Joint Statement for the Record

to the

Senate Armed Services Committee

Foreign Cyber Threats to the United States

The Honorable James R. Clapper
Director of National Intelligence

The Honorable Marcel Lettre
Undersecretary of Defense for Intelligence

Admiral Michael S. Rogers, USN
Commander, U.S. Cyber Command
Director, National Security Agency

5 January 2017

JOINT STATEMENT FOR THE RECORD

5 January 2017

INTRODUCTION

Chairman McCain, Vice Chairman Reed, and Members of the Committee thank you for the invitation to offer the testimony of the Department of Defense and the Intelligence Community on cyber threats to U.S. national security. Our statement reflects the collective insights of the Intelligence Community's extraordinary men and women whom we are privileged to lead. We in the Intelligence Community are committed every day to provide the nuanced, multidisciplinary intelligence that policymakers, warfighters, and domestic law enforcement personnel need to protect American lives and America's interests anywhere in the world.

The order of the topics presented in this statement does not necessarily indicate the relative importance or magnitude of the threat in the view of the Intelligence Community.

Information available as of 1 January 2017 was used in the preparation of this assessment.

JOINT STATEMENT FOR THE RECORD

Information and communication technologies play an increasing role in the security of the United States. Cyberspace is both a resource on which our continued security and prosperity depends, and a globally contested medium within which threats manifest themselves. As their cyber capabilities grow, our adversaries are demonstrating a willingness to use cyberspace as a platform for espionage, attack, and influence. Foreign Intelligence Entities continue to quietly exploit our nation's public and private sectors in the pursuit of policy and military insights, sensitive research, intellectual property, trade secrets, and personally identifiable information.

Cyber threats have already challenged public trust and confidence in global institutions, governance, and norms, while imposing costs on the global economy. These threats pose an increasing risk to public safety, as cyber technologies are integrated with critical infrastructure in key sectors. Adversaries also continue to use cyber operations to undermine U.S. military and commercial advantage by hacking into U.S. defense industry and commercial enterprises. The breadth of cyber threats posed to U.S. national and economic security has become increasingly diverse, sophisticated, and serious, leading to physical, security, economic, and psychological consequences.

Despite ever-improving cyber defenses, nearly all information, communication networks, and systems will be at risk for years to come from remote hacking to establish persistent covert access, supply chain operations that insert compromised hardware or software, malicious actions by trusted insiders, and mistakes by system users. In short, the cyber threat cannot be eliminated. Rather, cyber risk must be managed in the context of overall business and operational risk. At present, however, the risk calculus some private and public sector entities employ does not adequately account for foreign cyber threats or systemic interdependencies between different critical infrastructure sectors.

We assess that some countries might be willing to explore limits on cyber operations against certain targets, although few are likely to support total bans on the development of offensive capabilities. Many countries view cyber capabilities as a useful foreign policy tool that also is integral to their domestic security, and will continue developing these capabilities. Some also remain undeterred from conducting reconnaissance, espionage, and even preparation for attacks in cyberspace.

Physical Consequences

Our adversaries have capabilities to hold at risk U.S. critical infrastructure as well as the broader ecosystem of connected consumer and industrial devices known as the "Internet of Things." Security researchers continue to discover vulnerabilities in consumer products including automobiles and medical devices. Examples of cyber incidents with real world consequences include a cyber attack on a Ukrainian power network in 2015 that caused power outages for several hours and a "ransomware"—software designed to block a user's access to data, sometimes by encrypting it—infection that forced a hospital in the United Kingdom in late 2016 to cancel scheduled medical procedures, divert trauma patients to other hospitals, and impact

access to essential services such as blood transfusions. If adversaries achieve the ability to create significant physical effects inside the United States via cyber means, this would provide them new avenues for coercion and deterrence.

Commercial and Security Consequences

Our adversaries continue to use cyber operations to undermine U.S. military and commercial advantage by hacking into U.S. defense industry and commercial enterprises in the pursuit of scientific, technical, and business information. Examples include theft of data on the F-35 Joint Strike Fighter, the F-22 Raptor fighter jet, and the MV-22 Osprey. This espionage reduces our adversaries' costs and accelerates their weapon systems development programs, enables reverse-engineering and countermeasures development, and undermines U.S. military, technological, and commercial advantage. In addition, adversaries often target personal accounts of government and industry officials as well as their close associates to enable cyber operations.

Psychological Consequences

The impact of cyber threats extends beyond the physical, security and commercial realms. Online information operations and manipulation from both states and non-state actors can distort the perceptions of the targeted victim and other audiences through the anonymous delivery of manipulative content that seeks to gain influence or foment confusion and distrust. Information taken through cyber espionage can be leaked intact or selectively altered in content. For example, Russian actors have seeded falsified information into social media and news feeds and websites in order to sow doubt and confusion, erode faith in democratic institutions, and attempt to weaken Western governments by portraying them as inherently corrupt and dysfunctional.

