

STATEMENT OF
MR. AARON HUGHES
DEPUTY ASSISTANT SECRETARY OF DEFENSE
FOR CYBER POLICY
OFFICE OF THE SECRETARY OF DEFENSE
BEFORE THE
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
INFORMATION TECHNOLOGY AND NATIONAL SECURITY SUBCOMMITTEES
JULY 13, 2016

INTRODUCTION

Chairmen Hurd and DeSantis, Ranking Members Kelly and Lynch, and Members of the Subcommittees, thank you for inviting me to discuss the Department of Defense's (DoD) strategy as it relates to cyberspace and how that applies to cyberattacks. It is an honor to appear before you today, and I appreciate the opportunity to explain the progress the Department is making to improve America's cybersecurity posture.

I plan to focus my testimony on the Department's strategy and missions in cyberspace, including through deterrence, and the threats and challenges posed by State and non-state actors. Improving our collective cyber defenses is a whole-of-government and whole-of-nation endeavor that also requires close cooperation with our allies, partners, and the private sector.

DOD STRATEGY AND MISSIONS

Recognizing that DoD relies heavily on cyberspace for virtually everything we do, the Department's Cyber Strategy guides our efforts in cyberspace. The Strategy directs the Department to focus its efforts on three primary missions in cyberspace: (1) defend DoD information networks to ensure DoD mission effectiveness, (2) defend the United States against cyberattacks of significant consequence, and (3) provide full-spectrum cyber options to support contingency plans and military operations.

One of the Department's key policy goals in cyberspace is to deter cyberattacks. Incidents described as "cyberattacks" or "computer network attacks" are not necessarily "armed attacks" for the purposes of triggering a nation-state's inherent right of self-defense (as recognized in Article 51 of the United Nations Charter). In that vein, when determining whether a cyber incident constitutes an armed attack, the U.S. Government considers a number of factors including the nature and extent of injury or death to persons and the destruction of, or damage to, property. As such, cyber incidents are assessed on a case-by-case basis and, as the President has publicly stated, the U.S. Government's response to any particular cyber incident would come "in a place and time and manner that we choose."

DoD is supporting a comprehensive, whole-of-government cyber deterrence strategy to deter cyberattacks against U.S. interests. This strategy depends on the totality of U.S. actions, including its declaratory policy, overall defensive posture, effective response procedures, indications and warning capabilities, and the resiliency of U.S. networks and systems.

Fundamentally, deterrence is largely a function of perception, and DoD has three specific roles to play within a whole-of-government deterrence strategy. First, we seek to deny the adversary the ability to achieve the objectives of a cyberattack, so our adversary will believe any attack will be futile. We do this through strengthening our cyber defenses and reducing our attack surface. Second, we want to improve our resilience so our adversary will perceive that, even if any single attack is successful, we can reconstitute quickly so that their ultimate objective will not be achieved. The Department is already training to operate in a "cyber contested environment," to demonstrate that we can continue our mission even while under cyberattack. Lastly, for deterrence to be effective, the adversaries must believe that our ability to respond to an attack will result in unacceptable costs imposed on them. Costs may be imposed through a variety of mechanisms, including economic sanctions, diplomacy, law enforcement, and military action. Our task at the Department is to plan and prepare to conduct military operations, including through cyberspace, to impose costs on the adversary.

THE CYBER LANDSCAPE

We continue to face a diverse and persistent set of threats from State and non-state actors who probe and scan DoD networks for vulnerabilities. Although the United States has benefited greatly from the increasingly wired and interconnected global landscape, cyber threats are evolving, posing greater risks to the networks and systems of the Department of Defense and other Federal departments and agencies, our national critical infrastructure, and U.S. companies and interests.

In the last few years, there have been numerous high-profile malicious cyber or cyber-enabled events that have captured the public's attention, including incidents that have affected Sony Pictures Entertainment, the U.S. Office of Personnel Management (OPM), the Department of Defense unclassified Joint Staff network, and the Ukrainian power grid. If malicious cyber actors gain access to DoD networks, they can potentially manipulate information or software, destroy data, and impair the functioning of systems that computers control. Although DoD maintains and uses robust and unique cyber capabilities to defend our networks, often these measures alone are not sufficient. Securing systems and networks is everyone's responsibility – from the commander down to the individual network user and across the Federal Government – and requires a culture of cybersecurity.

Criminal activity in cyberspace is a significant and growing problem, but nations in many ways still represent the gravest threats because of the skill and resources they can bring to bear. The States that we watch most closely in cyberspace remain Russia, China, Iran, and North Korea. Russia and China have developed advanced cyber capabilities and strategies, and Russian actors in particular are stealthy in their cyber tradecraft, and their intentions are sometimes difficult to discern. In September 2015, the U.S. and China agreed to neither conduct nor knowingly support the cyber-enabled theft of intellectual property for commercial gain; we continue to monitor China's compliance. Iran and North Korea have demonstrated the capability and willingness to conduct damaging and destructive cyber-attacks against the United States in support of their policy objectives. Finally, the Islamic State of Iraq and the Levant (ISIL) represents a serious and complex threat, and continues to use the Internet to intimidate its enemies, recruit fighters, incite violence, and inspire attacks. As part of the efforts of the 66-member Global Coalition to counter ISIL, the Department is providing integrated cyber capabilities and support to Operation INHERENT RESOLVE.

At DoD, protecting the territory and people of the United States remains our highest priority, and we remain vigilant, and devote substantial resources and effort preparing for threats that could be directed against the U.S. homeland, and infrastructure that the Department relies on to operate during a contingency.

INTERNATIONAL COOPERATION

In line with the President's 2011 *United States International Strategy for Cyberspace*, the Department works with foreign partners bilaterally and multilaterally – through NATO, for example – to advance cyberspace cooperation to defend U.S., allied, and partner interests. Our international partners bring varying capabilities and expertise, but the Department prioritizes international cyberspace partnerships to enhance cyber defense and to build greater collective security. Cooperation in cyberspace increases our capacity to detect, monitor, prevent, and defeat threats in cyberspace while working to ensure that our allies and international partners develop and build strong cyber defense capabilities.

Beyond the Department's engagements with the international community, DoD supports the Department of State's diplomatic efforts to promote a framework for stability in cyberspace that includes affirmation of the applicability of international law to state conduct in cyberspace,

the identification of voluntary peacetime norms of state behavior in cyberspace, and the promotion of cyber confidence-building measures. In particular, as voluntary measures of self-restraint, the Department believes peacetime norms can contribute to conflict prevention and stability.

CONCLUSION

The Department is committed to the security and resiliency of our networks and to defending the U.S. homeland and interests from cyberattacks of significant consequence. We have undertaken comprehensive efforts, both unilaterally and in concert with our allies and partners, and the private sector to improve our Nation's cybersecurity posture and to ensure that DoD has the ability to operate in any environment at any time. Our relationship with Congress is absolutely critical to everything the Department is doing in cyberspace. To that end, I am grateful for the Committee's interest in these issues, and I look forward to your questions.