COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

Subcommittee Hearing Statement of Chairman Bennie G. Thompson (D-MS)

Securing the Future: Harnessing the Potential of Emerging Technologies while Mitigating Security Risks

June 22, 2022

Over the past several years, this country has seen a rapid proliferation of new technologies, from Artificial Intelligence (AI) to Internet of Things (IoT) to quantum computing. As a result of these new technologies, our attack surface has grown, and our adversaries have developed new tactics designed to directly harm U.S. democratic institutions, economic interests, and national security. As these new technologies have entered the marketplace, many became so mesmerized by their potential for good that we failed to appreciate and plan for the security consequences. With an enhanced threat landscape, we are now facing more cyber threats from our adversaries than ever before.

Furthermore, our adversaries are continuing to increase their own capabilities to take advantage of the security vulnerabilities within these new technologies. The DNI's 2022 Annual Threat Assessment of the U.S. Intelligence Community noted that a growing number of state and non-state actors are developing novel approaches to utilize both mature and new technologies to directly threaten U.S. national security. We are already very aware that this is happening.

There is a myriad of examples of Russia relying on its cyber and influence capabilities to directly threaten emerging technologies in the U.S., including those that are upholding our democratic institutions and critical infrastructure. Additionally, there is continuing concern that Russia will employ an array of tools targeting various emerging technologies to retaliate against the United States for its sanctions in the wake of their unlawful and horrific war with Ukraine.

When it comes to China, we know that they have engaged in intelligence-gathering and economic espionage. We know they have strong hacking capabilities. Chinese hackers were recently able to hack poorly secured IoT devices on the Indo-China border. Additionally, China is continuing to invest and grow in the field of quantum computing – this is only going to increase in the coming years, which is a great concern for the security value of encryption moving forward.

Furthermore, China's AI Plan for 2030 highlights the government's plan to become a leader in AI, which they believe is vital to their military and economic position in the world. The Chinese government could easily take advantage of their continued work in this field and utilize it to directly harm U.S. interests. Notably, there are serious questions regarding the influence of the Chinese government in global standards-setting bodies related to information and communications technology. The unchecked influence of our adversaries in global standards-setting bodies would disrupt the security of supply chains for decades to come. Moreover, there are many unanswered questions regarding Federal government's role in regulating these technologies to promote strong security.

I appreciate Chairwoman Clarke for holding this hearing today because it gives us an opportunity to understand the challenges emerging technologies present, how the private sector is proactively preparing for those challenges, and the right role for the Federal government. We must prepare ourselves to harness the security benefits and economic opportunities that emerging technologies like AI, IoT, and quantum computing will yield, while defending ourselves against adversaries who would use technology against us. But the government cannot do it alone.

Achieving our national and economic security goals will depend on whether the Federal government can partner with the private sector, as well as state and local partners, to develop policies that will enhance investment in emerging technology while also managing the risks associated with these technologies. I am eager to hear from our witnesses how the Federal government can ensure both the responsible deployment of emerging technologies, as well as managing security risks.

# # #

Media contact: Adam Comis at (202) 225-9978