Testimony of Christopher M. E. Painter, Coordinator for Cyber Issues,
U.S. Department of State
Before the Senate Foreign Relations Committee Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy
Hearing Titled: "Cybersecurity: Setting the Rules for Responsible Global Behavior"

May 14, 2015

Chairman Gardner, Ranking Member Cardin, members of the Senate Foreign Relations Committee Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy, it is a pleasure to be here today to speak about our cyber foreign policy.

Before I begin, I would like to commend your Subcommittee for recently taking on "International Cybersecurity Policy" as a part of your portfolio. This development is yet another important step in our government's efforts to strengthen our foreign policy on cyber issues. It is also further recognition of the growing importance of cyber policy to our national security, foreign policy, economy, values, and way of life. Moreover, the fact that cyber policy is the subject of the subcommittee's first hearing during the legislative session indicates the importance you place on this new role. On behalf of my office and the State Department, I look forward to working with you.

Cyber Issues: A New Foreign Policy Imperative

When it comes to the foreign policy implications of cyber issues, it is important to begin with the recognition that this Subcommittee and the State Department are working in a still-nascent policy space. While the Internet has been growing and evolving for a few decades now, the international community has only more recently begun to fully grasp cyber issues as a foreign policy priority.

Only four years ago this month, the White House issued its *International Strategy for Cyberspace*, leading the world in recognizing the need for a comprehensive and crosscutting strategic approach to this key area. We were also the first country to establish a foreign ministry office like the one I lead —the State Department's Office of the Coordinator for Cyber Issues— to coordinate diplomatic efforts across the full range of international cyber policy issues.

The world has changed dramatically even since then. Now there are offices like ours in foreign ministries throughout the world, and new ones are steadily being created as more countries look to engage in the global cyber policy dialogue. Cyber issues have become central topics of discussion in virtually every international venue, and cyber diplomacy is increasingly viewed by governments as a foreign policy imperative.

Nonetheless, cyber issues remain in many respects an emerging area of foreign and national security policy. The global community is still in an early stage of tackling these

challenging issues and building consensus towards solutions that are consistent with the core values of democracy and human rights. In the United States, we have made great strides in articulating our strategic vision for cyberspace, but we are still working to fully develop the necessary capabilities to ensure we can continue to lead in this dynamic policy area and respond to crises as they emerge.

These efforts occur in a context of growing threats—both technical and policy related—to the open and interoperable global Internet we seek to preserve and expand. On the technical side, we face increasing risks from state and non-state actors that conduct malicious cyber activity for the purpose of stealing trade secrets or personal information for commercial or financial gain, suppressing freedom of expression, destroying data, harming our critical infrastructure, or causing various other types of harm. North Korea's cyber attack on Sony Pictures Entertainment demonstrated the potential coercive effects of such activity. The more recent targeting of Github highlights a new and worrying trend of cyber capabilities being used from abroad to influence public expression within the United States. While, as the Director of National Intelligence recently noted, the "likelihood of a catastrophic attack from any particular actor is remote at this time," we are likely to see "an ongoing series of low-to-moderate level cyber attacks from a variety of sources" that will, over time, "impose costs on US economic competitiveness and national security."

In the policy context, we face significant and growing challenges, especially from China, Russia, and other authoritarian governments that seek increased sovereign control over the Internet and its content. These challenges surface in a variety of fora and across a range of policy issues. Internet governance is a prime example of a challenging cyber policy area. Here, we see governments that are more concerned with regime stability than with economic and social development pushing to shift from the long-standing and successful multistakeholder model—one that involves active participation by governments, the private sector, civil society, and academia in an inclusive and bottom-up process—to an intergovernmental and exclusive system that could fundamentally undermine the future growth and potential of the Internet. The fight against transnational cybercrime is another area where we face a policy challenge. China and Russia are aggressively advocating for a new global cybercrime agreement that would serve as a vehicle for controlling speech and undermining civil and political rights, while at the same time criticizing the effectiveness of existing international instruments like the Council of Europe Convention on Cybercrime, or Budapest Convention.

