National Counterintelligence Strategy

of the United States of America 2020-2022

Executive Summary

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

Office of the Director of National Intelligence
Director of the National Counterintelligence and Security Center
Washington, DC 20511

The United States is facing increasingly aggressive and complex threats from foreign intelligence services, as well as state and non-state actors. To anticipate and deter these threats, the U.S. Government continues to address its fundamental, core counterintelligence missions: identifying, assessing, and neutralizing foreign intelligence activities and capabilities in the United States; mitigating insider threats, countering espionage and assassination attempts by foreign intelligence services from occurring on U.S. soil and abroad; and protecting U.S. sensitive and classified information and sensitive facilities from technical penetrations or espionage.

This *National Counterintelligence Strategy of the United States of America, 2020-2022* presents a new perspective on how to effectively address foreign intelligence threats as a nation. Five strategic objectives encompass the most critical areas where foreign intelligence services are targeting the United States: Critical Infrastructure; Key U.S. Supply Chains; the U.S. Economy; American Democracy; and Cyber and Technical Operations.

This *Strategy* identifies areas where foreign threat actors could cause serious damage to our national and economic security and where we need to invest attention and resources. It also describes activities currently being undertaken, or planned, to counter threats from foreign adversaries.

It is essential that we engage and mobilize all elements of United States society and fully integrate sound counterintelligence and security procedures into our business practices, and strengthen our networks against attempts by foreign threat actors or malicious insiders to steal or compromise our sensitive data, information, and assets.

My office is committed to working with federal, state and local governments, the private sector, universities, as well as with our foreign partners to counter the threats posed by foreign adversaries. Together we will build on past successes to safeguard our nation's most sensitive information and assets.

William R. Evanina
Director, National Counterintelligence and Security Center

NATIONAL COUNTERINTELLIGENCE STRATEGY OF THE UNITED STATES

Strategic Objectives

Protect the Nation's Critical Infrastructure

Protect the nation's civil and commercial, defense mission assurance and continuity of government infrastructure from foreign intelligence entities seeking to exploit or disrupt national critical functions.

Reduce Threats to Key U.S. Supply Chains

Reduce threats to key U.S. supply chains to prevent foreign attempts to compromise the integrity, trustworthiness, and authenticity of products and services purchased and integrated into the operations of the U.S. government, the Defense Industrial Base, and the private sector.

Counter the Exploitation of the U.S. Economy

Counter the exploitation of the U.S. economy to protect America's competitive advantage in world markets and our technological leadership, and to ensure our economic prosperity and security.

Defend American Democracy against Foreign Influence

Defend the United States against foreign influence to protect America's democratic institutions and processes, and preserve our culture of openness.

Counter Foreign Intelligence Cyber and Technical Operations

Counter foreign intelligence cyber and technical operations that are harmful to U.S. interests.

CORE COUNTERINTELLIGENCE MISSIONS

The U.S. Government will continue to address core and continuing counterintelligence missions: identifying, assessing, and neutralizing foreign intelligence activities and capabilities in the United States and abroad and protecting U.S. national secrets and sensitive facilities from technical penetrations or espionage, countering espionage and mitigating insider threats.

Foreign intelligence actors are employing innovative combinations of traditional spying, economic espionage, supply chain and cyber operations to gain access to critical infrastructure, and steal sensitive information, research, technology, and industrial secrets. Three principal trends characterize the current and emerging counterintelligence[1] environment:

1. **The number of actors targeting the United States is growing.** Russia and China operate globally, use all instruments of national power to target the United States, and have a broad range of sophisticated intelligence capabilities. Other state adversaries such as Cuba, Iran, and North Korea; non-state actors such as Lebanese Hizballah, ISIS, and al-Qa'ida; as well as, transnational criminal organizations and ideologically motivated entities such as hacktivists, leaktivists, and public disclosure organizations, also pose significant threats. Additionally, foreign nationals with no formal ties to foreign intelligence services steal sensitive data and intellectual property.

2. **Threat actors have an increasingly sophisticated set of intelligence capabilities** at their disposal and are employing them in new ways to target the United States. The global availability of technologies with intelligence applications—such as biometric devices, unmanned systems, high resolution imagery, enhanced technical surveillance equipment, advanced encryption, and big data analytics—and the unauthorized disclosures of U.S. cyber tools have enabled a wider range of actors to obtain intelligence capabilities previously possessed only by well-financed intelligence services.

3. **Threat actors are using these capabilities against an expanded set of targets and vulnerabilities.** Foreign intelligence entities are targeting most U.S. government departments and agencies—even those without a national security mission—as well as national laboratories, the financial sector, the U.S. industrial base and other private sector and academic entities. Some adversaries are conducting intelligence operations to exploit, disrupt, and damage U.S. and allied critical infrastructure and military capabilities during a crisis.

To meet the increasing challenges posed by foreign intelligence actors, the United States will need to employ whole-of-government counterintelligence and security approaches that effectively integrate offensive and defensive measures and leverage all instruments of American power.

[1] Counterintelligence: Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities. – Executive Order 12333, as amended, United States Intelligence Activities.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE