Testimony of Christopher M. E. Painter, Coordinator for Cyber Issues
U.S. Department of State
Before the Senate Foreign Relations Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy

Hearing on "International Cybersecurity Strategy: Deterring Foreign Threats and Building Global Cyber Norms"

May 25, 2016

Chairman Gardner, Ranking Member Cardin, members of the Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy, it is a pleasure to appear again before your Subcommittee to provide an update on key developments in our cyber foreign policy efforts.

Since I testified before your Subcommittee one year ago, the Department of State (the Department) has continued to work closely with other Federal departments and agencies and has made significant progress in a number of areas.

It is also important to note that last month, as required by the Consolidated Appropriations Act for 2016, the Department submitted to Congress the *Department of State International Cyberspace Policy Strategy* (the Strategy) that included a report on the Department's work to implement the President's 2011 *International Strategy for Cyberspace*, as well as a discussion of our efforts to promote norms of responsible state behavior in cyberspace, alternative concepts for norms promoted by certain other countries, threats facing the United States, tools available to the President to deter malicious actors, and resources required to build international norms. I appreciate the opportunity today to provide an update on our progress as well as the challenges we face in a number of areas.

As reflected in the Strategy we provided to Congress last month, the Department of State structures its cyberspace diplomacy in close cooperation with our interagency partners – including the Departments of Justice, Commerce, Defense, Homeland Security, and Treasury, and the Intelligence Community – around the following interrelated, dynamic, and cross-cutting policy pillars drawn from the President's *International Strategy for Cyberspace*: digital economy; international security; promoting cybersecurity due diligence; combating cybercrime; Internet governance; Internet freedom; and international development and capacity building, as well as cross-cutting issues such as countering the use of the Internet for terrorist purposes. In addition, as we noted, the Department actively is mainstreaming cyberspace issues into its foreign diplomatic engagements and building the necessary internal capacity.

I am happy to answer any questions regarding the Strategy, which discusses all of these policy priorities in greater detail, including specific accomplishments from our robust bilateral and multilateral diplomatic engagements and highlights from the roles and contributions of other Federal agencies.

In spite of the successes outlined in the Strategy, the U.S. vision for an open, interoperable, secure, and reliable Internet faces a range of policy and technical challenges. Many of these challenges were described in my testimony last year, and they largely remain. I would like to focus my time today delving specifically into our efforts to promote a broad international framework for cyber stability, as well some of the alternative views regarding the Internet that some governments are promoting. I will also spend some time discussing the technical challenges and threats posed by continuing malicious cyber activity directed at the United States, as well as our allies, and the tools we have at our disposal to deter these actions.

Diplomatic Efforts to Shape the Policy Environment

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), 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 international cyberspace norms and CBMs. The UN GGE process will continue to play a central role in our efforts to fully promulgate this framework when it reconvenes in August 2016.

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 landmark 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 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 affirming the applicability of the inherent right to 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 which 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, including the cybersecurity of critical infrastructure, the protection of computer security incident response teams (CSIRTs), and cooperation between states in responding to appropriate requests in mitigating malicious cyber activity emanating from their territory. 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 law and voluntary norms, cyber CBMs have the potential to contribute substantially to international cyber stability. CBMs have been used 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 an initiative to combat a particular cyber incident or threat actor; 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 an American audience, it is important to recognize that cyber issues are new to many states, and as I describe later in my testimony, there are also many states that hold alternative views on how we should 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 have made substantial progress in recent years towards advancing our strategic framework of international cyber stability. At this point, I would like to highlight examples from last year that reflect our progress.