Our work to respond to these threats is guided by the vision of the U.S. *International Strategy for Cyberspace*, which seeks "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." The State Department—not just my office, but the full complement of security, economic, human rights, law enforcement and regionally-focused bureaus and offices throughout the Department—works across a range of interconnected cyber policy issues to achieve this vision through our diplomatic

efforts. This includes promoting cyber stability among states through norms and confidence building measures, building the domestic cybersecurity capacity of our partners and channels for international cooperation on incident response, fighting cybercrime, advancing human rights online, promoting the continuation of an effective multistakeholder model of Internet governance, and, in cooperation with our colleagues at USAID among others, promoting capacity building, technical assistance, and development programs to tackle security challenges and address Internet access and affordability issues.

Accordingly, my office works closely with offices and officials across the Department—including Under Secretary for Economic Growth, Energy, and the Environment, Catherine Novelli, who serves as the Senior Coordinator for International Information Technology Diplomacy; the Bureau of Democracy, Human Rights and Labor; the Bureau of International Narcotics and Law Enforcement; the Bureau of Economics and Business Affairs Office of International Communications and Information Policy; the Bureau of Counterterrorism; the Bureau of Arms Control and Verification; among other functional components, and every regional bureau. We also coordinate our work with colleagues throughout the Federal Government, including at the Departments of Defense, Justice, Homeland Security, Commerce, and Treasury.

The State Department is a key player in all U.S. government interagency cyber policy processes, ensuring that timely and pertinent foreign policy guidance is provided to decision makers at all levels. Given the global nature of the Internet, even ostensibly domestic cyber policy decisions typically have a foreign policy or diplomatic dimension. We also leverage State's global diplomatic corps, including our growing cadre of cyber officers, to support the vision articulated in the U.S. *International Strategy for Cyberspace*, and respond to growing threats.

Review of the Global Cyber Landscape

Before describing our international priorities in detail, it is useful to review some of the most recent cyber developments from around the world to better frame the kinds of challenges and opportunities that we face. We can call it a short "cyber policy world tour."

Given the Subcommittee's focus on **East Asia and the Pacific**, I will begin there. As you know, this dynamic region is playing an increasingly important role in the world, particularly in the area of cyber policy. Within the region, there is much focus on China's role in cyberspace. In recent years, China has become more assertive in promoting its vision for cyberspace—government-controlled, with an absolutist conception of sovereignty over technology and content—that stands in stark contrast to our own policy priorities. As we push back against these repressive concepts, we also continue to engage China on areas of potential cooperation, such as network defense and other practical measures that could reduce the risk of conflict in cyberspace. At the same time, the Administration has been clear, consistent, and

direct in raising our concerns with the Chinese regarding issues such as state-sponsored cyber-enabled theft of intellectual property for commercial gain. We have also been concerned by recent reports that China has used a new cyber capability to interfere with the ability of worldwide Internet users to access content hosted outside of China, including the web developer site Github. Although we regret China's decision to suspend the activities of the U.S.-China Cyber Working Group, we have continued to engage Chinese cyber experts on areas of concern. We remain committed to expanding our cooperation with the Chinese government on cyber matters where we have common ground and to candidly and constructively addressing differences.

The United States maintains strong and on-going diplomatic relations on cyber issues with a number of other countries in the region. We work very closely across the range of cyber policy topics with our friends in Japan, South Korea, Australia and New Zealand, with whom we share a common vision for cyberspace. During Prime Minister Shinzo Abe's visit to Washington in April 2015, both the United States and Japan reaffirmed their commitment to working together "to ensure the safe and stable use of cyber space based on the free flow of information and an open internet." The United States also engages on regional security issues in the ASEAN Regional Forum, where we are actively promoting the development of regional cyber confidence building measures. We are seeking to expand our bilateral engagement with several ASEAN states, including Indonesia, Singapore and Malaysia, and actively promoting cybercrime capacity building efforts in the region in partnership with Japan and Australia.

Finally, the region includes North Korea, which was responsible for the November 2014 cyber attack on Sony Pictures Entertainment. The destructiveness of that cyber attack, coupled with its coercive nature, sets it apart from other malicious cyber activity we have observed in recent years. This is why the President publicly attributed the cyber attack to North Korea and vowed that we would "respond proportionally . . . in a place and time and manner that we choose." In January 2015, the President signed a new Executive Order, increasing our ability to apply sanctions pressure in response to the provocative, destabilizing, and repressive actions and policies of the government of North Korea, such as the destructive and coercive Sony Pictures cyber attack.

Next, we can turn to **Europe**, which largely shares our vision for an open and secure Internet, but which still contains security and policy challenges. The United States has very close relations with much of Europe and our cooperation in the region on cyber issues is increasing. We engage directly with the European institutions on cyber, notably the European External Action Service (EAS). Working with the EAS, we have launched a U.S.-E.U. Cyber Dialogue to address the cyber foreign policy matters of mutual concern and align our foreign policy posture on key issues in international fora.

My office leads regular bilateral engagements on cyber policy with individual countries like the United Kingdom, Germany, and France and has built regional collaborative engagements

with the Nordic and Baltic countries, including a cyber partnership statement with Estonia. We have emerging engagements, including increased outreach from our embassies, with Spain, Portugal, and Italy, among others, as they have increasingly joined in global cyber policy discussions. Our bilateral engagements with some countries, primarily Germany, have been punctuated by continued reactions to unauthorized disclosures and allegations of NSA electronic surveillance activities. We continue to work closely with the Administration and our colleagues within the Department to address the concerns we hear from our foreign partners.

While Eastern Europe has traditionally been the source—or conduit—for significant online criminal activity, there are numerous efforts underway at our embassies, and through other channels, to help build constructive engagement with a number of countries. This includes utilizing resources such as the International Visitor Leadership Program on one hand, and law enforcement capacity building and liaison programs on the other. As a result, we are starting to see some positive changes in national attitudes, most notably in Ukraine.

Russia is obviously an important cyber actor on the international stage, where it continues to assert its repressive agenda on a wide range of cyber issues. We are closely watching and working to counter their efforts to impose greater state control over the Internet and undermine security and human rights online. Given Russia's ongoing violation of Ukraine's sovereignty and territorial integrity, the United States has suspended our bilateral cyber dialogue with Russia. Nevertheless, we continue to interact with Russia on multilateral efforts in the United Nations and the Organization for Security and Cooperation in Europe (OSCE) to build greater stability and reduce the risk of conflict among states in cyberspace, through the development of norms of responsible state behavior and cyber confidence building measures. As long as Russia advocates an anti-democratic world view on cyber policy issues, we must work with our international partners to counter its destabilizing policies and activities.

The **Middle East** is a complex place, and we can see cyber issues becoming an increasingly important feature of the already multifaceted security and human rights challenges facing the region. There are real dangers of malicious cyber activity becoming enmeshed within—and potentially escalating—existing regional rivalries, and we have seen groups like ISIL harness the Internet as a tool for terrorist purposes. To guard against these threats, we are committed to working with our international partners in the region, including Israel and the Gulf states, to build a shared understanding of the threat, develop effective strategies and policy, and shore up vulnerabilities, especially in critical infrastructure. Through all of our efforts, we will help protect key U.S. interests and promote regional stability. Of course, promoting cybersecurity cannot come at the expense of the open Internet, which provides a tremendous set of opportunities for economic growth in a region that will be key to long-term development and stability.

South and Central Asia is a region where, despite challenges in some countries, we see new opportunities for engagement and growth. India is pursuing an exciting "Digital India"

agenda and is making progress on developing its cybersecurity capabilities. Its dynamic civil society, private industry, and technology sectors are increasingly playing leadership roles in cyber policy issues, such as Internet governance. With our shared democratic values, robust economic relationship, and people-to-people ties, the United States is primed for close strategic cooperation with India on the full range of cyber issues, and we are eager to strengthen our engagement. When Prime Minister Modi visited the United States in September 2014, we agreed to develop closer cybersecurity cooperation and to reinitiate our whole-of-government Cyber Consultations, which we look forward to pursuing this summer. We are also seeing leadership on cyber issues elsewhere in the region—for instance, Sri Lanka is taking important steps towards becoming the first state in the region to join the Budapest Convention, which will enable it to be a strong partner in combating global cybercrime. Other states are still figuring out how to grapple with cybersecurity and cybercrime challenges, but they are increasingly aware of the economic opportunities an open and interoperable Internet brings and increasingly paying attention.

Closer to home, within the **Western Hemisphere** we are presented with numerous opportunities to build stronger partnerships on the range of cyber issues, working bilaterally, within regional bodies like the Organization of American States (OAS), with civil society and with the private sector. The United States has had long-standing relationships with important actors in this region, including Canada with which we have a shared perspective on cyber policy. Brazil is another important actor on cyber policy, and I co-lead a bilateral whole-of-government working group with the Brazilians on Internet and ICT policy. As more people within the region gain reliable access to the Internet, more governments are recognizing the need to develop a coordinated strategic approach to cyber policy. With support from the United States and other partners in the region, the OAS has successfully trained law enforcement, judicial experts, and policy makers on the importance of increasing cybersecurity and combatting cybercrime. We believe that the OAS work, along with our longstanding efforts to engage bilaterally in the hemisphere, have contributed to the fact that nine Latin American countries are now in various stages of joining the Budapest Convention. Countries like Jamaica, Colombia, Costa Rica, and Chile are making a concerted effort to consult across ministries and to include experts from a variety of local sectors as they develop new legislation, update digital agendas, and craft cybersecurity strategies. Countries like Argentina and Uruguay are honing the skills of their workforce and working to expand their community of cyber experts from urban centers to rural areas. Taken as a whole, our friends in the region are working towards a truly cyber-savvy citizenry, and we are supporting that growth by strengthening existing partnerships and seeking new opportunities for engagement.

The final region on our tour, but certainly not last in our list of priorities, is **Africa**, a region with relatively low but fast-growing Internet penetration and a strong incentive to build an open, secure and interoperable Internet as an engine for economic growth. As the use of the Internet and mobile phones expands throughout sub-Saharan Africa, nations are faced with a

corresponding increase in the number of cyber threats. Vulnerable networks erode the development benefits of ICTs and pose economic and security challenges to individuals, nations and the international community. Yet this same technology is contributing to stronger democratic institutions, boosting broad-based economic growth through trade and investment, advancing peace and prosperity, and promoting opportunity and development. This is why African nations have been a significant focus of my office's Foreign Assistance programming. We are working with African leaders and citizens in an enduring, multi-faceted partnership on cyber issues—one that is not about overnight solutions or one-off deals, but instead focuses on long-term collaborative efforts among all stakeholders. We are bringing key partners together bilaterally, while working multilaterally with the African Union Commission (AUC) and key Regional Economic Communities to help our partners build and shape effective and sustainable cyber architecture that serves Africa on a regional and global scale. This includes continuing our tradition of training and engagement on cybersecurity best practices, building the requisite legal frameworks for states and individuals to combat the threat of cybercrime, working to maintain open and unfettered access for all Africans, and encouraging African voices and perspectives in the very relevant conversation we are having on how states should work together to prevent cyber conflict. These were the topics of utmost interest to African officials I met in June 2014 when I joined colleagues from across the Southern African Development Community for a four-day cyber policy training session—the fourth regional workshop in a series that we have presented across the continent—and they will continue to be the focus of our work on the continent in 2015.

Lastly, our cyber world tour would not be complete without discussing the cyber policy debates that are currently taking place in **multilateral venues**. Here the picture is complicated by the fact that there is a multitude of fora that address the range of cyber issues. For our work in promoting international security and stability in cyberspace, we look to the United Nations and within regional security organizations like the OSCE and the ASEAN Regional Forum. Issues around cybercrime are dealt with in fora like the Council of Europe and the United Nations Office of Drugs and Crime (UNODC). However, cyber issues do not only arise in traditional international fora. Dynamic and decentralized multistakeholder venues that include representation from the private sector and civil society as well as states play a key role in Internet governance, and we work with this range of stakeholders to promote our vision for the Internet.

It is within multilateral venues that we most frequently encounter the types of policy threats that I noted earlier. Countries like Russia and China use these venues to press for greater government control over the Internet, for example, by advocating that the International Telecommunication Union take a greater role in Internet governance and pushing for a United Nations cyber treaty. To date, the United States has worked very effectively with likeminded countries to stave off the challenges in these venues. At the same time, there have been a number of successes in multilateral fora, particularly on security issues, as discussed below.

Cyber Policy Priorities

This is the world that we face. I am optimistic about our ability to respond to the threats, build cyber stability and resilience, and ultimately continue to capitalize on the rich economic and expressive opportunities that the Internet offers us. But there is much work to be done. I want to spend some time now talking about what the State Department is doing to support whole-of-government efforts to engage the world that we have just toured on cyber policy issues.

1. Security and Cybercrime

With respect to **security issues**, our long term vision is to strive for a state of "international cyber stability": a more peaceful environment where all states are able to enjoy the benefits of cyberspace; where there are benefits to state-to-state cooperation and avoiding conflict; and where there is little incentive for states to attack one another. We are pursuing efforts along two lines to achieve this longer term goal.

First, we are working to develop a shared understanding about norms of responsible state behavior in cyberspace, which will help enhance stability, ground foreign and defense policies, guide international partnerships, and help prevent the misunderstandings that can lead to conflict. In recent years, we have had tangible successes in developing these norms. The 2013 UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE)—a group of fifteen countries that included the United States as well as countries like Russia and China—reached a landmark consensus that international law applies to state conduct in cyberspace. In the current round of the GGE, we are working to build on this important consensus with an even broader group and look more closely at how international law applies to state conduct in cyberspace.

As part of these efforts, the United States has also been considering what voluntary measures of self-restraint states should implement, since cyber tools can be used across the spectrum of conflict, most notably below the threshold of the use of force. Accordingly we have sought to identify some voluntary norms of responsible state behavior during peacetime that would be universally appropriate and that will keep all of us safer if states adopt them. They include:

- 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 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 cyber crimes, collecting electronic evidence, and mitigating malicious cyber activity emanating from its territory. States must take robust and co-operative action to investigate criminal activity by non-State actors.

- 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.

These voluntary measures are beginning to gain traction internationally. During the current round of the GGE, we proposed the inclusion of several of these norms in the group's draft report and many states have spoken positively about their inclusion. In addition, on the occasion of Prime Minister Abe's recent visit to Washington, Japan and the United States released a leaders-level statement that affirmed that states should uphold additional, voluntary norms of state behavior in cyberspace during peacetime, noting that wide affirmation among states would contribute to international stability in cyberspace. Australia's Foreign Minister also affirmed some of these concepts in recent remarks.

Second, in addition to promoting norms, our international security work has also focused on the establishment of practical cyber risk reduction and confidence building measures (CBMs), which are intended to reduce the risk of escalation due to misunderstanding or miscalculation regarding a cyber incident of national security concern emanating from U.S. or another country's territory. The first ever bilateral cyber CBMs were announced by President Obama and President Putin in June 2013. And in December 2013, at the ministerial of the OSCE, we achieved an agreement among the 57 participating states for the first ever cyber CBMs for a multinational security organization. We are now working to implement the current CBMs, and we are also pursuing the development of cyber CBMs in other regional organizations, such as the ASEAN Regional Forum.

Alongside these efforts, and with a shorter term focus, we are working to strengthen the ability of the U.S. government as well as our foreign partners to respond to cyber events as they occur. We strongly favor increased direct international cooperation among Computer Security Incident Response Teams (CSIRTs) and law enforcement entities to respond to and investigate cyber incidents, and we use our diplomatic engagements to support the building of those ties. Among our foreign partners, we encourage the development of whole-of-government national strategies as well as cooperation with the private sector on cybersecurity matters.

When incidents occur, we stand ready to support the whole-of-government response. State, as the lead foreign policy agency, plays a key role in interagency deliberations on major cyber events, and it engages diplomatic channels where needed. For example, during the 2012-2013 distributed denial of service attacks against financial institutions, State used diplomatic channels as a supplement to incident response efforts through more technical channels, ensuring that policy makers in foreign governments were aware of U.S. requests for assistance. More

recently, in response to the cyber attack on Sony Pictures Entertainment, we were pleased to see a number of foreign partners come to our support in condemning North Korea's actions. We have also used diplomatic channels to raise concerns regarding the cyber-enabled theft of trade secrets for commercial gain.

Beyond these efforts, State has supported the Administration's on-going efforts to fully develop its toolkit for deterring and responding to cyber threats. For example, we participated in the development and release of the recently announced Executive Order 13694, which allows for the targeted imposition of financial sanctions against persons engaging in certain significant malicious cyber-enabled activities that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States.

State also works closely with Department of Justice colleagues to strengthen international cooperation to combat trans-national **cybercrime** and other forms of high-tech crime. The continued expansion of the Budapest Cybercrime Convention – which has 45 parties representing the Americas, Europe, Asia, the Pacific, and Africa, and more than a dozen additional countries in the final stages of joining – demonstrates the growing realization by governments around the world that cybercrime must be tackled head on, using a consistent and proven legal framework, in order to eliminate criminal safe-havens. Another key tool in our arsenal to counter high-tech crime is the G-7 24/7 Network which allows the national police in seventy countries to request rapid assistance in significant investigations involving digital evidence. The State Department is committed to working with like-minded partners around the globe to build both the will and capacity to effectively counter cybercrime, and we will continue to devote significant resources to that goal.

2. Internet Governance and Internet Freedom

We have also seen some recent successes in the areas of **Internet governance** and **promoting human rights online**, and we continue to take those efforts forward. In 2014, our work to maintain the current multistakeholder system was bolstered by the U.S. government announcement of the intent to transfer key Internet domain name functions to the global multistakeholder community; the strong, multistakeholder, consensus-based outcome of the NETmundial conference in Brazil; and the successful completion of the ITU Plenipotentiary Conference in Busan, South Korea, where, with the leadership of my colleague, Ambassador Daniel Sepulveda, we achieved a consensus that avoided expanding or establishing any new mandates for the ITU related to Internet governance or cybersecurity.

This year, we are looking forward to the tenth annual Internet Governance Forum, which will take place in Brazil. The IGF continues to provide a venue for global, multistakeholder dialogue on Internet policy issues that alleviates the need for a more centralized, intergovernmental approach to decisions about how the Internet works and the policies

surrounding it. A decision about whether to extend the IGF's mandate will be taken later this year by the UN General Assembly as part of their 10-Year Review of the World Summit on the Information Society—the so called WSIS+10 review. The focus of this year's review will be on the growth of the Information Society, essentially ICTs for development, over the last ten years. We believe there has been tremendous progress, as shown by the exceptional growth of the Internet around the world. Nonetheless, going forward, we will focus our attention and collective efforts on practical measures to close the remaining gaps in access and capacity.

The United States can also count successes in our efforts to promote Internet freedom and human rights online, thanks in large part to the efforts of State's Bureau of Democracy, Human Rights, and Labor (DRL). At the core of our policy approach is the maxim that the same human rights that people have offline also apply online—a view that was adopted by the UN Human Rights Council in a 2012 resolution and reaffirmed again in 2014 —and this position is mainstreamed across all of State's work, including our efforts to promote cybersecurity and fight cybercrime. Together with my colleague Tom Malinowski, Assistant Secretary of State for DRL, I have just returned from this year's meeting in Ulaanbaatar, Mongolia, of the Freedom Online Coalition, a group of now 26 governments committed to taking concrete action in support of Internet freedom. Programmatically, DRL works with USAID, our Near East Asia bureau and others, to support advocates who promote freedom online, as well as the development of technologies that assist in those efforts.

3. Bilateral Engagements

State's cyber diplomacy also focuses specifically on our **bilateral relationships** with a number of key countries. Bilateral engagements, or engagements with smaller groupings of countries, provide a valuable opportunity to share views with partners, identify areas of agreement, address differences of opinion, and develop areas for cooperation.

State has pioneered a whole-of-government model for conducting bilateral engagements on cyber policy issues, which brings together cyber policy experts from across our government (for example, from DoD, Justice, DHS, and Commerce) to engage simultaneously with foreign government counterparts. We find that this approach helps avoid uncoordinated discussions between individual agencies on certain topics and at times has the added benefit of encouraging interagency cooperation among our partners.

