OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
FROM THE OFFICE OF STRATEGIC COMMUNICATIONS

Tulsi Gabbard, Director of National Intelligence
Congressional Testimony
Annual Threat Assessment of the U.S. Intelligence Community
March 25, 2025

Chairman Cotton, Vice Chair Warner, Members of the Committee, thank you for the opportunity to present to you the Intelligence Community's 2025 Annual Threat Assessment, joined by my colleagues from CIA, DIA, FBI, and NSA.

Our testimony offers the collective assessment of the 18 U.S. intelligence elements making up the U.S. Intelligence Community and draws on intelligence collection, information available to the IC from open-source and the private sector, and the expertise of our analysts.

This report evaluates what the IC assesses most threatens our people and our nation's ability to live in a peaceful, free, secure and prosperous society. We face an increasingly complex threat environment that is affecting us here at home, and our interests abroad.

I'll begin by focusing on what most immediately and directly threatens the United States and the wellbeing of the American people -- non-state criminal groups and terrorists putting American lives and livelihood at risk, followed by key nation states who have the capability to threaten the interests of the United States. In this complex environment, non-state and state actors are able to exploit or take advantage of the effects of each other's activities. Conventional and asymmetric capabilities even the traditionally weakest of actors are able to acquire from available advanced technologies creates an even more complex and serious threat landscape.

First, I will highlight threats presented by several non-state actors. Cartels, gangs, and other transnational criminal organizations in our part of the world are engaging in a wide array of illicit activity, from narcotics trafficking, to money laundering, to smuggling of illegal immigrants and human trafficking, which endanger the health, welfare, and safety

of everyday Americans. Based on the latest reporting available, for a year-long period ending October 2024, cartels were largely responsible for the deaths of more than 54,000 U.S. citizens from synthetic opioids. Mexico-based transnational criminal organizations (TCOs) are the main suppliers of illicit fentanyl to the U.S. market and are adapting to enforcement and regulatory pressures by using multiple sources and methods to procure precursor chemicals and equipment primarily from China and India, many of which are dual-use chemicals used in legitimate industries. Independent fentanyl producers are increasingly fragmenting the drug trade in Mexico. The availability of precursor chemicals and ease of making illicit fentanyl have enabled independent actors to increase illicit fentanyl production and smuggling operations in Mexico.

Cartels profit from human-trafficking, and likely facilitated more than 2 million illegal immigrants encountered by law enforcement at the U.S. southwest border in 2024, straining vital resources and putting the American people at risk. Criminal groups drive much of the unrest and lawlessness in the Western Hemisphere. They also engage in extortion, weapons and human smuggling, and other illicit and dangerous revenue-seeking operations, including kidnappings for ransom, forced labor, and sex trafficking. These and other human traffickers exploit vulnerable individuals and groups by promising well-paying jobs and confiscating identification documents. They operate in the shadows, exploiting lawlessness in various areas, and by using coercion and intimidation to control their victims.

While key drivers of migrants are expected to persist, heightened U.S. border security enforcement and deportations under the Trump administration are proving to serve as a deterrent for migrants seeking to illegally cross U.S. borders. U.S. Border Patrol apprehensions along the southwest border in January 2025 dropped 85% from the same period in 2024.

Transnational Islamist extremists, such as ISIS and al-Qa'ida, and affiliated jihadi groups, continue to pursue, enable, or inspire attacks against the United States and our citizens, abroad and within the Homeland, to advance their ultimate objective of establishing a global Islamist caliphate. This includes heightened efforts to spread their ideology to recruit and radicalize individuals in the U.S. and the West. While the New

Year's Day attacker in New Orleans had no known direct contact with ISIS terrorists, he was influenced and radicalized by ISIS ideological propaganda, for example. Al-Qa'ida and its' affiliates continues to call for attacks against the United States, as they conduct attacks overseas. These jihadist groups have shown an ability to adapt and evolve, including using new technologies and tactics to spread their ideology and recruit new followers.