U.S.-China Cyber Commitments

The United States strongly opposes the use of cyber technology to steal intellectual property for commercial advantage, and has raised this concern with Chinese interlocutors for several years. In 2014, the U.S. indicted five members of the Chinese military for hacking, economic espionage, and other offenses directed at six U.S. entities. This led China to suspend the U.S.-China Cyber Working Group. The U.S. and China, however, reached agreement during President Xi Jinping's state visit in September 2015 on several key commitments on cyber issues. These commitments are:

(1) both governments agreed to cooperate and provide timely responses to requests for information and assistance regarding malicious cyber activity emanating from their territories;
(2) neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property for commercial advantage;
(3) both governments will work together to further identify and promote appropriate norms of state behavior in cyberspace and hold a senior experts group on international security issues in cyberspace; and
(4) both governments will establish a Ministerial-level joint dialogue mechanism on fighting cybercrime and related issues.

Two weeks ago today – on May 11 – the United States hosted the first meeting of the senior experts group in Washington on international security issues in cyberspace, which provided a forum to further engage China on its views and seek common ground regarding norms of state behavior in cyberspace and other topics. The Department of State led the U.S. delegation that included participation from the Department of Defense and other U.S. government agencies. The senior experts group helps us advance the growing international consensus on international law and voluntary cyber norms of state behavior. We also have encouraged China to join us in pushing for other states to affirm these principles in international forums like the Group of Twenty (G20), and will continue to do so.

To implement other commitments reached during President Xi's visit, the United States and China held the first ministerial level dialogue on cybercrime and other related issues in Washington on December 1, 2015. Attorney General Loretta Lynch and Homeland Security Secretary Jeh Johnson, together with Chinese State Councilor Guo Shengkun, co-chaired the first U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues to foster mutual understanding and enhance cooperation on law enforcement and network protection issues. The second dialogue is scheduled to occur next month in Beijing, China.

Moreover, regarding the commitment that neither government will conduct or knowingly support cyber-enabled theft for commercial gain, Deputy Secretary of State Blinken testified last month before the full Committee on Foreign Relations that the United States is "watching very closely to ensure this commitment is followed by action."

The outcomes of last year's Xi-Obama summit focus on concrete actions and arrangements that will allow us to hold Beijing accountable to the commitments they have made. These commitments do not resolve all our challenges with China on cyber issues. However, they do represent a step forward in our efforts to address one of the sharpest areas of disagreement in the U.S.-China bilateral relationship.

Group of Twenty (G20) Antalya Summit

In November 2015, the leaders of the G20 met in Antalya, Turkey, to discuss and make progress on a wide range of critical issues facing the global economy. At the conclusion of the Antalya Summit, the strong final communique issued by the G20 leaders affirmed the U.S.-championed vision of international cyber stability and its pillars.

Among other things, the G20 leaders affirmed in their statement that "no country should conduct or support the ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors." They also highlighted the "key role played by the United Nations in developing norms" and the work of the UN GGE and its 2015 report. Addressing our overall framework, the G20 leaders stated that they "affirm that international law, and in particular the UN Charter, is applicable to state conduct in the use of ICTs and commit ourselves to the view that all states should abide by norms of responsible state behavior in the use of ICTs… ."

The G20 leaders' communique represents a remarkable endorsement of our approach to promoting stability in cyberspace. But there is still more to do. The United States will continue to work within the G20 and in other bilateral and multilateral engagements to promote and expand these policy pronouncements regarding responsible state behavior in cyberspace.

Organization for Security and Cooperation in Europe

As a result of the leadership by the United States and like-minded countries, the 57 member states of the OSCE, which includes not only Western allies 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 CBMs, builds upon the 11 CBMs announced by the OSCE in 2013 that member states are already working to implement.

The initial 11 CBMs were primarily focused on building transparency and putting in place mechanisms for de-escalating conflict. For example, there were CBMs calling upon participating states to identify points of contact that foreign governments could reach out to in the event of a cyber incident emanating from the state's territory and put in place consultation and mediation mechanisms. The additional five CBMs focused more on cooperative measures focusing on issues like cybersecurity of critical infrastructure and developing public-private partnerships. Secure and resilient critical infrastructure, including in the communications sector, requires the integration of cyber, physical, and human elements. Since most critical infrastructure is privately owned, public-private partnerships are essential for strengthening critical infrastructure. Given the distributed nature of critical infrastructure, these efforts also require international collaboration. Work will continue this year to strengthen implementation of the previous CBMs and to begin implementing the new ones as well. This will build on the cooperation we have underway with many international partners in this and other similar fora. We also hope that this further success within the OSCE context can serve to strengthen CBMs as a model that other regional security organizations can adopt.

