Statement for the Record

U.S. Cybersecurity and Policy

Senate Armed Services Committee

James R. Clapper

Director of National Intelligence

September 29, 2015

STATEMENT FOR THE RECORD

Worldwide Cyber Threats

September 29, 2015

INTRODUCTION

Chairman McCain, Ranking Member Reed, Members of the Committee, thank you for the invitation to offer this Statement for the Record. My statement reflects the collective insights of the Intelligence Community's extraordinary men and women, whom I am privileged and honored 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.

Information available as of September 28, 2015 was used in the preparation of this Statement for the Record.

Worldwide Cyber Threats

Overview

Cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact. The ranges of cyber threat actors, methods of attack, targeted systems, and victims are also expanding. Overall, the unclassified information and communication technology (ICT) networks that support U.S. Government, military, commercial, and social activities remain vulnerable to espionage and/or disruption. However, the likelihood of a catastrophic attack from any particular actor is remote at this time. Rather than a "Cyber Armageddon" scenario that debilitates the entire U.S. infrastructure, we envision something different. We foresee an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time, which will impose cumulative costs on U.S. economic competitiveness and national security.

- Several nations-including Iran and North Korea-have undertaken offensive cyber operations against private sector targets to support their economic and foreign policy objectives, at times concurrent with political crises.

Risk. Despite ever-improving network defenses, the diverse possibilities available through remote hacking intrusion, supply chain operations to insert compromised hardware or software, actions by malicious insiders, and mistakes by system users will hold nearly all ICT networks and systems at risk for years to come. In short, the cyber threat cannot be eliminated; rather, cyber risk must be managed. Moreover, the risk calculus employed by some private sector entities does not adequately account for foreign cyber threats or the systemic interdependencies between different critical infrastructure sectors.

Costs. We continue to witness an increase in the scale and scope of reporting on malicious cyber activity that can be measured by the amount of corporate data stolen or deleted, personally identifiable information (PII) compromised, or remediation costs incurred by U.S. victims. For example:

- Earlier this year, the Office of Personnel Management (OPM) discovered that a number of its systems were compromised. In April 2015, OPM discovered that the personnel data of 4.2 million current and former Federal government employees had been compromised. Further, in the course of investigating this initial incident, OPM discovered that additional systems had been compromised, including those that contain background investigation records of current, former, and prospective Federal government employees and

contractors. OPM and the interagency incident response team have concluded with high confidence that sensitive information from the background investigation databases on as many as 21.5 million individuals, was potentially compromised.

- After the 2012-13 distributed denial of service (DDOS) attacks on the U.S. financial sector, JPMorgan Chase (JPMorgan) announced plans for annual cyber security expenditures of $250 million by the end of 2014. After the company suffered a hacking intrusion in 2014, JPMorgan's CEO said he would probably double JP Morgan 's annual computer security budget within the next five years.

- The 2014 data breach at Home Depot exposed information from 56 million credit/debit cards and 53 million customer email addresses. Home Depot estimated the cost of the breach to be $62 million.

- In August 2014, the U.S. company, Community Health Systems, informed the Securities and Exchange Commission that it believed hackers "originating from China" had stolen PII on 4.5 million individuals.

Attribution. Although cyber operators can infiltrate or disrupt targeted ICT networks, most can no longer assume that their activities will remain undetected indefinitely. Nor can they assume that if detected, they will be able to conceal their identities. Governmental and private sector security professionals have made significant advances in detecting and attributing cyber intrusions.

- In May 2014, the U.S. Department of Justice indicted five officers from China's Peoples' Liberation Army on charges of hacking and economic espionage against U.S. companies to steal information that would be useful to Chinese competitors.

- In December 2014, computer security experts reported that members of an Iranian organization were responsible for computer operations targeting U.S. military, transportation, public utility, and other critical infrastructure networks.

Determining attribution or responsibility for a malicious cyber activity is a complicated process, and we can have differing levels of confidence in our assessment of where geographically the activity came from, who conducted it, and who made the decisions or gave the orders. Publicly naming the malicious actor responsible for an intrusion or other malicious cyber act is a step that, once taken, cannot readily be undone, and that the U.S.

Government will consider using when it furthers our ability to impose costs or otherwise hold those actors accountable.

Deterrence. Numerous actors remain undeterred from conducting economic cyber espionage or perpetrating cyber attacks. The absence of universally accepted and enforceable norms of behavior in cyberspace has contributed to this situation, although some progress is being made on issues of mutual concern to all states (e.g., refraining from cyber attacks against critical infrastructure in peacetime). The motivation to conduct cyber attacks and cyber espionage will probably remain strong because of the relative ease of these operations and the gains they bring to the perpetrators. The result is a cyber environment in which multiple actors continue to test their adversaries' technical capabilities, political resolve, and thresholds. The muted response by most victims to cyber attacks has created a permissive environment in which low-level attacks can be used as a coercive tool short of war, with relatively low risk of retaliation. Additionally, even when a cyber attack can be attributed to a specific actor, the forensic attribution often requires a significant amount of time to complete. Long delays between the cyber attack and determination of attribution likewise reinforce a permissive environment.

Threat Actors

Politically motivated cyber attacks are a growing reality, and foreign actors are reconnoitering and developing access to U.S. critical infrastructure systems, which might be quickly exploited for disruption if an adversary's intent became hostile. In addition, those conducting cyber espionage are targeting U.S. government, military, and commercial networks on a daily basis. These threats come from a range of actors, including: (1) nation states with highly sophisticated cyber programs (such as Russia or China),
(2) nations with lesser technical capabilities but possibly more disruptive intent (such as Iran or North Korea), (3) profit-motivated criminals, and (4) ideologically motivated hackers or extremists. Distinguishing between state and non-state actors within the same country is often difficult-especially when those varied actors actively collaborate, tacitly cooperate, condone criminal activity that only harms foreign victims, or utilize similar cyber tools.

Russia. Russia's Ministry of Defense is establishing its own cyber command, which-according to senior Russian military officials-will be responsible for conducting offensive cyber activities, including propaganda operations and inserting malware into enemy command and control systems. Russia's armed forces are also establishing a specialized branch for computer network operations.

- Computer security studies assert that Russian cyber actors are developing means to remotely access industrial control systems (ICS) used to manage critical infrastructures. Unknown Russian actors successfully compromised the product supply chains of at least three ICS vendors so that customers downloaded malicious software ("malware") designed to facilitate exploitation directly from the vendors' websites along with legitimate software updates, according to private sector cyber security experts.

China. Chinese cyber-enabled theft of U.S. companies' intellectual property for commercial gain remains a significant issue. Although China is an advanced cyber actor in terms of capabilities, Chinese hackers are often able to succeed in establishing access to their targets using less sophisticated cyber tools and techniques. Improved cyber security would require these hackers to use more sophisticated capabilities and would make China's economic espionage more costly and difficult to conduct.

Iran. Iranian actors have been implicated in the 2012-13 DDOS attacks against U.S. financial institutions and in the February 2014 cyber attack on the Las Vegas Sands casino company. Iran very likely views its cyber program as one of many tools for carrying out asymmetric but proportional retaliation against political foes, as well as a sophisticated means of collecting intelligence.

North Korea. North Korea is another state actor that uses its cyber capabilities for political objectives. The North Korean Government was responsible for the November 2014 cyber attack on Sony Pictures Entertainment (SPE), which stole corporate information and introduced hard drive erasing malware into the company's network infrastructure, according to the FBI. The attack coincided with the planned release of a SPE feature film satire that depicted the fictional assassination of the North Korean leader.

Profit-motivated criminals. Profit motivated cyber criminals rely on loosely networked online marketplaces, often referred to as the cyber underground, that provide a forum for the merchandising of illicit tools, services, infrastructure, stolen PII and financial data. As media reports have documented, cyber criminals continue to successfully compromise the networks of retail businesses and financial institutions in order to collect financial information, biographical data, home addresses, email addresses, and medical records that serve as the building blocks to criminal operations that facilitate identity theft and healthcare fraud. The most significant financial cyber criminal threats to U.S. entities and our international partners can be attributed to a relatively small subset of actors, facilitators, infrastructure, and criminal

forums.

However, our Federal law enforcement colleagues continue to have successes capturing key cyber criminals by cooperating with international partners. For example, in late June, the Department of Justice and the United States Secret Service worked with their German counterparts to extradite Ercan Findikoglu, a Turkish national, responsible for multiple cyber crime campaigns that targeted the U.S. financial sector stealing $55 million dollars between 2011 and 2013. Findikoglu was apprehended by the German Federal Police after U.S. Secret Service agents confirmed he was traveling through Germany in December 2013. Additionally, this month an FBI-led coalition of international partners from 20 countries dismantled an online criminal forum known as Darkode. According to the Department of Justice, this forum represented one of the gravest threats to the integrity of data stored on computers in the United States and elsewhere.