Cyber Policy, Diplomacy, and Warfare

Foreign Cyber Policies. National and domestic security interests are an important component of global Internet policy, as is a robust and stable global digital economy and the free flow of information online. As foreign countries seek to balance security, economic growth, and interoperability objectives, many are implementing new laws and technical changes to monitor and control access to information within and across their borders and to control user access through means such as restrictions on encryption and steps to reduce anonymity online. However, these states will probably not significantly erode the overall global connectivity of the Internet. Furthermore, some state information control efforts will almost certainly be challenged by a broad coalition of states and non-state cyber stakeholders, including innovative technologists, industry leaders, privacy advocates, hackers, and others with an interest in opposing censorship or government control of cyberspace.

Diplomacy. In 2015, following a China-U.S. bilateral joint statement on this issue, G-20 leaders affirmed that that no country should conduct or support cyber-enabled theft of intellectual property with the intent of providing competitive advantages to companies or commercial sectors. U.S. diplomatic efforts continue to focus on the promotion of a strategic framework of international cyber stability during peacetime and during armed conflict that is built on three pillars: global affirmation of the applicability of existing international law to State activity in cyberspace; the development of international consensus on certain additional voluntary, non-binding norms of responsible State behavior in cyberspace during peacetime; and the development and implementation of practical confidence-building measures to facilitate inter-

State cooperation on cyber-related matters. The promotion of this framework is complicated by efforts to build and enhance international cooperation to address shared threats. These efforts also are hampered by the lack of consensus over key concepts such as what constitutes an armed attack, act of aggression, or the use of force in cyberspace. Furthermore, countries do not widely agree on how such principles of international law as proportionality of response or even the application of sovereignty apply in cyberspace.

Cyber Warfare. As of late 2016 more than 30 nations are developing offensive cyber attack capabilities. The proliferation of cyber capabilities coupled with new warfighting technologies will increase the incidence of standoff and remote operations, especially in the initial phases of conflict. Cyber attacks against critical infrastructure and information networks also will give actors a means of bypassing traditional defense measures and minimizing the advantage of geography to impose costs directly on their targets from a distance. Russian officials, for example, have noted publicly that initial attacks in future wars might be made through information networks in order to destroy critically important infrastructure, undermine an enemy's political will, and disrupt military command and control. Adversaries equipped with similar offensive cyber capabilities could be prone to preemptive attack and rapid escalation in a future crisis, because both sides would have an incentive to strike first. Cyber attacks against private sector networks and infrastructure could provoke a cyber-response by the intended target, raising the possibility of corporate and other non-state actor involvement in future cyber conflict and blurring the distinction between state and non-state action. Protecting critical infrastructure, such as crucial energy, financial, manufacturing, transportation, communication, and health systems, will become an increasingly complex national security challenge.

Cyber Threat Actors

Russia. Russia is a full-scope cyber actor that poses a major threat to U.S. Government, military, diplomatic, commercial, and critical infrastructure and key resource networks because of its highly advanced offensive cyber program and sophisticated tactics, techniques, and procedures. In recent years, we have observed the Kremlin assume a more aggressive cyber posture. Russian cyber operations targeted government organizations, critical infrastructure, think tanks, universities, political organizations, and corporations often using spearphishing campaigns. In foreign countries, Russian actors conducted damaging and/or disruptive cyber-attacks, including attacks on critical infrastructure networks. In some cases Russian intelligence actors have masqueraded as third parties, hiding behind false online personas designed to cause the victim to misattribute the source of the attack. We assess that only Russia's senior-most officials could have authorized the recent election-focused data thefts and disclosures, based on the scope and sensitivity of the targets. Russia also has used cyber tactics and techniques to seek to influence public opinion across Europe and Eurasia. Looking forward, Russian cyber operations will likely target the United States to gather intelligence, support Russian decisionmaking, conduct influence operations to support Russian military and political objectives, and prepare the cyber environment for future contingencies.

China. Beijing continues to conduct cyber espionage against the U.S. Government, our allies, and U.S. companies. Since the China-U.S. cyber commitments in September 2015, private-sector security experts continue to detect cyber activity from China, although at reduced levels and without confirmation that stolen data was used for commercial gain. Beijing has also

selectively used cyber attacks against foreign targets that it probably believes threaten Chinese domestic stability or regime legitimacy. China continues to integrate and streamline its cyber operations and capabilities into a dedicated cyber element that will be increasingly difficult to detect or counter.