In addition to our work with governmental organizations, the Department of State engages extensively with a range of stakeholders outside of government, who play critical roles in helping to preserve and promote the same vision of cyberspace held by the United States. Non-government stakeholders are often part of our delegations to key meetings, for which there is intensive consultation, and we often engage with our stakeholders before and after key events to hear their views and to inform them of our activities. We also engage extensively with the stakeholder community ahead of and immediately following major cyber conferences, such as

the Global Conference on Cyberspace, most recently in The Hague, the Netherlands, and previously in Seoul, South Korea.

Policy Challenge: Alternative Views of the Internet

A challenge to the implementation of our cyberspace strategy is a competing and alternative view of the Internet. The United States and much of the broader international community support the open flow and movement of data on the Internet that drives economic growth, protects human rights, and promotes innovation. The United States believes in a multistakeholder approach whereby governments, private sector, civil society, and the technical and academic communities cooperate to address both technical and policy threats through inclusive, transparent, consensus-driven processes.

China's approach to cyberspace in the international context is propelled by its desire to maintain internal stability, maintain sovereignty over its domestic cyberspace, and combat what it argues is an emerging cyber arms race and 'militarization' of cyberspace. China has been willing to consider cyber confidence building measures, and has affirmed that international law applies in cyberspace, but has not been willing to affirm more specifically the applicability of the law of armed conflict or other laws of war, because it believes it would only serve to legitimize state use of cyber tools as weapons of war.

This has led to a set of external policies that reinforces traditional Chinese foreign policy priorities of non-interference in internal affairs, national sovereignty over cyberspace, and "no first use" of weapons. China views its expansive online censorship regime – including technologies such as the Great Firewall – as a necessary defense against destabilizing domestic and foreign influences, and it has promoted this conception internationally. China also urges creation of new "cyber governance" instruments, which would, *inter alia*, create new binding rules designed to limit the development, deployment, and use of "information weapons," promote speech and content controls, seek to replace the framework of the Council of Europe Convention on Cybercrime (Budapest Convention), elevate the role of governments vis-à-vis other stakeholders, and likely give the United Nations authority for determining attribution and responding to malicious cyber activity. While the United States and its partners seek to focus our cyber policy efforts on combatting threats to networks, cyber infrastructure, and other physical threats from cyber tools, China also emphasizes the threats posed by online content. In addition, some of these policies stand in sharp contrast to the U.S. view that all stakeholders should be able to contribute to the making of public policy regarding the Internet.

Russia's approach to cyberspace in the international context has focused on the maintenance of internal stability, as well as sovereignty over its "information space." While Russia co-authored the Code of Conduct, with China and other Shanghai Cooperation Organization members, Russia's ultimate goal is also a new international cyber convention, which they pair with criticism of the Budapest Convention.

Russia has nonetheless found common ground with the United States on our approach of promoting the applicability of international law to state conduct in cyberspace as well as voluntary, non-binding norms of state behavior in peacetime. Russia has also committed to the

first ever set of bilateral cyber confidence building measures with the United States, as well as the first ever set of cyber CBMs within a multilateral institution, at the OSCE in 2013 and 2016 that I previously discussed.

We counter these alternative concepts of cyberspace policy through a range of diplomatic tools that include not only engagement in multilateral venues, but also direct bilateral engagement and awareness-raising with a variety of state and non-state actors. I now would like to discuss some of the technical challenges and threats the U.S. faces and some of the tools we have to respond to and prevent cyber incidents.

Responding to and Preventing Cyber Incidents

Continuing Cyber Threats

Cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity. In 2015, high profile cyber incidents included the breach of health insurance company Anthem, Inc.'s IT system that resulted in the theft of account information for millions of customers; an unauthorized breach of the Office of Personnel Management's systems that resulted in the theft of approximately 22 million personnel files; and hackers launching an unprecedented attack on the Ukraine power grid that cut power to hundreds of thousands of customers.