We are currently conducting formal whole-of-government cyber dialogues with Germany, the Republic of Korea, Japan, the European Union, and the eight Nordic-Baltic states, and we are in the process of reinvigorating dialogues with Brazil and India. As mentioned earlier, we also have official dialogues with China and Russia, both of which are presently suspended. We also regularly engage with Australia, Canada, New Zealand and the United Kingdom in both formal and informal settings, consistent with our close relationship across the spectrum of security issues. In addition, the State Department conducts less formal cyber

bilateral engagements with a number of countries and multilateral organizations. Finally, it should be noted that there are a number of other State policy dialogues that complement our efforts, such as the ICT policy dialogues that Ambassador Sepulveda's office in the Bureau of Economic and Business Affairs leads with key economic partners as well as the human rights dialogues led by DRL.

4. Capacity Building

The State Department and USAID are actively **working to build the capacity of foreign governments** across a range of interconnected cyber policy issues—with a principal focus on expanding internet access through innovation, improving domestic cybersecurity through the development of CSIRTs and national strategies, improving the ability to fight cybercrime and other forms of high-tech crime, and ensuring the ability to cooperate with global partners to address shared threats. Recently, the U.S. became a founding member of the Global Forum for Cyber Expertise, which was launched on April 16, 2015, during the Dutch-hosted Global Conference on Cyberspace in The Hague, reaffirming our commitment to cyber capacity building.

In particular, recognizing that our ability to fight transnational cybercrime and respond to foreign cyber threats is greatly impacted by the strength of our international partners, State, including our Bureau for International Narcotics and Law Enforcement Affairs, is working with colleagues at the Departments of Justice and Homeland Security to build the capacity of foreign governments to secure their own networks as well as investigate and prosecute cybercriminals within their borders. Working with multilateral organizations like the AUC, the UNODC (via its Global Cybercrime Capacity Building Program), the Council of Europe, the European Union, the G-7, and the OAS, we promote cybercrime policies in line with the Budapest Convention and share cybersecurity best practices, such as writing national cyber strategies, forming cybersecurity incident response teams, and promoting public awareness campaigns on good cybersecurity practice. Most recently, at the end of fiscal year 2014, my office obligated over $1 million of our limited foreign assistance funds to Carnegie Mellon University's Software Engineering Institute, a federally funded research and development center, to begin a project in Sub-Saharan Africa on cybersecurity incident response and incident management capabilities and coordination. We are hopeful that this and related efforts can expand and serve as a model for future capacity building assistance programs.

We believe that cybercrime and cybersecurity capacity building overall must be a priority for the U.S. Government going forward. If they are not adequately addressed by the United States and key partners, then we run the risk that as the Internet continues to expand in the developing world, it will do so without necessary cybersecurity safeguards, creating global risks and undermining the conditions necessary to realize the economic and social benefits offered by expanded broadband access.

5. Mainstreaming Cyber Policy at State

Last, we are working to **mainstream cyber policy issues across State and USAID**, so that we can more effectively leverage both personnel and budget resources as tools for implementing our cyber policies. Nearly every bureau within the Department—whether regional or functional—now plays some role in cyber policy making. To prioritize our engagements and resources, we have worked with our regional bureaus to develop cyber-specific regional strategies focusing on key partners in each part of the world. To better leverage our embassies in implementing these regional strategies, we have brought 163 State Foreign Service Officers and USAID employees from 121 Missions together with U.S. Government experts through an innovative new training program created by my office to train diplomatic officers and support them in their own local cyber engagements. To identify resources and needs, we worked to incorporate cyber priorities into Department budget planning efforts. While this line of work does not involve actual engagement with foreign partners, it is an important part of building our government's capabilities to advance cyber policy issues going forward.

Conclusion

Thank you for the opportunity to provide State's perspective on global cyber issues and on our international cyber priorities. We look forward to working with the Subcommittee towards protecting our security here at home and ensuring that all of us can continue to benefit from an open, interoperable, secure, and reliable global Internet.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu