COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

Hearing Statement of Cybersecurity, Infrastructure Protection, & Innovation Subcommittee Chairwoman Yvette Clarke (D-NY)

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

June 22, 2022

With each passing day, we see the pace of innovation accelerate exponentially. Advances in quantum computing, Artificial Intelligence (AI), 5G, and the Internet of Things present both opportunities and challenges in national security. As such, we must constantly reevaluate the threat landscape and adapt our defenses accordingly.

Today, we will explore how to harness the potential of these technologies while mitigating the security risks associated with them. In doing so, we will discuss how the Federal government and the private sector can better work together to anticipate future threats stemming from emerging technologies, inform international standards, and protect U.S. economic and national security interests.

Quantum computing, for example, is a transformative sophisticated computing system that can operate at higher speeds and process large amounts of data in shorter periods of time. The National Academy of Science predicts this technology could improve machine learning, sensor technology, electronic warfare capabilities, and communications, among other things. Our adversaries have also taken note of the potential that quantum computing presents.

China and other state actors are investing in quantum in pursuit of gaining a strategic advantage over the United States. We expect, for instance, that quantum computers will be able to break conventional encryption standards, which could expose sensitive information held by the U.S. government, military, and the private sector. As the global competition for quantum supremacy continues, the U.S. must not only work to innovate in this space but proactively mitigate against threats posed by adversaries.

For its part, the Biden Administration has provided much-needed White House leadership on the United States' quantum technology strategy. Last month, President Biden signed an Executive Order and a National Security Memorandum to preserve the United States' position as the global leader in quantum computing. Together, these documents chart a course for public-private collaboration in the following key areas: developing and deploying quantum-resistant encryption on Federal networks, educating non-Federal entities about risks to encryption from quantum computing, and promoting U.S. supremacy in this space.

Turning to AI, there is broad agreement that it has security applications that could enable network defenders to automate threat detection and prioritize response, spot irregular network activity, and better detect new malware. At the same time, there is concern that hackers will be able to exploit vulnerabilities in AI for nefarious purposes. We have already seen advances in AI fostering conditions for the growing spread of deepfakes, which is a class of synthetic media that appears to be authentic.

As deepfake technology becomes more sophisticated, experts anticipate that it will be used to further sow political tensions, disrupt public confidence in election outcomes, violate human rights, and facilitate criminal activity. That is why I have introduced the *DEEPFAKES Accountability Act* to implement criminal and civil penalties for malicious deepfakes. My legislation also directs DHS to establish a task force to better prepare for the national security implications of deepfakes. Emerging technologies carry with them national security implications and should be developed in a manner that protects national security.

This hearing comes at a critical time, as the House and Senate are engaged in a conference committee on the *America COMPETES Act*, which passed the House earlier this year. We have a historic opportunity to preserve the United States' place as a global leader in emerging technologies and chart a course for further advancements well into the future. As we close in on this urgent need, it is incumbent upon us to make sure that economic security and national security are part and parcel of how we support innovation.

# # #

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