
**Statement for the Record**

**Mr. Michael Moss**

**Deputy Director**

**Cyber Threat Intelligence Integration Center**

**Office of the Director of National Intelligence**

**FOR A HEARING ON**

***"Cyber Threats to Our Nation's Critical Infrastructure"***

**BEFORE THE**

**UNITED STATES SENATE**

**COMMITTEE ON JUDCIARY**

**SUBCOMMITTEE ON CRIME AND TERRORISM**

**Tuesday 21 August 2018 Senate Dirksen 226 2:30pm – 4:00pm**

**Washington, DC**

Chairman Graham, Ranking Member Whitehouse, Members of the Subcommittee, thank you for the opportunity to appear before you today to discuss cyber threats.

I would first like to extend my appreciation for your efforts to focus attention on cyber threats through such forums as this subcommittee hearing.

It is hard to believe that just a year or two ago, cyber security experts routinely lamented the lack of attention these threats received in our public discourse. Now, it seems that we do not go a single day without a headline about a concerning vulnerability, a serious breach, or a call to action from a local, state, or federal official. Awareness of the threat is a critical first step to action, not only by the government but also, especially, every citizen, each of whom can take important steps to protect themselves while also increasing our collective cyber security.

The Director of National Intelligence wants the American people to know the Intelligence Community (IC) is postured to identify threats of all kinds against the U.S. and our allies, and to provide appropriate warnings.

Regarding the threat to our elections, and efforts to undermine our democracy, the IC's TOP priority is to identify threats against the U.S. and provide accurate, timely warnings. With respect to operations that target elections, it is important to distinguish between two types: (1) cyber operations that target our election systems, such as voting machines and voter databases, and (2) foreign malign influence operations designed to influence the views of voters, depress voter turnout, or undermine confidence in election results.

- The IC continues to be concerned about threats to upcoming US elections – both the mid-terms and the 2020 election cycle.
- Regarding Russian involvement in the mid-term elections, we continue to see a pervasive messaging campaign by Russia to try to weaken and divide the U.S. These efforts are not exclusive to the election, but certainly cover issues relevant to the election.
- We also know Russia tries to hack into and steal information from candidates and government officials alike.
- We are very cognizant that Russia is not the only country that has an interest in trying to influence our domestic political environment. We know there are others who have the capability and may be considering influence activities.

We have incorporated lessons learned from the 2016 elections, and implemented a broad spectrum of initiatives to share more information across the federal government, state and local governments, and with the private sector. Among those initiatives:

- The Office of the Director of National Intelligence's (ODNI's) National Counterintelligence and Security Center (NCSC) and Cyber Threat Intelligence Integration Center (CTIIC) co-sponsored an elections-focused Tabletop Exercise (TTX) in April, where we examined how to strengthen the U.S. Government's ability to share information on foreign threats to U.S. elections. The day-long TTX was attended by more than 50 senior representatives from the National Security Council and offices in the Central Intelligence Agency (CIA),

Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), National Security Agency (NSA), and ODNI that have cyber, counterintelligence, regional, and intelligence reporting responsibilities.

- ODNI leads the interagency working group with the Department of Justice (DOJ), FBI, DHS, CIA and NSA, regional, cyber and counterintelligence experts now meeting weekly as we push towards November all focused on ensuring election security and integration of our efforts.
- ODNI supports both DHS and FBI, in their respective roles, in their efforts to effectively provide States and State Election Officials with up to date and relevant information from the IC.

**Cyber Threat Intelligence Integration**

Enhanced awareness of cyber threat is one of the core missions of the center I am privileged to lead CTIIC and I would like to share with you our approach to this important mission.

CTIIC is the newest of four multiagency intelligence centers under the ODNI and was authorized under the Intelligence Authorization Act for Fiscal Year 2016. Our mission is to build understanding of foreign cyber threats to U.S. national interests to support decision-making. We do this by working with, and integrating information from, the Federal centers, and other departments and agencies that make up the federal cyber community. Elements of this community specialize in intelligence, law enforcement, network defense, operations, and incident response. CTIIC brings together information from these partners to build awareness, integrate analysis context, and identify opportunities to mitigate and counter cyber threats using all instruments of national power.

CTIIC's workforce is mostly composed of personnel on loan to us from these very partners. Our leadership team includes senior executives from FBI, NSA, and CIA; and our workforce includes analysts from those three agencies, DHS, the Defense Intelligence Agency, the Department of Energy, and the ODNI. These professionals contribute their unique expertise, knowledge and tradecraft, and notably their reach back to other experts in their parent Agency. Anticipating and countering foreign cyber threats is a whole-of-government effort, and the makeup of CTIIC is reflective of that effort.

