COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

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

Preparing for the Future: An Assessment of Emerging Cyber Threats

October 22, 2019

I'd like to thank Chairman Richmond for holding today's hearing on emerging cyber threats. I have served on the Homeland Security Committee since its inception. Over that period of time, I have watched the tactics our adversaries use against us evolve and the threat landscape grow. As new networked devices and information technologies entered the market place, many became so mesmerized by their potential for good that we failed to appreciate and plan for the security consequences. Although I am encouraged that we are having more conversations about the nexus between technology and security today, there is still much to be done. So I commend Chairman Richmond for holding today's hearing. When this Committee was established a decade-and-a-half ago, we once focused our efforts on defending against physical attacks committed by terrorists who would readily claim responsibility. Now, we are faced with cyber threats from state and non-state actors who use cyber tools to carry out attacks in secret, blur attribution, and complicate our ability to impose consequences. As technology continues to evolve, so too will the tools of our adversaries.

Last December, DHS, DoD, the State Department, and the Office of the Director of National Intelligence identified Internet of Things (IoT) devices, Artificial Intelligence (AI), and quantum technologies as emerging, dual-use technologies that pose a threat to our national security. A month later, then-Director of National Intelligence Dan Coats warned that our "adversaries and strategic competitors will increasingly use cyber capabilities-including cyber espionage, attack, and influence-to seek political, economic, and military advantage over the United States and its allies and partners." Unfortunately, much of what DNI's warning about is in fact already happening.

We know that Russia has relied on its cyber capabilities to carry out influence campaigns designed to divide Americans and swing elections. Its efforts to manipulate Americans on social media platforms were wide-spread, but technologically simple. I worry about the influence campaign of the future, where Russia uses AI to create "deepfakes" that make it nearly impossible to discern fact from fiction. We know that China has engaged in intelligence- gathering and economic espionage, and has successfully breached OPM, navy contractors, and non-government entities from hotels to research institutions. We also know that China is investing heavily in developing quantum computing capabilities, which could undermine the security value of encryption within the next decade.

Over the past year, the Department of Justice has indicted two Iranians for their role in the ransomware attack against the City of Atlanta, and Microsoft recently revealed that Iran had attempted to breach a Presidential campaign. And according to the UN Security Council, North Korea has used its cyber capabilities to evade sanctions, stealing $670 million in various foreign and crypto-currencies between 2015 and 2018. The momentum Russia, China, Iran, and North Korea have demonstrated related to their use of cyber tools show no signs of slowing. We must prepare ourselves to harness the security, economic, and healthcare benefits of emerging technologies like AI and quantum computing will yield while defending ourselves against adversaries who would use technology against us. But the government cannot do it alone. The private sector is a critical partner in this effort. I am eager to hear from our witnesses how the Federal government can ensure the responsible deployment of emerging technologies.

# # #

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