Prepared Statement
by
Honorable Eric Rosenbach
Former DoD Chief of Staff; former Assistant Secretary of Defense for Homeland Defense and Global Security

Before the
United States Senate Committee on Commerce, Science and Transportation

Hearing on
"The Promises and Perils of Emerging Technologies for Cybersecurity"
Wednesday, March 22, 2017

Chairman Thune, Ranking Member Nelson, and distinguished members of the Committee, thank you for calling this important hearing on "The Promises and Perils of Emerging Technologies for Cybersecurity" and for the invitation to testify today.

The rapid rise of emerging technologies and the internet-of-things will result in essential economic growth for America. This is important: the United States must continue to make the development and adoption of emerging technologies an economic center of gravity. But as the number of internet-connected, artificial intelligence (AI) driven devices increases, policymakers and legislators need to address the associated increase in the nation's vulnerability to strategic cyberattacks. The fragility of our national cybersecurity posture, combined with our adversaries' perception that Russia's recent cyberattacks achieved unprecedented success, increases the likelihood that the United States will experience more serious attacks in the coming years.

As we unlock new technological innovation, we will live in a glass house that must be better protected. Without an improved defensive posture, this vulnerability may impact the calculus of US national security policymakers. Thus, it's important to understand the strategic perspectives of two competitors and adversaries in the cyber domain: China and Russia.

Chinese and Russian Strategy for Emerging Technologies

Over the past decade, China has pursued a national strategy to challenge the United States world leadership in emerging technologies. The Chinese government has invested heavily in the research and development of technology that underpins supercomputing, artificial intelligence, and blockchain. Those investments have resulted in genuine achievements. Last year, for example, China unveiled the world's fastest supercomputer – and announced that it owned more of the top 500 supercomputers than any other nation in the world. Chinese firms and research institutions, nearly always supported with state funds, have made advances in artificial intelligence that some corporate leaders believe will make China the world leader in hardware-based AI.

Over the past three years, China has also strategically established itself as the world leader in the research and deployment of blockchain technologies, particularly in the area of financial technology (known as Fintech). China currently leads the world in the number of citizens using internet payment and fintech applications, and the government continues to facilitate the growth of this sector with a permissive regulatory environment and strong investments fintech firms. China recognizes that the "Fintech Revolution" is about more than fancy payment apps and Bitcoin. It has the potential to disrupt the American-dominated financial sector and increase Chinese economic influence around the world.

Although the vast majority of China's investment and research in these emerging technologies focuses on improving the country's economic competitiveness, China also has programs dedicated to integrating new technology into security-focused cyber capabilities. For example, the Chinese have incorporated AI and supercomputing technology into the massive "Great Firewall of China" used to isolate Chinese internet users from the outside world. These advances give China an upper hand in not only defending their domestic critical infrastructure networks, but also in taking offensive actions against key targets, including in the United States.

In Russia, investment and research in emerging technologies are likely a decade behind the US and China; however, President Putin has taken a deep personal interest in quickly closing this gap. In the meantime, the clear recognition that Russia’s military does not have the ability to go head-to-head with next-generation US military capabilities has driven the Russian strategy to develop military cyber capabilities to disrupt new technologies in both civilian and military environments.   In short, the Russians know that they can impact American strategic calculus -and control the escalation ladder of conflict- by attacking civilian targets in the internet-of-things and the military networks that connect AI-enabled weapons. Combined with the Russians’ proven deep experience with spreading strategic disinformation, this form of cyberwar should be a serious concern.

Russia’s demonstrated willingness to conduct cyberattacks against civilian targets is unprecedented and has serious implications for a world that relies on the internet-of-things.   Recent Russian cyberattacks against Ukraine, which took down significant portions of that country’s power grid and represented one of the first known cyberattacks that resulted in a physical effect, barely drew criticism -let alone action- from the international community.   The Russians’ inevitable perception that they can conduct strategic cyberattacks with impunity is likely to encourage further attacks in the future.

Every American should be deeply concerned that the United States’ democratic system of governance was attacked by a foreign nation during an important presidential election. This is not a partisan matter. Our democratic system serves as an example to the free world. We must overcome politics to protect ourselves and our allies from being undermined by our adversaries in the future.

Chinese and Russian strategies for dealing with emerging technologies present the United States with two very different challenges: In China, the US faces a competitor who is focused primarily on developing next-generation technologies more quickly than the US in order displace us as the world’s economic and military leader. In Russia, the US faces an adversary who seeks use advanced cyberattacks and information operations to undermine the strength of our democracy and the efficacy of next-generation military technologies.

Although the challenges posed by these nations differ, both cases underscore the need for a new national cybersecurity strategy that forces bold action and cooperation by the government and private sector. To mitigate the risk of cyberattacks, one essential component of this strategy should be for the government and private sector to invest in and adopt new technologies that will aid cyber defense, such as AI-enabled cybersecurity, cloud-based security-as-a-service solutions, blockchain and super/quantum computing. Facilitating the development of these technologies will not only improve our cybersecurity, but also strengthen one of the few remaining American economic centers of gravity.

Additionally, a new strategy for national cybersecurity cyberspace contains at least three other components: 1) the US must immediately bolster deterrence of cyberattacks that threaten vital national interests; 2) Congress must clarify key regulatory issues that would promote the growth of key technologies with large potential to facilitate economic growth, such as blockchain and FinTech, and; 3) Congress must pass targeted legislation that provides the private sector with a framework for improved cybersecurity standards and incentives for information sharing.

The U.S. has enjoyed extraordinary economic success because of the open internet we created – it is imperative we lead the world in securing it for decades to come.