A range of non-state cyber criminals are also targeting our economic interests, critical infrastructure, and advanced commercial capability for extortion, other coercive pursuits, and financial gain. These actors use a variety of tactics, including phishing, ransomware, and denial-of-service attacks, to disrupt our systems and steal sensitive and lucrative information, using available technologies and U.S. cyber vulnerabilities. Ransomware actors last year, for example, attacked the largest payment processor for U.S. healthcare transactions, and another set of criminal actors conducted cyber attacks against U.S. water utilities.

Some of these non-state cyber actors also operate as proxies for or emulate similar activities carried out by major state actors. While these non-state cyber actors often seek financial and intellectual property gains, they also carry out cyber operations for espionage purposes, targeting our critical infrastructure.

Turning to our key state-actors, the IC sees China, Russia, Iran, and North Korea engaging in activities that could challenge U.S. capabilities and interests, especially related to our security and economy. These actors are, in some cases, working together in different areas to target U.S. interests and protect themselves from U.S. sanctions.

At this point, the IC assesses that China is our most capable strategic competitor. Under the leadership of President Xi Jinping, the People's Republic of China seeks to position itself as a leading power on the world stage, economically, technologically and militarily. Beijing is driven in part by a belief that Washington is pursuing a broad effort to contain China's rise and undermine CCP rule.

China's most serious domestic challenge is probably China's slowing economy and potential instability if socioeconomic grievances lead to large-scale unrest. Growing

economic tensions with the United States and other countries could also weigh on China's plans for economic growth and domestic job creation.

China's military is fielding advanced capabilities, including hypersonic weapons, stealth aircraft, advanced submarines, stronger space and cyber warfare assets, and a larger, arsenal of nuclear weapons. While it would like to develop and maintain positive ties with the United States and the Trump Administration to advance its interests and avoid conflict, China is building its' military capability, in part, to gain advantage in the event of a military conflict with the United States around the issue of China's efforts toward unification with the Republic of China, Taiwan. China's military is also expanding its presence in the Asia-Pacific region, with a focus on disputed territorial claims in both the East China and South China Seas.

Beijing is advancing its cyber capabilities for sophisticated operations aimed at stealing sensitive U.S. government and private sector information, and pre-positioning additional asymmetric attack options that may be deployed in a conflict. China's cyber activities have been linked to multiple high-profile breaches, including last year's massive compromise of the U.S. telecommunications infrastructure, also referred to as Salt Typhoon.

Beijing currently dominates global markets and strategically important supply chains, for example with the mining and processing of several critical minerals. In December, China imposed an export ban to the United States on gallium, germanium, and antimony, all of which are important to the production of semiconductors and defense technologies. This was in direct response to U.S. export controls on chips designed to broadly limit PRC access to advanced chips and chipmaking equipment.

China also aims to compete in other critical global industries, including AI, legacy semiconductor chip production, biomanufacturing and genetic sequencing, and medical and pharmaceutical supply production. Leveraging often heavily state-subsidized production at greater scale, lower costs, and weaker regulatory standards than required in the West, Beijing's strategy has given it a leading position in many parts of these sectors and supply chains supporting them. In 2023, China had five first-in-class domestic drug approvals and three FDA approvals.

Turning to Russia: Russia's nuclear and conventional military capabilities, along with its demonstrated economic and military resilience, make it a formidable competitor. Moscow has more nuclear weapons than any other nation, that could inflict catastrophic damage on the United States and the world in the event of a major war that Russian leaders feared put them and their regime at serious risk. In late 2024, Russia announced updates to its public nuclear doctrine, expanding the conditions under which Russia would consider using nuclear weapons.

Russia is building a more modern and survivable nuclear force designed to circumvent U.S. missile defense through reliable retaliatory strike potential. Russia intends to deter the U.S. by both holding the U.S. homeland at risk and by having the capabilities to threaten nuclear war in a conflict.

Russia has developed advanced cyber capabilities and has attempted to pre-position access on U.S. critical infrastructure for asymmetric options and make it a persistent cyber threat. Russia's cyber activities have been linked to multiple high-profile breaches, including the 2023 hack of Microsoft.

Russia is also fielding new capabilities and antisatellite weapons meant to degrade U.S. and allied space infrastructure. Among Russia's most concerning developments is a new satellite intended to carry a nuclear weapon as an antisatellite weapon, violating longstanding international law against such activity and putting the U.S. and global economy at risk.

Iran continues to seeks expansion of its influence in the Middle East, despite the degradation to its proxies and defenses during the Gaza conflict. Iran has developed and maintains ballistic missiles, cruise missiles, and UAVs, including systems capable of striking U.S. targets and allies in the region. Tehran has shown a willingness to use these weapons, including during a 2020 attack on U.S. forces in Iraq and in attacks against Israel in April and October 2024. Iran's cyber operations and capabilities also present a serious threat to U.S. networks and data.

The IC continues to assess that Iran is not building a nuclear weapon and Supreme Leader Khamanei has not authorized the nuclear weapons program he suspended in

2003. The IC is closely monitoring if Tehran decides to reauthorize its nuclear weapons program. In the past year, we have seen an erosion of a decades-long taboo in Iran on discussing nuclear weapons in public, likely emboldening nuclear weapons advocates within Iran's decision-making apparatus. Iran's enriched uranium stockpile is at its highest levels and is unprecedented for a state without nuclear weapons.

Iran will likely continue efforts to counter Israel and press for a U.S. military withdrawal from the region by aiding, arming, and helping to reconstitute its loose consortium of like-minded terrorist and militant actors, which it refers to as its "Axis of Resistance." Although weakened, this collection of actors still presents a wide range of threats, including to Israel's population, U.S. forces deployed in Iraq and Syria, and to U.S. and international military and commercial shipping and transit.

North Korean Leader Kim Jong Un is pursuing stronger strategic and conventional capabilities that can target U.S. forces and allies in the region, as well as the U.S. Homeland, to bolster North Korea's leverage and stature, defend the regime, and achieve at least tacit recognition as a nuclear weapons power. Kim's recently cemented strategic partnership with Russia supports these goals by providing him greater financial, military, and diplomatic support; reduced reliance on China and the need to defer to Beijing's terms for support; and providing North Korean forces and weapons systems authentic warfighting experience.

Kim views his strategic weapons advances since 2019, deepening ties with Russia, and North Korea's economic durability as strengthening his negotiating position against Washington's demands for denuclearization and lessening his need for sanctions relief.

North Korea is probably prepared to conduct another nuclear test on short notice and continues to flight test ICBMs to demonstrate their increasing capabilities as leverage in future negotiations.

Since 2022, China, Russia, Iran and North Korea have grown closer. Removing the accelerant of the war in Ukraine is unlikely to revert these bilateral relationships to a pre-war, 2021 baseline, leaving room for new strategic priorities and world events to create new incentives or challenges to their currently high levels of cooperation. Russia

has been the catalyst for much of this expanded cooperation, driven heavily by the support it has needed for its war effort against Ukraine, including protection from U.S. and Western sanctions. In addition to its exchange of military and other resource capabilities with North Korea, Russia has relied more heavily on China's financial and defense industry backing, and also has increased combined military exercises with China to signal shared fortitude against the United States and U.S. allies in the Asia-Pacific region. With Iran, Russia has also expanded financial ties to mitigate sanctions. Iran has become a critical military supplier to Russia, especially of UAVs, in exchange for Russian technical support for Iranian weapons, intelligence, and advanced cyber capabilities.

In conclusion, the threats we see to U.S. national security are both complex and multifaceted, and put the lives, safety and wellbeing of the American people at serious risk.

As the heads of the American people's Intelligence Community, we will provide the President, Congress, our warfighters, and the American people the timely, unbiased, relevant intelligence to keep the United States secure, free, prosperous and at peace.

To the American people, specifically, our Intelligence Community exists to serve you, and ensure your safety, security, and freedom.

Thank you.