For Immediate Release:
26 July 2018

Contact: (301) 243-0408

NCSC Releases *2018 Foreign Economic Espionage in Cyberspace* Report

The National Counterintelligence and Security Center (NCSC) today released its 2018 *Foreign Economic Espionage in Cyberspace* report, which highlights current threats and future trends in foreign intelligence efforts to steal U.S. intellectual property, trade secrets, and proprietary information via cyberspace.

"Our goal in releasing this document is simple: to provide U.S. industry and the public with the latest unclassified information on foreign efforts to steal U.S. trade secrets through cyberspace," said William R. Evanina, Director of the NCSC. "Building an effective response to this tremendous challenge demands understanding economic espionage as a worldwide, multi-vector threat to the integrity of both the U.S. economy and global trade."

The report underscores the strategic threat of cyber economic espionage, noting that next generation technologies such as Artificial Intelligence and the Internet-of-Things offer great opportunities, but also introduce new vulnerabilities to U.S. networks for which the cybersecurity community largely remains unprepared.

The report also provides insights into the most pervasive nation-state threat actors – including China, Russia and Iran – and recent examples of their economic espionage activities in the United States through cyberspace. Despite advances in cybersecurity, the report notes that cyberespionage offers such actors a relatively low-cost, high-yield avenue to obtain a wide spectrum of U.S. intellectual property.

The report also identifies those U.S. industrial sectors and technologies that are of greatest interest to foreign threat actors, including energy, biotechnology, defense, environmental protection, high-end manufacturing, and information and communications technology.

In addition, the report highlights several emerging threats that warrant attention, including:

- **Software supply chain infiltration, which has already threatened the U.S. critical infrastructure and is poised to threaten other sectors**. According to the report, 2017 represented a watershed year for public reporting of such incidents. There were numerous events involving hackers targeting software supply chains with backdoors for cyber espionage, organizational disruption or demonstrable financial impact.

- **Laws in foreign countries, such as those in China and Russia, that can pose an increased intellectual property risk to U.S. companies doing business there**. The report notes that China's 2017 cybersecurity law mandates that foreign companies submit their technology to the Chinese government for national security reviews; and that Russia has dramatically increased its demand of source code reviews – which are overseen by Russian intelligence – to approve of foreign technology sold in their country.

- **Foreign technology firms that are subject to foreign state influence or have links to foreign governments with high-threat intelligence services**. Citing the examples of Kaspersky Lab and Netcracker Technology Corp., the report notes that such companies often provide services that require access to control points of computer networks they support, presenting opportunities for foreign nations to acquire sensitive information.

The full report is available at www.ncsc.gov. The report was compiled by the NCSC with the support, coordination, and contributions of several agencies across the Intelligence Community.

A center within the Office of the Director of National Intelligence, the NCSC is the nation's premier source for counterintelligence and security expertise and a trusted mission partner in protecting America against foreign and other adversarial threats.

# # #