Overall, the unclassified information and communications technology networks that support U.S. government, military, commercial, and social activities remain vulnerable to espionage and disruption. As the Department noted in the Strategy we submitted last month, however, the likelihood of a catastrophic attack against the United States from any particular actor is remote at this time. The Intelligence Community instead foresees an ongoing series of low-to-moderate level cyber operations from a variety of sources, which will impose cumulative costs on U.S. economic competitiveness and national security, pose risks to Federal and private sector infrastructure in the United States, infringe upon the rights of U.S. intellectual property holders, and violate the privacy of U.S. citizens.

In February, Director of National Intelligence James Clapper testified before Congress on the 2016 *Worldwide Threat Assessment of the US Intelligence Community*, and stated: "Many actors remain undeterred from conducting reconnaissance, espionage, and even attacks in cyberspace because of the relatively low costs of entry, the perceived payoff, and the lack of significant consequences." He highlighted the malicious cyber activities of the leading state actors, non-state actors such as Da'esh, and criminals who are developing and using sophisticated cyber tools, including ransomware for extortion and malware to target government networks.

The Intelligence Community continues to witness an increase in the scale and scope of reporting on malicious cyber activity that can be measured by the amount of corporate data stolen or deleted, personally identifiable information compromised, or remediation costs incurred by U.S. victims. The motivation to conduct cyber attacks and cyber espionage will probably remain strong because of the gains for the perpetrators.

Tools Available to Counter Cyber Threats

The United States works to counter technical challenges through a whole-of-government approach that 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.

The United States believes that deterrence in cyberspace is best accomplished through a combination of "deterrence by denial" – reducing the incentive of potential adversaries to use cyber capabilities against the United States by persuading them that the United States can deny their objectives – and "deterrence through cost imposition" – threatening or carrying out actions to inflict penalties and costs against adversaries that conduct malicious cyber activity against the United States. It is important to note that there is no one-size-fits-all approach to deterring or responding to cyber threats. Rather, the individual characteristics of a particular threat determine the tools that would most appropriately be used.

The President has at his disposal a number of tools to carry out deterrence by denial. These include a range of policies, regulations, and voluntary standards aimed at increasing the security and resiliency of U.S. government and private sector computer systems. They also include incident response capabilities and certain law enforcement authorities.

With respect to cost imposition, the President is able to draw on a range of response options from across the United States government.

Diplomatic tools provide a way to communicate to adversaries when their actions are unacceptable and to build support and greater cooperation among, or seek assistance from, allies and like-minded countries to address shared threats. Diplomatic démarches to both friendly and potentially hostile states have become a regular component of the United States' response to major international cyber incidents. In the longer term, U.S. efforts to promote principles of responsible state behavior in cyberspace, including peacetime norms, are intended to build increasing consensus among like-minded states that can form a basis for cooperative responses to irresponsible state actions.

Law enforcement tools can be used to investigate crimes and prosecute malicious cyber actors both within the United States and abroad. International cooperation is critical to cybercrime investigations, which is why the United States has promoted international harmonization of substantive and procedural cybercrime laws through the Budapest Convention, created an informal channel for data preservation and information sharing through the G7 24/7 network, and promoted donor partnerships to assist developing nations.

Economic tools, such as financial sanctions, may be used as a part of the broader U.S. strategy to change, constrain, and stigmatize the behavior of malicious actors in cyberspace. Since January 2015, the President has provided guidance to the Secretary of the Treasury to impose sanctions to counter North Korea's malicious cyber-enabled activities. Executive Order 13687 was issued, in part, in response to the provocative and

destructive attack on Sony Pictures Entertainment, while Executive Order 13722 targets, among others, significant activities by North Korea to undermine cybersecurity, in line with the recently-signed *North Korea Sanctions and Policy Enhancement Act of 2016*. Aside from these North Korea-specific authorities, in April 2015, the President issued Executive Order 13694, *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*, which authorizes the imposition of sanctions against persons whose malicious cyber-enabled activities could pose a significant threat to the national security, foreign policy, or economic health or financial stability of the United States.

Military capabilities provide an important set of options for deterring and responding to malicious cyber activity. The Department of Defense continues to build its cyber capabilities and strengthen its cyber defense and deterrence posture. As part of this effort, the Department of Defense is building its Cyber Mission Force, which is already employing its capabilities to defend Department of Defense networks, defend the Nation against cyberattacks of significant consequence, and generate integrated cyberspace effects in support of operational plans and contingency operations. In addition, Secretary of Defense Ashton Carter announced earlier this year that U.S. forces are using cyber tools to disrupt Da'esh's command and control systems and to negatively impact its networks.

Intelligence capabilities are also an important tool at the President's disposal in detecting, responding to, and deterring malicious activities in cyberspace, particularly given the unique challenges associated with attributing and understanding the motivation behind such malicious activities.

Even with this broad range of tools, deterring cyber threats remains a challenge. Given the unique characteristics of cyberspace, the United States continues to work to develop additional and appropriate consequences that it can impose on malicious cyber actors.

Capacity Building

In addition to the tools that I have just outlined, the ability of the United States to respond to foreign cyber threats and fight transnational cybercrime is greatly enhanced by the capabilities and strength of our international partners in this area. Therefore, the Department of State is working with departments and agencies, allies and multilateral partners to build the capacity of foreign governments, particularly in developing countries, to secure their own networks as well as investigate and prosecute cybercriminals within their borders. The Department also actively promotes donor cooperation, including bilateral and multilateral participation in joint cyber capacity building initiatives.

In 2015, for example, the United States joined the Netherlands in founding the Global Forum on Cyber Expertise, a global platform for countries, international organizations, and the private sector to exchange best practices and expertise on cyber capacity building. The United States partnered with Japan, Australia, Canada, the African Union Commission, and Symantec on four cybersecurity and cybercrime capacity building initiatives. The Department also

provided assistance to the Council of Europe, the Organization of American States, and the United Nations Global Program on Cybercrime to enable delivery of capacity building assistance to developing nations. Many traditional bilateral law enforcement training programs increasingly include cyber elements, such as training investigators and prosecutors in the handling of electronic evidence. Much of our foreign law enforcement training on combating intellectual property crime focuses on digital theft.

In another example of capacity building, the Department of State, through its Bureau of International Narcotics and Law Enforcement Affairs, manages five International Law Enforcement Academies (ILEAs) worldwide, and one additional Regional Training Center. These six facilities provide law enforcement training and instruction to law enforcement officials from approximately 85 countries each year. The ILEA program includes a wide variety of cyber investigation training courses, from basic to advanced levels, taught by subject matter experts from the U.S. Secret Service and other agencies and policy-level discussions with senior criminal justice officials. This serves as a force multiplier to enhance the capabilities of the international law enforcement community to collaborate in the effort to fight cybercrime.

The Department of State is committed to continuing its capacity building initiatives as another effective way to counter international cyber threats and promote international cyber stability.

Looking ahead

Cybersecurity will continue to be a challenge for the United States when we take into consideration the rapidly expanding environment of global cyber threats, the increasing reliance on information technology and number of "smart devices," the reality that many developing nations are still in the early stages of their cyber maturity, and the ongoing and increasingly sophisticated use of information technology by terrorists and other criminals. Thus, the Department of State anticipates a continued increase and expansion of our cyber-focused diplomatic and capacity building efforts for the foreseeable future.

The Department will continue to spearhead the effort to promote international consensus that existing international law applies to state actions in cyberspace and build support for certain peacetime norms through assisting states in developing technical capabilities and relevant laws and policies, to ensure they are able to properly meet their commitments on norms of international cyber behavior.

The Department of State remains appreciative of this Subcommittee's continued support. Thank you for the opportunity to testify today. I am happy to answer your questions.