Testimony of Christopher M. E. Painter, Coordinator for Cyber Issues
U.S. Department of State
Before the House of Representatives Committee on Oversight and Government Reform
Subcommittees on Information Security and National Security

Hearing on "Digital Acts of War: Evolving the Cybersecurity Conversation"

July 13, 2016

Chairmen Hurd and DeSantis, Ranking Members Kelly and Lynch, members of the Subcommittee on Information Technology and the Subcommittee on National Security, thank you for the opportunity to speak to you today on this very timely subject.

Over the last few decades, the Internet and information and communications technologies (ICTs) more broadly have brought profound benefits to the United States and the rest of the world – enabling innovation, connecting people to information and services, and providing a new forum for people to express their views and to dissent. Given all of these benefits as well as our growing dependence on technology, it is not surprising that governments as well as certain non-state actors have increasingly come to view cyberspace as a place where they too can pursue their objectives. A number of militaries around the world – including our own – have publicly stated their intention to operate in cyberspace, while still more are actively developing their cyber capabilities. Reports of cyber incidents potentially linked to state-sponsored activity have become a regular feature of the public conversation on cybersecurity issues.

Although there is no question that we face new challenges, our goal remains what was articulated in the President's 2011 U.S. *International Strategy for Cyberspace*: "to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation." We must work every day to ensure that even as the number and variety of online threats grow and evolve, the Internet remains a place where people can do business, connect with friends, and express their views. We need to ensure that the Internet remains a greater source of stability than it is a source of instability and that governments and other actors behave responsibly as they conduct their activities in cyberspace. In short, we need a framework for international stability in cyberspace.

During my time today, I will discuss the framework for stability in cyberspace that the U.S. government and the State Department in particular are working to promote internationally and some of our recent successes in that regard. Much of what I will address on this topic is also covered by the *Department of State International Cyberspace Policy Strategy* that was submitted in April as required by the Consolidated Appropriations Act for 2016 (Public Law 114-113). I will also discuss some of the other topics raised in your invitation, including when an incident in cyberspace might rise to level of an armed attack and how the U.S. government thinks about the proper response to individual cyber incidents, including through public attribution.

Building a Framework for International Stability in Cyberspace

The Department of State, working with our interagency partners, is guided by the vision of the President's *International Strategy for Cyberspace*, which is to promote a strategic framework of international cyber stability designed to achieve and maintain a peaceful cyberspace environment where all states are able to fully realize its benefits, where there are advantages to cooperating against common threats and avoiding conflict, and where there is little incentive for states to engage in disruptive behavior or to attack one another.

This framework has three key elements: (1) global affirmation that international law applies to state behavior in cyberspace; (2) development of an international consensus on and promotion of additional voluntary norms of responsible state behavior in cyberspace that apply during peacetime; and (3) development and implementation of practical confidence-building measures (CBMs) among states, which promote stability in cyberspace by reducing the risks of misperception and escalation.

Since 2009, the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) has served as a productive and groundbreaking expert-level venue for the United States to build support for this framework. The consensus recommendations of the three UN GGE reports in 2010, 2013, and 2015 have set the standard for the international community on the applicability of international law in cyberspace, voluntary peacetime norms, and CBMs. The conclusions captured in these reports have in turn been endorsed by political leaders in a range of settings. When it reconvenes in August 2016, the UN GGE process will continue to play a central role in our efforts to promulgate this framework fully.

Applicability of international law. The first and most fundamental pillar of our framework for international cyber stability is the applicability of existing international law to state behavior in cyberspace. The 2013 UN GGE report was a significant achievement that affirmed the applicability of existing international law, including the UN Charter, to state conduct in cyberspace. The 2013 report underscored that states must act in cyberspace under the established international obligations and commitments that have guided their actions for decades – in peacetime and during conflict – and that states must meet their international obligations regarding internationally wrongful acts attributable to them. The 2014-2015 UN GGE also made progress on issues related to international law by highlighting that the UN Charter applies in its entirety, affirming the applicability of the inherent right of self-defense as recognized in Article 51 of the UN Charter, and noting the law of armed conflict's fundamental principles of humanity, necessity, proportionality, and distinction.

Norms of responsible state behavior. The United States is also building consensus on a set of additional, voluntary norms of responsible state behavior in cyberspace that define key areas of risk that would be of national and/or economic security concern to all states and that should be off-limits during times of peace. If observed, these stability measures – which are measures of self-restraint – can contribute substantially to conflict prevention and stability. The United States was the first state to propose a set of specific peacetime cyber norms. Those norms are as follows:

- A state should not conduct or knowingly support online activity that intentionally damages critical infrastructure or otherwise impairs the use of critical infrastructure to provide services to the public.

- A state should not conduct or knowingly support activity intended to prevent national computer security incident response teams (CSIRTs) from responding to cyber incidents. A State should also not use CSIRTs to enable online activity that is intended to do harm.

- A state should cooperate, in a manner consistent with its domestic law and international obligations, with requests for assistance from other states in investigating cybercrimes, collecting electronic evidence, and mitigating malicious cyber activity emanating from its territory.

- A state should not conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to its companies or commercial sectors.

In May 2015, Secretary of State Kerry highlighted these norms in his speech in Seoul, South Korea, on an open and secure Internet. The 2015 UN GGE report's most significant achievement was its recommendation for voluntary norms of state behavior designed for peacetime, which included concepts championed by the United States.

Confidence-building measures. Together with our work on international law and voluntary norms, cyber CBMs have the potential to contribute substantially to international cyber stability. CBMs have been used by governments for decades to build confidence, reduce risk, and increase transparency in other areas of international concern. Examples of cyber CBMs include: transparency measures, such as sharing national strategies or doctrine; cooperative measures, such as building points of contact networks to respond rapidly to cyber incidents; and stability measures, such as committing to refrain from a certain activity of concern. Cyber CBMs are being developed, and are in the first stages of implementation, in two regional venues – the Organization for Security and Cooperation in Europe (OSCE) and the ASEAN Regional Forum where agreement was reached in 2015 on a detailed work plan with a proposed set of CBMs for future implementation.

Although many of the elements of the framework I have described above may seem self-evident to a U.S. audience, it is important to recognize that cyber issues are new to many states and, as I am happy to discuss during the question and answer period, there are also states that hold alternative views on how to promote cyber stability. Notwithstanding these headwinds, as well as the fact that diplomatic negotiations on other issues can take many years, if not decades, the United States and its allies and partners have made substantial progress in recent years towards advancing our strategic framework of international cyber stability.

In addition to the GGE reports, I would like to briefly highlight a few examples from the last year that reflect our progress in achieving broader adoption of the framework.

- First, in September 2015, during President Xi Jinping's state visit, the United States and China made several key commitments on cyber issues. These include a commitment that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property for commercial advantage, as well as a statement welcoming the 2015 GGE report.

- Second, last November, the leaders of the G20, meeting in Antalya, Turkey, strongly endorsed the U.S. approach to promoting stability in cyberspace. The leaders' communique affirmed that states should not conduct or support the cyber-enabled theft of intellectual property for commercial advantage. The communique also highlighted the 2015 UN GGE report I discussed; affirmed that international law, and in particular the UN Charter, applies to state conduct in cyberspace; and endorsed the view that all states should abide by norms of responsible state behavior in cyberspace.

- Finally, although it received less publicity than the previous two developments, the 57 member states of the OSCE, which includes not only the United States and its Western allies and partners but also Russia and other former Soviet states, reached consensus in March 2016 on an expanded set of CBMs. This expanded set, which includes five new cooperative CBMs, focusing on issues like cybersecurity of critical infrastructure and developing public-private partnerships as well as mechanisms for the exchange of best practices, builds upon the existing 11 CBMs announced in 2013 that focus on building transparency and putting in place mechanisms for de-escalating conflict.

On the Concept of a "Digital Act of War"

Given the title of this hearing, "Digital Acts of War," I would like to discuss how the U.S. government thinks about these issues, which, consistent with its broader approach to promoting stability in cyberspace, is through the prism of existing international law.

As an initial matter, the United States has been clear that it believes that cyber activities may in certain circumstances constitute an armed attack that triggers our inherent right of self-defense, as recognized in Article 51 of the UN Charter.

The United States has described publicly how it would evaluate whether a cyber activity constitutes an armed attack under international law. Of primary importance to such a determination are the actual or anticipated effects of a particular incident. When determining whether a cyber activity constitutes an armed attack sufficient to trigger a state's inherent right of self-defense, the U.S. government believes that states should consider the nature and extent of injury or death to persons and the destruction of, or damage to, property. Although this is necessarily a case-by-case, fact-specific inquiry, in general, cyber activities that proximately result in death, injury, or significant destruction, or represent an imminent threat thereof, likely would be viewed as an armed attack.

