I. Context and Commentary

Statement for the Record, Worldwide Threat Assessment of the U.S. Intelligence Community

By Daniel R. Coats, Director of National Intelligence

Senate Select Committee on Intelligence Washington D.C.

February 13, 2018

FOREWORD

Competition among countries will increase in the coming year as major powers and regional aggressors exploit complex global trends while adjusting to new priorities in US foreign policy. The risk of interstate conflict, including among great powers, is higher than at any time since the end of the Cold War. The most immediate threats of regional interstate conflict in the next year come from North Korea and from Saudi-Iranian use of proxies in their rivalry. At the same time, the threat of state and nonstate use of weapons of mass destruction will continue to grow.

- Adversaries and malign actors will use all instruments of national power—including information and cyber means—to shape societies and markets, international rules and institutions, and international hot spots to their advantage.

- China and Russia will seek spheres of influence and to check US appeal and influence in their regions. Meanwhile, US allies’ and partners’ uncertainty about the willingness and capability of the United States to maintain its international commitments may drive them to consider reorienting their policies, particularly regarding trade, away from Washington.

- Forces for geopolitical order and stability will continue to fray, as will the rules-based international order. New alignments and informal networks—outside traditional power blocs and national governments—will increasingly strain international cooperation.

Tension within many countries will rise, and the threat from Sunni violent extremist groups will evolve as they recoup after battlefield losses in the Middle East.

- Slow economic growth and technology-induced disruptions in job mar-
kets are fueling populism within advanced industrial countries and the very nationalism that contributes to tension among countries.

- Developing countries in Latin America and Sub-Saharan Africa face economic challenges, and many states struggle with reforms to tamp down corruption. Terrorists and criminal groups will continue to exploit weak state capacity in Africa, the Middle East, and Asia.

- Challenges from urbanization and migration will persist, while the effects of air pollution, inadequate water, and climate change on human health and livelihood will become more noticeable. Domestic policy responses to such issues will become more difficult—especially for democracies—as publics become less trusting of authoritative information sources.

### GLOBAL THREATS

#### CYBER THREATS

The potential for surprise in the cyber realm will increase in the next year and beyond as billions more digital devices are connected—with relatively little built-in security—and both nation states and malign actors become more emboldened and better equipped in the use of increasingly widespread cyber toolkits.

The risk is growing that some adversaries will conduct cyber attacks—such as data deletion or localized and temporary disruptions of critical infrastructure—against the United States in a crisis short of war.

- In 2016 and 2017, state-sponsored cyber attacks against Ukraine and Saudi Arabia targeted multiple sectors across critical infrastructure, government, and commercial networks.

- Ransomware and malware attacks have spread globally, disrupting global shipping and production lines of US companies. The availability of criminal and commercial malware is creating opportunities for new actors to launch cyber operations.

- We assess that concerns about US retaliation and still developing adversary capabilities will mitigate the probability of attacks aimed at causing major disruptions of US critical infrastructure, but we remain concerned by the increasingly damaging effects of cyber operations and the apparent acceptance by adversaries of collateral damage.

#### Adversaries and Malign Actors Poised for Aggression

Russia, China, Iran, and North Korea will pose the greatest cyber threats to the United States during the next year.

These states are using cyber operations as a low-cost tool of statecraft, and we assess that they will work to use cyber operations to achieve strategic objectives
unless they face clear repercussions for their cyber operations. Nonstate actors will continue to use cyber operations for financial crime and to enable propaganda and messaging.

- The use of cyber attacks as a foreign policy tool outside of military conflict has been mostly limited to sporadic lower-level attacks. Russia, Iran, and North Korea, however, are testing more aggressive cyber attacks that pose growing threats to the United States and US partners.

**Russia**

*We expect that Russia will conduct bolder and more disruptive cyber operations during the next year, most likely using new capabilities against Ukraine.* The Russian Government is likely to build on the wide range of operations it is already conducting, including disruption of Ukrainian energy-distribution networks, hack-and-leak influence operations, distributed denial-of-service attacks, and false flag operations. In the next year, Russian intelligence and security services will continue to probe US and allied critical infrastructures, as well as target the United States, NATO, and allies for insights into US policy.

**China**

*China will continue to use cyber espionage and bolster cyber attack capabilities to support national security priorities.* The IC and private-sector security experts continue to identify ongoing cyber activity from China, although at volumes significantly lower than before the bilateral US-China cyber commitments of September 2015. Most detected Chinese cyber operations against US private industry are focused on cleared defense contractors or IT and communications firms whose products and services support government and private sector networks worldwide. China since 2015 has been advancing its cyber attack capabilities by integrating its military cyber attack and espionage resources in the Strategic Support Force, which it established in 2015.

**Iran**

*We assess that Iran will continue working to penetrate US and Allied networks for espionage and to position itself for potential future cyber attacks, although its intelligence services primarily focus on Middle Eastern adversaries—especially Saudi Arabia and Israel.* Tehran probably views cyberattacks as a versatile tool to respond to perceived provocations, despite Iran’s recent restraint from conduct-
ing cyber attacks on the United States or Western allies. Iran’s cyber attacks against Saudi Arabia in late 2016 and early 2017 involved data deletion on dozens of networks across government and the private sector.

**North Korea**

We expect the heavily sanctioned North Korea to use cyber operations to raise funds and to gather intelligence or launch attacks on South Korea and the United States. Pyongyang probably has a number of techniques and tools it can use to achieve a range of offensive effects with little or no warning, including distributed denial of service attacks, data deletion, and deployment of ransomware.

- North Korean actors developed and launched the WannaCry ransomware in May 2017, judging from technical links to previously identified North Korean cyber tools, tradecraft, and operational infrastructure. We also assess that these actors conducted the cyber theft of $81 million from the Bank of Bangladesh in 2016.

**Terrorists and Criminals.** Terrorist groups will continue to use the Internet to organize, recruit, spread propaganda, raise funds, collect intelligence, inspire action by followers, and coordinate operations. Given their current capabilities, cyber operations by terrorist groups mostly likely would result in personally identifiable information (PII) disclosures, website defacements, and denial-of-service attacks against poorly protected networks. Transnational criminals will continue to conduct for-profit cyber-enabled crimes, such as theft and extortion against US networks. We expect the line between criminal and nation-state activity to become increasingly blurred as states view cyber criminal tools as a relatively inexpensive and deniable means to enable their operations.

**WEAPONS OF MASS DESTRUCTION AND PROLIFERATION**

State efforts to modernize, develop, or acquire weapons of mass destruction (WMD), their delivery systems, or their underlying technologies constitute a major threat to the security of the United States, its deployed troops, and its allies. Both state and nonstate actors have already demonstrated the use of chemical weapons in Iraq and Syria. Biological and chemical materials and technologies—almost always dual-use—move easily in the globalized economy, as do personnel with the scientific expertise to design and use them for legitimate and illegitimate purposes. Information about the latest discoveries in the life sciences also diffuses rapidly around the globe, widening the accessibility of knowledge and tools for beneficial purposes and for potentially nefarious applications.

**Russia**

Russia has developed a ground-launched cruise missile (GLCM) that the United States has declared is in violation of the Intermediate-Range Nuclear Forces (INF) Treaty. Despite Russia’s ongoing development of other Treaty-compliant missiles with intermediate ranges, Moscow probably believes that the new GLCM provides sufficient military advantages to make it worth risking the political reper-
cussions of violating the INF Treaty. In 2013, a senior Russian administration official stated publicly that the world had changed since the INF Treaty was signed in 1987. Other Russian officials have made statements complaining that the Treaty prohibits Russia, but not some of its neighbors, from developing and possessing ground-launched missiles with ranges between 500 and 5,500 kilometers.

China
The Chinese People’s Liberation Army (PLA) continues to modernize its nuclear missile force by adding more survivable road-mobile systems and enhancing its silo-based systems. This new generation of missiles is intended to ensure the viability of China’s strategic deterrent by providing a second-strike capability. China also has tested a hypersonic glide vehicle. In addition, the PLA Navy continues to develop the JL-2 submarine-launched ballistic missile (SLBM) and might produce additional JIN-class nuclear-powered ballistic missile submarines. The JIN-class submarines—armed with JL-2 SLBMs—give the PLA Navy its first long-range, sea-based nuclear capability. The Chinese have also publicized their intent to form a triad by developing a nuclear-capable next-generation bomber.

Iran and the Joint Comprehensive Plan of Action
Tehran’s public statements suggest that it wants to preserve the Joint Comprehensive Plan of Action because it views the JCPOA as a means to remove sanctions while preserving some nuclear capabilities. Iran recognizes that the US Administration has concerns about the deal but expects the other participants—China, the EU, France, Germany, Russia, and the United Kingdom—to honor their commitments. Iran’s implementation of the JCPOA has extended the amount of time Iran would need to produce enough fissile material for a nuclear weapon from a few months to about one year, provided Iran continues to adhere to the deal’s major provisions. The JCPOA has also enhanced the transparency of Iran’s nuclear activities, mainly by fostering improved access to Iranian nuclear facilities for the IAEA and its investigative authorities under the Additional Protocol to its Comprehensive Safeguards Agreement.

Iran’s ballistic missile programs give it the potential to hold targets at risk across the region, and Tehran already has the largest inventory of ballistic missiles in the Middle East. Tehran’s desire to deter the United States might drive it to field an ICBM. Progress on Iran’s space program, such as the launch of the Simorgh SLV in July 2017, could shorten a pathway to an ICBM because space launch vehicles use similar technologies.

North Korea
North Korea will be among the most volatile and confrontational WMD threats to the United States over the next year. North Korea’s history of exporting ballistic missile technology to several countries, including Iran and Syria, and its assistance during Syria’s construction of a nuclear reactor—destroyed in 2007—illustrate its willingness to proliferate dangerous technologies.

In 2017 North Korea, for the second straight year, conducted a large number of
ballistic missile tests, including its first ICBM tests. Pyongyang is committed to developing a long-range, nuclear-armed missile that is capable of posing a direct threat to the United States. It also conducted its sixth and highest yield nuclear test to date.

We assess that North Korea has a longstanding BW capability and biotechnology infrastructure that could support a BW program. We also assess that North Korea has a CW program and probably could employ these agents by modifying conventional munitions or with unconventional, targeted methods.

**Pakistan**

Pakistan continues to produce nuclear weapons and develop new types of nuclear weapons, including short-range tactical weapons, sea-based cruise missiles, air-launched cruise missiles, and longer-range ballistic missiles. These new types of nuclear weapons will introduce new risks for escalation dynamics and security in the region.

**Syria**

We assess that the Syrian regime used the nerve agent sarin in an attack against the opposition in Khan Shaykhun on 4 April 2017, in what is probably the largest chemical weapons attack since August 2013. We continue to assess that Syria has not declared all the elements of its chemical weapons program to the Chemical Weapons Convention (CWC) and that it has the capability to conduct further attacks. Despite the creation of a specialized team and years of work by the Organization for the Prohibition of Chemical Weapons (OPCW) to address gaps and inconsistencies in Syria’s declaration, numerous issues remain unresolved. The OPCW-UN Joint Investigative Mechanism (JIM) has attributed the 4 April 2017 sarin attack and three chlorine attacks in 2014 and 2015 to the Syrian regime. Even after the attack on Khan Shaykhun, we have continued to observe allegations that the regime has used chemicals against the opposition.

**ISIS**

We assess that ISIS is also using chemicals as a means of warfare. The OPCW-UN JIM concluded that ISIS used sulfur mustard in two attacks in 2015 and 2016, and we assess that it has used chemical weapons in numerous other attacks in Iraq and Syria.

**TERRORISM**

Sunni violent extremists—most notably ISIS and al-Qa’ida—pose continuing terrorist threats to US interests and partners worldwide, while US-based homegrown violent extremists (HVEs) will remain the most prevalent Sunni violent extremist threat in the United States. Iran and its strategic partner Lebanese Hizballah also pose a persistent threat to the United States and its partners worldwide.

**Sunni Violent Extremism**

*Sunni violent extremists are still intent on attacking the US homeland and US interests overseas, but their attacks will be most frequent in or near conflict zones or against enemies that are more easily accessible.*
• Sunni violent extremist groups are geographically diverse; they are likely to exploit conflict zones in the Middle East, Africa, and Asia, where they can co-mingle terrorism and insurgency.

• ISIS and al-Qa‘ida and their respective networks will be persistent threats, as will groups not subordinate to them, such as the Haqqani Taliban Network.

**Sunni Violent Extremists’ Primary Operating Areas as of 2017**

**ISIS**

*Over the next year, we expect that ISIS is likely to focus on regrouping in Iraq and Syria, enhancing its global presence, championing its cause, planning international attacks, and encouraging its members and sympathizers to attack in their home countries. ISIS’s claim of having a functioning caliphate that governs populations is all but thwarted.*

• ISIS core has started—and probably will maintain—a robust insurgency in Iraq and Syria as part of a long-term strategy to ultimately enable the reemergence of its so-called caliphate. This activity will challenge local CT efforts against the group and threaten US interests in the region.