Iran. Tehran continues to leverage cyber espionage, propaganda, and attacks to support its security priorities, influence events and perceptions, and counter threats—including against U.S. allies in the Middle East. Iran has also used its cyber capabilities directly against the United States, as in distributed denial of service attacks in targeting the U.S. financial sector in 2012-13.

North Korea. Pyongyang remains capable of launching disruptive or destructive cyber attacks to support its political objectives, as demonstrated by its destructive attack against Sony Pictures Entertainment in 2014. South Korean officials have also concluded that North Korea was probably responsible for the 2014 compromise, exfiltration, and disclosure of data from a South Korean nuclear plant, and for numerous denial of service and data deletion attacks.

Terrorists. Terrorists groups—to include al-Qa'ida, Hizballah, HAMAS, and the Islamic State of Iraq and the Levant (ISIL)—continue to use the Internet to collect intelligence, coordinate operations, raise funds, spread propaganda, and incite action. Groups such as the Taliban also use Internet-based technology for similar purposes. While not as sophisticated as some state actors, Hizballah and HAMAS will continue to build on their cyber successes inside and outside the Middle East. ISIL personnel will continue to seek opportunities to target and release sensitive information about U.S. citizens in an effort to spur "lone-wolf" attacks as demonstrated in their 2015 operations that disclosed potential targeting information about U.S. military personnel.

Criminals. Cybercrime remains a persistent and prevalent malicious activity in cyberspace. Criminals develop and use sophisticated cyber tools for a variety of purposes including theft, extortion, and facilitation of other criminal activity. "Ransomware has become a particularly popular and effective tool for extortion, one for which few options for recovery or remediation are available if the victim has not previously backed up the affected data. In 2016, criminals employing ransomware targeted the medical sector, disrupting patient care and undermining public confidence in medical institutions. Some criminals use markets conducted on the so-called dark web to sell or lease malware to anyone willing to pay, including state and non-state actors.

Responses

Perhaps the most significant counterintelligence threat to our nation, both currently and in the future, involves the rapid development and proliferation of disruptive, advanced technologies that provide adversaries with capabilities that even just a few years ago were not considered plausible. Sophisticated technical collection through a variety of means is available to more adversaries than ever before and can occur virtually anywhere and involve telephones, computers, Internet, cell phones, wired and wireless networks, as well as conversations and activities in offices, homes, vehicles, and public spaces. Disruptive technology is being built and fielded at an unprecedented rate, and we are already dealing with the consequences of a hyper-connected world. The complexity of technological advances, both in the tools themselves and

the methods used to compromise them, necessitates a much greater technical and cyber literacy than what was required of us even five years ago.

As we face this ever-changing cyber threat environment, the Intelligence Community and U.S. Cyber Command have been hardening internal U.S. Government systems, increasing knowledge and awareness among industry and the community, and engaging more closely with a host of partners to share best practices and threat information. The National Security Agency, in particular, has taken aggressive measures to hire and retain the cybersecurity talent needed to operate in this challenging environment. In addition, Cyber Command leverages the capacity and capabilities of 133 Cyber Mission Force teams that are responsible for synchronizing and executing cyber operations to support combatant command operations, and for the defense and security of service component and Department of Defense Information Networks. Cyber Command has established close working relationships with both international and interagency partners and stands ready to support a whole of nation response. The National Counterintelligence and Security Center's (NCSC) innovative public awareness campaign has resulted in placing numerous short informative videos on its public-facing website concerning cyber and associated threats, which are of immediate, practical use to federal, industry and community partners alike. NCSC also established a National Counterintelligence Task Force for Critical Infrastructure to coordinate counterintelligence efforts to mitigate this threat.

While many government organizations can make a unique contribution to securing our networks and the nation, no one agency has the capability to do so alone. The security of systems and networks is not the responsibility of one person or one agency or one industry, but rather requires a whole of nation response and a culture of cybersecurity among all users of the information space across private and public sectors.

The Intelligence Community and U.S. Cyber Command have been working to provide the Secretary of Defense and DoD policymakers with effective options for operational cyber responses to threats to U.S. interests. This remains a work in progress, and we welcome the assistance of this Committee in ensuring that we have the resources and authorities to succeed in this mission.

Conclusion

In summary, the breadth of cyber threats to U.S. national and economic security has become increasingly diverse, sophisticated, and dangerous. Over the next five years, technological change will only accelerate the intersection of cyber and physical devices, creating new risks. Adversaries are likely to further explore cyber-enabled psychological operations and may look to steal or manipulate data to gain strategic advantage or undermine confidence. The Intelligence Community has been vigilant in the detecting and sharing of cyber threat information with partners such as U.S. Cyber Command, as well as our nation's network protection organizations such as the Department of Homeland Security, and will continue to do so for the safety of our nation.