Opening Statement on Foreign Cyber Threats
Chairman John McCain
January 5, 2017

Before we begin, I want to welcome all of our members back to the committee and extend a special welcome to the new members joining us. On the majority side, we are joined by Senator Perdue and Senator Sasse. On the minority side, we are joined by Senator Warren and Senator Peters.

It is a special privilege to serve on this committee, most of all because it affords us the opportunity to spend so much time in the company of heroes—the men and women who serve and sacrifice on our behalf every day. I hope you will come to cherish your service on this committee as much as I have over the years. And I look forward to working with each of you.

The committee meets this morning for the first in a series of hearings on cybersecurity to receive testimony on foreign cyber threats to the United States. I'd like to welcome our witnesses this morning:

- James Clapper, Director of National Intelligence;
- Marcel Lettre, Under Secretary of Defense for Intelligence; and
- Admiral Mike Rogers, Commander of U.S. Cyber Command, Director of the National Security Agency, and Chief of the Central Security Service.

This hearing is about the broad range of cybersecurity challenges confronting our nation—threats from countries like Russia, China, North Korea, and Iran, as well as non-state actors from terrorist groups to transnational criminal organizations. In recent years, we have seen a growing series of cyberattacks by multiple actors—attacks that have targeted our citizens, businesses, military, and government. But there is no escaping the fact that this committee meets today for the first time in this new Congress in the aftermath of an unprecedented attack on our democracy.

At the President's direction, Director Clapper is leading a comprehensive review of Russian interference in our recent election with the goal of informing the American people as much as possible about what happened. I am confident that Director Clapper will conduct this review with the same integrity and professionalism that has characterized his nearly half a century of government and military service. I am equally confident in the dedicated members of our intelligence community.

The goal of this review, as I understand it, is not to question the outcome of the presidential election. Nor should it be. As both President Obama and President-elect Trump have said, our nation must move forward. But we must do so with full knowledge of the facts. I trust Director Clapper will brief the Congress on his review when it is completed. This is not the time or place to preview its findings.

That said, we know a lot already. In October, our intelligence agencies concluded unanimously that "the Russian Government directed … compromises of e-mails from U.S. persons and institutions, including from U.S. political organizations." They also assessed that "disclosures of alleged hacked e-mails … [were] consistent with the methods and motivations of Russian-directed efforts," and that "these thefts and disclosures [were] intended to interfere with the U.S. election process."

Since then, our intelligence community has released additional information concerning these Russian activities, including a Joint Analysis Report that provided technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence services to attack the United States.

Every American should be alarmed by Russia's attacks on our nation. There is no national security interest more vital to the United States of America than the ability to hold free and fair elections without foreign interference. That is why Congress must set partisanship aside, follow the facts, and work together to devise comprehensive solutions to deter, defend against, and, when necessary, respond to foreign cyberattacks.

As we do, we must recognize that the recent Russian attacks are one part of a much bigger cyber problem. Russian cyberattacks have targeted the White House, the Joint Staff, the State Department, and our critical infrastructure. Chinese cyberattacks have reportedly targeted NASA, the Departments of State and Commerce, congressional offices, military labs, the Naval War College, and U.S. businesses, including major defense contractors. Most recently, China compromised over 20 million background investigations at the Office of Personnel Management. Iran has used cyber tools in recent years to attack the U.S. Navy, U.S. partners in the Middle East, major U.S. financial institutions, and a dam just 25 miles north of New York City. And of course, North Korea was responsible for the massive cyberattack on Sony Pictures in 2014.

What seems clear is that our adversaries have reached a common conclusion: that the reward for attacking America in cyberspace outweighs the risk. For years, cyberattacks on our nation have been met with indecision and inaction. Our nation has had no policy, and thus no strategy, for cyber deterrence. This appearance of weakness has been provocative to our adversaries, who have attacked us again and again, with growing severity. Unless we demonstrate that the costs of attacking the United States outweigh the perceived benefits, these cyber threats will only grow.

This is also true beyond the cyber domain. It should not surprise us that Vladimir Putin would think he could launch increasingly severe cyberattacks against our nation when he has paid little price for invading Ukraine, annexing Crimea, subverting democratic values and institutions across Europe, and of course, helping Bashar Assad slaughter civilians in Syria for more than a year with impunity. The same is true for China, Iran, North Korea, and any other adversary that has recently felt emboldened to challenge the world order. Put simply, we cannot achieve cyber deterrence without restoring the credibility of U.S. deterrence more broadly.

To do so, we must first have a policy, which means finally resolving the long list of basic cyber questions that we as a nation have yet to answer. What constitutes an act of war or aggression in cyberspace that would merit a military response, be it by cyber or other means? What is our theory of cyber deterrence, and what is our strategy to implement it? Is our government organized appropriately to handle this threat, or are we so stove-piped that we cannot deal with it effectively? Who is accountable for this problem, and do they have sufficient authorities to deliver results? Are we in the Congress just as stove-piped on cyber as the executive branch, such that our oversight actually reinforces problems rather than helping to resolve them? Do we need to change how we are organized?

This committee intends to hold a series of hearings in the months ahead to explore these and other questions. And we look forward to hearing the candid views of our distinguished witnesses today, who have thought about and worked on these questions as much as anyone in our nation.