies, transportation, and utilities. The cost of this attack to FedEx and Maersk was approximately $300 million each.

- A malware operation dubbed Kingslayer, targeted system administrator accounts associated with U.S. firms to steal credentials in order to breach the system and replace the legitimate application and updates with a malware version containing an embedded backdoor. Although it is not known which and how many firms were ultimately infected, at least one U.S. defense contractor was targeted and compromised.

## Foreign Laws Could Enable Intellectual Property Theft

New and enhanced cyber, national security, and import laws in effect in foreign countries are posing an increasing risk to U.S. technology and propriety information. For example, in 2017, China and Russia aggressively enforced laws that bolstered their domestic companies at the expense of U.S. companies and also might allow their companies access to U.S. intellectual property and proprietary information.

In 2017, China put into effect a new cyber security law that restricts sales of foreign information and communication technology (ICT) and mandates that foreign companies submit ICT for government-administered national security reviews. The law also requires that firms operating in China store their data in China, and it requires government approval prior to transferring data outside China. The U.S. Chamber of Commerce has gone on record to explain that if a foreign company is forced to localize a valuable set of data or information in China, whether for research and development purposes or simply to conduct its business, it will have to assume a significant amount of risk. Its data or information may be misappropriated or misused, especially given the environment in China, where companies face significant legal and other uncertainties when they try to protect their data and information.

### Required Steps for U.S. Companies to Do Business in China

1. Pass National Security Reviews for Technology and Services
2. Store All Data in China
3. Form Joint Venture to Open Data Center
4. Obtain Government Approval for Data Transfers
5. Buy Government-Approved Encryption and Virtual Private Networks (VPNs)

▶ China has Access to U.S. Intellectual Property and Proprietary Information

Similarly, in recent years Russia has dramatically increased its demand for source code reviews for foreign technology being sold inside the country. Russia's Federal Security Service (FSB), associated with economic espionage missions in the past, serves as the authority charged with directing these source code reviews and approving the sale of technology products and services sold inside Russia.

High intelligence threat countries, such as China and Russia, could exploit these laws to significantly improve their access to the intellectual property of foreign companies operating in their countries and subsequently share this sensitive information with domestic firms.

## Foreign Technology Companies with Links to Host Governments

Foreign information and communications technology companies are often subject to foreign state influence. This presents a risk to U.S. trade secrets and intellectual property. These companies provide valuable services that often require access to the physical and logical control points of the computers and networks they support. These unique accesses also present an opportunity for foreign countries to obtain sensitive proprietary information. Recent events underscore the potential risks posed by technology companies that have links to foreign governments with high threat intelligence services:

- Recent Chinese laws—including laws on national security and cybersecurity—provide Beijing a legal basis to compel technology companies operating in China to cooperate with Chinese security services.

- In September 2017, the Department of Homeland Security issued a directive to Federal departments and agencies to remove Kaspersky Lab products and services based on the information security risks posed by the company and its links to Russia.

- In December 2017, the Department of Justice made public an agreement with Netcracker Technology Corp. that resulted in the company agreeing that it would not store sensitive information and data from its U.S.-based technology clients in overseas locations, including most notably Russia.

# Annex – Decreasing the Prevalence of Economic or Industrial Espionage in Cyberspace

The U.S. Government (USG) continues to undertake numerous actions to counter economic espionage in cyberspace. Perhaps most evident are current USG efforts to protect critical infrastructure and other sensitive computer networks from malicious cyber activities. The USG also continues to work with the private sector to address science and technology gaps through cyber research and development as a way of mitigating the malicious activities of threat actors in cyberspace. The USG will continue to improve its efforts to disrupt, deny, exploit, or increase the costs of foreign cyber operations that are targeting the nation's most critical economic assets.

Examples of USG actions include the following:

- Sharing information about cyber threats, vulnerabilities, and other risks;
- Promoting best practices, risk assessments, and capability development;
- Improving our responses to cyber incidents;
- Building and driving the market towards a more secure cyber ecosystem; and
- Partnering with allies to address cyber issues.

The USG has the capability to impose costs on adversaries who engage in economic cyber espionage through various actions, including diplomatic, informational, military, law enforcement, and economic response. The details of many of these actions are too sensitive to discuss in this publication; however, we have provided a few general examples that illustrate the USG's response, such as:

- Public statements and attribution;
- Diplomatic demarches;
- Economic sanctions; and
- Law enforcement actions.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE