Statement of LTG H.R. McMaster (U.S. Army, retired)
Senior Fellow, Hoover Institution, Stanford University

Before The House Committee on Homeland Security's
Subcommittee on Cybersecurity and Infrastructure Protection
Silicon Valley

Field Hearing on "Innovation Nation: Leveraging Technology to Secure Cyberspace and Streamline Compliance"

28 May 2025, 2:00pm PDT

This committee's work to understand U.S. cybersecurity posture and develop solutions to improve critical infrastructure resilience, foster technological innovation, and harmonize regulations is vitally important. And this panel's focus on how the United States can raise the cost of cyberattacks and strengthen deterrence is timely because, in recent years, responses to adversary state attacks have been slow and inadequate.

In 2017 during President Trump's first term, his national security team prioritized the competitive domains of cyberspace and space as part of his integrated national security strategy. Emphasis was on protecting critical infrastructure as well as data, sensitive technology, and intellectual property. We were particularly concerned about the security of what we labeled the National Security Innovation Base (NSIB), defined as the network of knowledge, capabilities, and people, including academia, National Laboratories, and the private sector, that turns ideas into innovations, transforms discoveries into successful commercial products and companies, and protects and enhances the American way of life. The NSIB develops technologies (such as those associated with fifth-generation communications (5G), artificial intelligence, quantum computing, and biogenetics) that are vital to maintaining America's advantages in defense and in the global economy.

Since 2017, despite efforts to improve the security of the NSIB and protect critical infrastructure, data, and technology, the threat in cyberspace has grown due to AI advancements and the increased connectivity of physical objects to cyberspace. To reduce the threat from malicious cyber actors, the United States and its allies must enhance both offensive and defensive cyber capabilities. We must also improve system and infrastructure resilience through cooperation across government, businesses, and academia. And, consistent with the premise of this hearing, it is vital to integrate all elements of national power and efforts of likeminded partners to impose high costs on nation states and non-state actors that attack or threaten our nation through cyber espionage or attacks.

AI technologies are making cyber-attacks easier as more of the physical world becomes connected to cyberspace and the malicious actors who operate within it. AI technologies can defeat encryption and allow systems to perform tasks usually reserved for humans such as hacking through firewalls. Combined with communications networks such as 5G, supercomputers (and eventually quantum computing), and the "internet of things" (i.e., the internet of computing devices embedded in everyday objects), an AI-enabled cyberattack could affect everything from power grids to public transportation to financial transactions to global logistics to driverless cars to home appliances. As the Volt Typhoon discovery revealed, People's Republic of China (PRC) cyber actors are already on IT networks and possess the capability to conduct disruptive or destructive cyberattacks against U.S. critical infrastructure.

Deterrence by denial requires a combination of offensive and defensive capabilities, resilient systems, and a high degree of cooperation across government, businesses, and academia. Unfortunately, such cooperation is a challenge in our decentralized, democratic systems. During

the first year of the Trump 45 administration, our NSC staff worked to remove bureaucratic impediments to timely identification and response to cyber threats. I was frustrated with the slow progress, but new authorities combined with General Paul Nakasone's superb leadership of NSA and U.S. Cyber Command improved our responsiveness. But there is much more that we can do to foster cooperation across the public and private sectors.

Deterrence by denial and effective response to cyber-attacks also requires actions against hostile cyber actors that extend beyond the cyber domain. Those include sanctions and financial actions, but they are often inadequate. It is sometimes difficult to hold something of value to an adversary or an enemy at risk. Elusive terrorist and criminal organizations hide their leadership and other important assets. And as hostile regimes like Iran and North Korea come under increased international and internal pressure, their leaders may conclude that they have little to lose. A physical military response may be appropriate and necessary against actors that prove difficult to deter. And it is important to convince difficult-to-deter adversaries that they cannot accomplish their objectives through a cyber-attack because our defenses are strong and we can recover rapidly.

The threat to infrastructure critical to U.S. security extends far beyond the shores of North America. The CCP's ambition is to control physical as well as digital infrastructure to achieve dominance of global logistics and supply chains. The vanguard of this twenty-first-century conquest is China's state-owned and state-sponsored enterprises, including telecommunications, port, and shipping companies. Democratic, free-market economies continue to furnish the CCP with "rope" as China has set about acquiring a global maritime infrastructure that complements its control of communications infrastructure. China has targeted EU countries and other U.S. allies such as Israel for control of ports. And many of these ports under Chinese control, such as Antwerp, Trieste, Marseille, and Haifa, are located near clusters of scientific and industrial research facilities. By 2020, according to China's Ministry of Transport, fifty-two ports in thirty-four countries were managed or constructed by Chinese companies, and that number was growing.[1] That is why it will be important to share this committee's work with allies and partners and urge the Trump administration to coordinate a multinational response to these threats as well as common standards for how their governments interact with the private sector and with one another when it comes to how data is managed and how it is collected, processed, stored, and shared.