Terrorists. Terrorist groups will continue to experiment with hacking, which could serve as the foundation for developing more advanced capabilities. Terrorist sympathizers will probably conduct low-level cyber attacks on behalf of terrorist groups and attract attention of the media, which might exaggerate the capabilities and threat posed by these actors.

With respect to the Islamic State of Iraq and the Levant (ISIL), since last summer, the group began executing a highly strategic social media campaign using a diverse array of platforms and thousands of online supporters around the globe. The group quickly builds expertise in the platforms it uses and often leverages multiple tools within each platform. ISIL and its adherents' adept use of social media allows the group to maximize the spread of its propaganda and reach out to potential recruits.

Integrity of Information

Most of the public discussion regarding cyber threats has focused on the confidentiality and availability of information; cyber espionage undermines confidentiality, whereas denial-of-service operations and data- deletion attacks undermine availability. In the future, however, we might also see more cyber operations that will change or manipulate electronic information in order to compromise its integrity (i.e. accuracy and reliability) instead of deleting it or disrupting access to it. Decision-making by senior government officials (civilian and military), corporate executives, investors, or others will be impaired if they cannot trust the information they are receiving.

- Successful cyber operations targeting the integrity of information would need to

overcome any institutionalized checks and balances designed to prevent the manipulation of data, for example, market monitoring and clearing functions in the financial sector.

Counterintelligence

Internet users are disclosing more information about themselves through social media platforms, online transactions, and search engine queries. New business models for online services often require disclosure of personal information or consent to allow corporate monitoring of one's online activities. Governments and third parties digitize public records and share them on the Internet for accessibility, making online records an unavoidable byproduct of living in a digitized society.

Counterintelligence risks are inherent when foreign intelligence agencies obtain access to an individual's PII or virtual identity information. Foreign intelligence agencies could target the individual, family members, coworkers, and neighbors using a variety of physical and electronic methods. The methods foreign intelligence agencies use to exploit targets require a comprehensive mitigation effort that involves CI awareness not only from the individual, but also from family members and coworkers that might have their data compromised as part of the individual's investigation.

An Integrated Approach

As the President has said, and as is evident from my testimony today, cyber threats pose one of the gravest national security dangers to the United States. As with our counterterrorism efforts, the United States Government is taking a "whole-of-government" approach to defend against and respond to these threats. The creation of the Cyber Threat Intelligence Integration Center (CTIIC) is a crucial part of this effort. The CTIIC will be a national cyber threat intelligence center that will "connect the dots" regarding malicious foreign cyber threats to the nation so that relevant departments and agencies are aware of these threats in as close to real time as possible. The CTIIC will provide integrated all-source analysis of foreign cyber threats and cyber incidents affecting U.S. national interests, help ensure that the U.S. government centers responsible for cybersecurity and network defense have access to the intelligence needed to perform their missions, and facilitate and support efforts by the government to counter foreign cyber threats.

In my view, the CTIIC will improve our situational awareness, enhance indications and

warning, and strengthen cyber unity of effort for the U.S. government. It will ensure indicators of malicious activity are downgraded to the lowest possible classification level to facilitate seamless intelligence flows among centers, including those responsible for sharing with the private sector. Most importantly, the CTIIC will augment that "whole-of-government" approach by providing policymakers with a cross-agency, integrated view of foreign cyber threats, their severity, and potential attribution.

Conclusion

In summary, the breadth of cyber threats posed to U.S. national and economic security has become increasing diverse, sophisticated, and impactful. Cyber intelligence -- collecting, analyzing, and disseminating intelligence on the intentions, capabilities, and operational activities of foreign cyber actors - is one of the core objectives in the National Intelligence Strategy we produced last year to guide the information and guide the activities of the IC. Ensuring the integration of such activities in support of our policy makers and national security is a core mission for the Office of the ODNI, and was one reason the President, directed me to form CTIIC. I look forward to working with the Senate and my interagency colleagues to enable the IC in general and CTIIC in particular to better support our nation in this vital area. Thank you.