It is worth emphasizing that a determination whether specific events constitute an actual or imminent armed attack sufficient to trigger a state's inherent right of self-defense is necessarily a case-by-case, fact-specific inquiry. This is the case whether the events occur in cyberspace or elsewhere. As a general matter, states have not sought to define precisely (or state conclusively) what situations would constitute armed attacks in other domains, and there is no reason cyberspace should be different. In fact, there is a good reason not to articulate a bright line, as strategic ambiguity could very well deter most states from getting close to it.

Responding to Cyber Incidents

Finally, I would hasten to note that the U.S. government uses a whole-of-government approach to responding to and deterring malicious activities in cyberspace. This approach brings to bear its full range of instruments of national power and corresponding policy tools – diplomatic, law enforcement, economic, military, and intelligence – as appropriate and consistent with applicable law. This means that regardless of whether a particular incident rises to the level of an armed attack, the President has a range of options for responding.

As suggested in the invitation for this hearing, public attribution is one such option. In cases where the actors responsible for a particular incident have been determined, the U.S. government will consider whether to identify those actors publicly when we believe it will further our national interests, including our ability to hold the actors accountable. North Korea's 2014 cyber attack against Sony Pictures Entertainment, for example, which rendered thousands of computers inoperable and was intended to interfere with the exercise of freedom of expression and inflict significant harm on a U.S. business, represented behavior in cyberspace that is simply unacceptable. This, in combination with the strength of the evidence linking North Korea to the cyber attack, contributed to the U.S. government's decision to make a public attribution in that case. However, the U.S. government also maintains the flexibility to avail itself of the other options that I have mentioned as appropriate.

* * *

In closing, I would like to express my appreciation for both Subcommittees' interest in these important topics. I look forward to addressing your questions.

Christopher Painter

Coordinator for Cyber Issues
Term of Appointment: 02/22/2011 to present

Mr. Painter has been on the vanguard of cyber issues for over twenty five years. In his current role as the Secretary's first Coordinator for Cyber Issues, Mr. Painter coordinates and leads the United States' diplomatic efforts to advance an open, interoperable, secure and reliable Internet and information infrastructure. He works closely with components across the Department, other agencies, the White House, the private sector and civil society to implement the President's International Strategy for Cyberspace and ensures that U.S. foreign policy positions on cross-cutting cyber issues are fully synchronized. These issues include promoting norms of responsible state behavior and cyber stability, advancing cybersecurity, fighting cybercrime, promoting multi-stakeholder Internet governance and advancing Internet freedom.

Mr. Painter and his team have launched "whole of government" cyber dialogues with numerous countries, designed and carried out regional capacity building initiatives, worked to reduce cyber threats worldwide by combatting operational threats such as Distributed Denial of Service and large-scale cyber intrusions for the purposes of stealing intellectual property and proprietary business information, worked to ensure that fundamental freedoms can be exercised online, and worked diplomatically to build a consensus around our vision of an open, interoperable, secure and reliable cyberspace. He and his team have also spearheaded the promotion of an international framework of cyber stability that includes building a consensus around norms of acceptable behavior and getting agreement on transparency and confidence-building measures designed to reduce the risk of miscalculation that could inadvertently lead to conflict in cyberspace.

Prior to joining the State Department, Mr. Painter served in the White House as Senior Director for Cyber Policy and Acting Cyber Coordinator in the National Security Council. During his two years at the White House, Mr. Painter was a senior member of the team that conducted the President's Cyberspace Policy Review and coordinated the development of the President's 2011 International Strategy for Cyberspace.

Mr. Painter began his federal career as an Assistant U.S. Attorney in Los Angeles where he led some of the most high profile and significant cybercrime prosecutions in the country, including the prosecution of notorious computer hacker Kevin Mitnick. He subsequently helped lead the case and policy efforts of the Computer Crime and Intellectual Property Section in the U.S. Department of Justice and served, for a short time, as Deputy Assistant Director of the F.B.I.'s Cyber Division.

Mr. Painter is a recognized leader in international cyber issues. He has represented the United States in numerous international fora, including chairing the cutting edge G8 High Tech Crime Subgroup from 2002-2012. He has worked with dozens of foreign governments in bilateral meetings and has been a frequent spokesperson and presenter on cyber issues around the globe. He is a recipient of the prestigious RSA Award for Excellence in the Field of Public Policy (2016), the Attorney General's Award for Exceptional Service, the Intelligence Community Legal Award (2008) and has been named to the "Federal 100" list, among other honors. Mr. Painter is a graduate of Stanford Law School and Cornell University.