In 2016, our first year of operation, CTIIC's role was further emphasized in Presidential Policy Directive 41. This PPD, outlining the Federal government's approach to *Cyber Incident Coordination,* named CTIIC as one of three Federal leads, along with DHS and FBI, responsible for coordinating the government's response to significant cyber incidents.

CTIIC does not direct or engage in intelligence collection, operations, or unilateral engagement with the private sector. Rather, we support the agencies who *do* have those responsibilities and relationships by providing integrated intelligence and assessments that support their efforts.

CTIIC is committed to overcoming the jargon barrier that sometimes limits our ability to have meaningful discussions of cyber threat. Part of enabling a whole-of-government

approach to countering these cyber threats is building understanding of how our adversaries are using capabilities in cyber space to address their strategic objectives. We, and our colleagues in ODNI, are focused on making that analysis available and comprehensible to the *non*-cyber experts in government, who vastly outnumber those of us who focus daily on this threat.

In many ways, the nature of the cyber threat requires that we, the national security community, also treat the private sector and American people as intelligence customers. That is why you will see us address this threat more publicly and why you will continue to see us publish unclassified estimates and statements to inform the American people.

## Cyber Threats to U.S. Critical Infrastructure

To that end, I will now address the IC's estimates of cyber threats to critical infrastructure. These threats include not only destructive attacks but also cyber-enabled theft of information that undermines our strategic advantage.

Our adversaries are becoming more assertive, more capable, and more adept at using cyberspace to threaten our interests. And, the number of adversaries is growing as nation states, terrorist groups, criminal organizations, and others continue to develop cyber capabilities.

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 U.S. in a crisis short of war.

The potential impact of these cyber threats is amplified by our growing interconnectedness. The advancing integration of technology—such as artificial intelligence and the internet of things—into both our critical infrastructure and our daily lives adds convenience but also significant risk.

The potential for surprise in the cyber realm will increase in the next year and beyond as billions of additional digital devices connect—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.

In 2016 and 2017, state-sponsored cyber attacks against Ukraine and Saudi Arabia targeted multiple sectors across critical infrastructure, government, and commercial networks. In the case of Ukraine, over 225,000 citizens lost power for over 3 hours.

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

In March, the city of Atlanta, Georgia, was hit by ransomware, crippling a large portion of the city's online systems. Citywide services came to a grinding halt. More than a third of the 424 software programs used by the city were knocked offline or partially disabled, and nearly 30% of those were "mission critical," affecting core city services.

We believe that concerns about U.S. retaliation, and still developing adversary capabilities, will mitigate the probability of attacks aimed at causing major disruptions of

U.S. 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 U.S. during the next year. These states are using cyber operations as a low-cost tool of statecraft, and we believe they will work to use cyber operations to achieve strategic objectives unless they face clear repercussions for their cyber operations. Meanwhile, non-state actors will continue to use cyber operations for financial crime and to enable propaganda and messaging.

Of these adversaries, we believe Russia poses the greatest threat to U.S. critical infrastructure. **We expect that Russia will conduct bolder and more disruptive cyber operations during the next year, most likely using new capabilities against Ukraine.** In June 2017, the Russian military launched the most destructive and costly cyber-attack in history. The attack, dubbed "NotPetya," quickly spread worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas. 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. Over the next year, Russian intelligence and security services will continue to probe U.S. and allied critical infrastructures, and target the U.S., NATO, and allies for insights into U.S. policy.

- In March, DHS and FBI issued a Technical Alert regarding Russian government targeting of U.S. Government entities and organizations in the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors.
- In April, as a result of analytic efforts between DHS, FBI, and the United Kingdom's National Cyber Security Centre, DHS and FBI issued an alert regarding the worldwide cyber exploitation of network infrastructure devices (e.g., router, switch, firewall, and Network-based Intrusion Detection System devices) by Russian state-sponsored cyber actors.
- In May, DOJ announced they had seized an internet domain at the center of a hacking campaign, thus thwarting the potential weaponization of a network of more than half a million web-connected devices across the globe. The network of infected devices, or "botnets", was one of the largest of its kind.

**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 lower than before the bilateral U.S.-China cyber commitments of September 2015. Most detected Chinese cyber operations against U.S. private industry are focused on cleared defense contractors or IT and communications firms whose products and services support government and private sector networks worldwide. Since 2015, China 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.

**We believe that Iran will continue working to penetrate U.S. and Allied networks for espionage and to position itself for potential future cyber attacks.** Tehran probably views cyberattacks as a versatile tool to respond to perceived provocations, despite Iran's recent restraint from conducting cyber attacks against the U.S. 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.

**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 U.S.** 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. We also believe that these actors conducted the cyber theft of $81 million from the Bank of Bangladesh in 2016.

**Terrorist and criminal 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 most 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 U.S. 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

Mr. Chairman, I look forward to the Sub-committee's questions.