Strong defense and rapid recovery require common understanding and increased cooperation across the public and private sectors. Organizations like the Cyber Policy Center here at Stanford play a vital role in fostering common understanding. The Defense Innovation Unit and the Cybersecurity and Infrastructure Security Agency (CISA) are examples of how to

[1] Yaakov Lappin, "Chinese Company Set to Manage Haifa's Port, Testing U.S.-Israeli Alliance," *South Florida Sun Sentinel*, January 29, 2019, https://www.sun-sentinel.com/florida-jewish-journal/fl-jj-chinese-company-set-manage-haifa-port-20190206-story.html.

structure such collaboration. Additionally, technology companies must be aware of the geopolitical implications of their innovations, avoiding complicity in aiding authoritarian regimes. Collaboration among scientists and between scientists and policy makers is vital for innovation. Here at the Hoover Institution we have been fostering common understanding and cooperation to counter threats through seminars under the Tech Track II Dialogue and sustained assessments of critical technologies under the Stanford Emerging Technology Review. The need for collaboration on crucial challenges to national security is growing because technology-based innovation is shifting away from governments and toward the private sector. To take full advantage of opportunities and protect against dangers in space and cyberspace requires an understanding of how technologies interact with one another and humanity. That is the premise of the Stanford Institute for Human-Centered Artificial Intelligence.

Private-sector companies that specialize in cybersecurity and countering cyber espionage hold promise to bridge the divide between the tech sector and government. It is important for engineers at tech firms to know how adversaries use cyberspace and emerging technologies and to be aware that their firms are competing against not only other companies, but also hostile nations. The ability of companies, universities, and research organizations to contract capabilities in cyber-defense, counterintelligence, and data recovery is growing. Private sector efforts that overlap with those of governments could lead to better civil-military coordination and cyber defense burden sharing. The line between government and private sector intelligence and security is blurring. Government would benefit from contracting cutting-edge commercial capabilities. And it is likely that some private-sector companies will conclude that they need to be active on adversary networks to detect and preempt attacks on their systems, data, or intellectual property. Because companies that go offensive in cyberspace risk incurring foreign government penalties, assuming liability for harm inflicted on innocent third parties, and sparking an escalation to armed conflict, public-and private-sector coordination is essential for integrating offense and defense in cyberspace.

A counterintuitive but key defensive action is, in addition to having a plan to recover rapidly from attack, to design cyber networks and systems for graceful degradation under the assumption that they will be attacked relentlessly. Exquisite systems based on the latest technology may be prone to catastrophic failure. Resiliency must be a critical design parameter not only for weapon systems, but also for communications, energy, transportation, and financial infrastructure. Resiliency requires keeping suspect hardware and software off networks and continuously identifying and, when appropriate, preempting enemy attacks. We must recognize that allowing hardware from companies such as China's Huawei or ZTE into our communications networks is tantamount to opening Troy's gates to the mythical Trojan horse. Purchasing other hardware from Chinese companies is also irresponsible as we have discovered with cranes and solar panels. Vigilance must be habitual and integrated into company and governmental operational culture. And vigilance must be comprehensive across a company's OT, IT, hardware, and supply chains. Third party risk is particularly difficult to manage.

Every company that develops sensitive technology or holds critical data should treat that technology and data like gold and strive to make their company or research organization "Fort Knox." Prior to the end of the Cold War, the U.S. model of technological development was relatively closed, meaning that the government funded and controlled access to major initiatives such as nuclear weapons, jet fighters, and precision-guided munitions. These programs were protected by security classifications, patents, and copyrights. When the government decided to declassify technologies such as microchips, touch screens, and voice-activated systems, private-sector engineers and entrepreneurs combined and refined those technologies to kick-start new industries such as the smartphone. In the twenty-first century, technological innovation truly opened up. Innovations increasingly derive from diffuse publicly financed research. Meanwhile, China has implemented its top-down military-civilian fusion strategy to steal technology and direct investments with the intention of surpassing the United States in strategic emerging industries (SEIs) and military capabilities.

For too long much of academia, the private sector, and the government were oblivious to how adversaries can steal and apply technologies developed in the United States to threaten security and undermine human rights. Congress should prohibit U.S. capital from accelerating the CCP's efforts to surpass the United States in a range of critical emerging technologies, such as quantum computing and AI-related technologies, important to achieving military superiority. Seven hundred Chinese companies, the majority of which are state-owned or -controlled, are traded in the U.S. debt and equity markets. U.S. citizens still fund companies that are building the next generation of the PLA's military aircraft, ships, submarines, unmanned systems, and airborne weapons. Until recently U.S. venture capital investment in Chinese AI companies exceeded investment in U.S. companies. Many U.S. and allied executives and financiers go beyond the quotation attributed to Vladimir Lenin that "The capitalists will sell us the rope with which to hang them." They are financing CCP's acquisition of the rope. The easiest first step in strengthening deterrence might be to stop underwriting our demise.