• ISIS almost certainly will continue to give priority to transnational terrorist attacks. Its leadership probably assesses that, if ISIS-linked attacks continue to dominate public discourse, the group’s narrative will be buoyed, it will be difficult for the counter-ISIS coalition to portray the group as defeated, and the coalition’s will to fight will ultimately weaken.

• Outside Iraq and Syria, ISIS’s goal of fostering interconnectivity and resiliency among its global branches and networks probably will result in local and, in some cases, regional attack plans.
Al-Qa’ida

Al-Qa’ida almost certainly will remain a major actor in global terrorism because of the combined staying power of its five affiliates. The primary threat to US and Western interests from al-Qa’ida’s global network through 2018 will be in or near affiliates’ operating areas. Not all affiliates will have the intent and capability to pursue or inspire attacks in the US homeland or elsewhere in the West.

- Al-Qa’ida’s affiliates probably will continue to dedicate most of their resources to local activity, including participating in ongoing conflicts in Afghanistan, Somalia, Syria, and Yemen, as well as attacking regional actors and populations in other parts of Africa, Asia, and the Middle East.

- Al-Qa’ida leaders and affiliate media platforms almost certainly will call for followers to carry out attacks in the West, but their appeals probably will not create a spike in inspired attacks. The group’s messaging since at least 2010 has produced few such attacks.

Homegrown Violent Extremists

Homegrown violent extremists (HVEs) will remain the most prevalent and difficult-to-detect Sunni terrorist threat at home, despite a drop in the number of attacks in 2017. HVE attacks are likely to continue to occur with little or no warning because the perpetrators often strike soft targets and use simple tactics that do not require advanced skills or outside training.

- HVEs almost certainly will continue to be inspired by a variety of sources, including terrorist propaganda as well as in response to perceived grievances related to US Government actions.

Iran and Lebanese Hizballah

Iran remains the most prominent state sponsor of terrorism, providing financial aid, advanced weapons and tactics, and direction to militant and terrorist groups across the Middle East and cultivating a network of operatives across the globe as a contingency to enable potential terrorist attacks.

Lebanese Hizballah has demonstrated its intent to foment regional instability by deploying thousands of fighters to Syria and by providing weapons, tactics, and direction to militant and terrorist groups. Hizballah probably also emphasizes its capability to attack US, Israeli, and Saudi Arabian interests.

COUNTERINTELLIGENCE AND FOREIGN DENIAL AND DECEPTION

The United States will face a complex global foreign intelligence threat environment in 2018. We assess that the leading state intelligence threats to US interests will continue to be Russia and China, based on their services’ capabilities, intent, and broad operational scope. Other states in the Near East, South Asia, East Asia, and Latin America will pose local and regional intelligence threats to US interests. For example, Iranian and Cuban intelligence and security services continue to view the United States as a primary threat.
Penetrating the US national decisionmaking apparatus and the Intelligence Community will remain primary objectives for numerous foreign intelligence entities. Additionally, the targeting of national security information and proprietary information from US companies and research institutions involved with defense, energy, finance, dual-use technology, and other areas will remain a persistent threat to US interests.

Nonstate entities, including international terrorists and transnational organized crime groups, are likely to continue to employ and improve their intelligence capabilities, including human, technical, and cyber means. As with state intelligence services, these nonstate entities recruit sources and perform physical and technical surveillance to facilitate their illicit activities and to avoid detection and capture.

Trusted insiders who disclose sensitive or classified US Government information without authorization will remain a significant threat in 2018 and beyond. The sophistication and availability of information technology that increases the scope and impact of unauthorized disclosures exacerbate this threat.

**Russia and Influence Campaigns**

*Influence operations, especially through cyber means, will remain a significant threat to US interests as they are low-cost, relatively low-risk, and deniable ways to retaliate against adversaries, to shape foreign perceptions, and to influence populations. Russia probably will be the most capable and aggressive source of this threat in 2018, although many countries and some nonstate actors are exploring ways to use influence operations, both domestically and abroad.*

*We assess that the Russian intelligence services will continue their efforts to disseminate false information via Russian state-controlled media and covert online personas about US activities to encourage anti-US political views. Moscow seeks to create wedges that reduce trust and confidence in democratic processes, degrade democratization efforts, weaken US partnerships with European allies, undermine Western sanctions, encourage anti-US political views, and counter efforts to bring Ukraine and other former Soviet states into European institutions.*

- Foreign elections are critical inflection points that offer opportunities for Russia to advance its interests both overtly and covertly. The 2018 US mid-term elections are a potential target for Russian influence operations.
- At a minimum, we expect Russia to continue using propaganda, social media, false-flag personas, sympathetic spokespeople, and other means of influence to try to exacerbate social and political fissures in the United States.

**EMERGING AND DISRUPTIVE TECHNOLOGY**

*New technologies and novel applications of existing technologies have the potential to disrupt labor markets and alter health, energy, and transportation systems.*
We assess that technology developments—in the biotechnology and communications sectors, for example—are likely to outpace regulation, which could create international norms that are contrary to US interests and increase the likelihood of technology surprise. Emerging technology and new applications of existing technology will also allow our adversaries to more readily develop weapon systems that can strike farther, faster, and harder and challenge the United States in all warfare domains, including space.

- The widespread proliferation of artificial intelligence (AI)—the field of computer science encompassing systems that seek to imitate aspects of human cognition by learning and making decisions based on accumulated knowledge—is likely to prompt new national security concerns; existing machine learning technology, for example, could enable high degrees of automation in labor-intensive activities such as satellite imagery analysis and cyber defense. Increasingly capable AI tools, which are often enabled by large amounts of data, are also likely to present socioeconomic challenges, including impacts on employment and privacy.

- New biotechnologies are leading to improvements in agriculture, health care, and manufacturing. However, some applications of biotechnologies may lead to unintentional negative health effects, biological accidents, or deliberate misuse.

- The global shift to advanced information and communications technologies (ICT) will increasingly test US competitiveness because aspiring suppliers around the world will play a larger role in developing new technologies and products. These technologies include next-generation, or 5G, wireless technology; the internet of things; new financial technologies; and enabling AI and big data for predictive analysis. Differences in regulatory and policy approaches to ICT-related issues could impede growth and innovation globally and for US companies.

- Advanced materials could disrupt the economies of some commodities-dependent exporting countries while providing a competitive edge to developed and developing countries that create the capacity to produce and use the new materials. New materials, such as nanomaterials, are often developed faster than their health and environmental effects can be assessed. Advances in manufacturing, particularly the development of 3D printing, almost certainly will become even more accessible to a variety of state and nonstate actors and be used in ways contrary to our interests.

TECHNOLOGY ACQUISITIONS AND STRATEGIC ECONOMIC COMPETITION

Persistent trade imbalances, trade barriers, and a lack of market-friendly policies in some countries probably will continue to challenge US economic security. Some countries almost certainly will continue to acquire US intellectual property and
propriety information illicitly to advance their own economic and national security objectives.

- China, for example, has acquired proprietary technology and early-stage ideas through cyber-enabled means. At the same time, some actors use largely legitimate, legal transfers and relationships to gain access to research fields, experts, and key enabling industrial processes that could, over time, erode America’s long-term competitive advantages.

SPACE AND COUNTERSPACE

Continued global space industry expansion will further extend space-enabled capabilities and space situational awareness to nation-state, nonstate, and commercial space actors in the coming years, enabled by the increased availability of technology, private-sector investment, and growing international partnerships for shared production and operation. All actors will increasingly have access to space-derived information services, such as imagery, weather, communications, and positioning, navigation, and timing for intelligence, military, scientific, or business purposes. Foreign countries—particularly China and Russia—will continue to expand their space-based reconnaissance, communications, and navigation systems in terms of the numbers of satellites, the breadth of their capability, and the applications for use.

Both Russia and China continue to pursue antisatellite (ASAT) weapons as a means to reduce US and allied military effectiveness. Russia and China aim to have nondestructive and destructive counterspace weapons available for use during a potential future conflict. We assess that, if a future conflict were to occur involving Russia or China, either country would justify attacks against US and allied satellites as necessary to offset any perceived US military advantage derived from military, civil, or commercial space systems. Military reforms in both countries in the past few years indicate an increased focus on establishing operational forces designed to integrate attacks against space systems and services with military operations in other domains.

Russian and Chinese destructive ASAT weapons probably will reach initial operational capability in the next few years. China’s PLA has formed military units and begun initial operational training with counterspace capabilities that it has been developing, such as ground-launched ASAT missiles. Russia probably has a similar class of system in development. Both countries are also advancing directed-energy weapons technologies for the purpose of fielding ASAT weapons that could blind or damage sensitive space-based optical sensors, such as those used for remote sensing or missile defense.

Of particular concern, Russia and China continue to launch “experimental” satellites that conduct sophisticated on-orbit activities, at least some of which are intended to advance counterspace capabilities. Some technologies with peaceful applications—such as satellite inspection, refueling, and repair—can also be used against adversary spacecraft.