Testimony of Christopher M.E. Painter
Before the House Foreign Affairs Committee

Hearing on "U.S. Cyber Diplomacy in an Era of Growing Threats"

February 6th, 2018

Chairman Royce, Ranking Member Engel, members of the House Foreign Affairs Committee: it is a pleasure to appear before your Committee to discuss the growing technical and policy threats in cyberspace and the vital role of diplomacy in combatting those threats and shaping an international environment that promotes an open, interoperable, secure and reliable information and communications infrastructure around the globe. For over twenty-six years I have devoted my life to these issues, serving as a federal prosecutor, a senior official at the Department of Justice and the FBI, a Senior Director at the National Security Council and, most recently, as the first Coordinator for Cyber Issues at the Department of State. I have continued to work on these issues since leaving the federal government, among other things, serving as a Commissioner on the Global Commission for the Stability of Cyberspace and a Board member of the Center for Internet Security.

Over the course of my career, I have seen the technical threats in cyberspace posed by state and non-state actors dramatically increase in both sophistication and number, and have seen the potential and actual impact of those threats grow exponentially. I have also seen the rise of serious policy threats to the very nature, structure and governance of the Internet as we know it, unprecedented attempts to undermine democratic processes, and the increasing drive by repressive regimes to suppress and control online discourse and undermine Internet freedom. Given the severity of the threat and our increasing dependence on cyberspace, the U.S. and other governments around the world have moved from treating cyber policy —including cybersecurity, cybercrime, Internet governance and Internet freedom — as niche or technical issues to treating them as core issues of national security, economic policy, human rights and, ultimately, core issues of foreign policy.

It is clear that responding to cyber threats and seizing the many opportunities in cyberspace requires a whole-of-government response, leveraging the capabilities of agencies across the federal government and working with the private sector and civil society. It is also clear, given the international nature of the threats and the technology itself, that the State Department should play a leading role in that effort and that effective cyber diplomacy — perhaps one of the most challenging and complicated foreign policy issues facing us today — is paramount. The United States has provided significant leadership in this area in the past. Indeed, my former office, the Office of the Coordinator for Cyber Issues — the first of its kind anywhere in the world — literally created and advanced a whole new area of foreign policy focus that simply did not exist before and made substantial progress on a number of policy and operational fronts. As a testament to our leadership, and as a refection that this set of issues has come of age as an international policy priority, over twenty-five countries (including Russia and

China) have followed our example by establishing high level positions in their foreign ministries to spearhead cyber diplomacy.

For the U.S. to continue to lead, as it must, cyber issues must be re-prioritized and appropriately resourced at the State Department. Moreover, it is important that the position of the individual leading these efforts be at a very high-level — not buried in the bureaucracy or reporting through any one functionally or perspective limited chain of command. This is particularly important given the cross-cutting and interrelated nature of cyberspace issues that span a broad gamut — including national security, criminal, counter-terrorism, economic and human rights matters. This is not the time to demote these issues or step back from the world stage and cede leadership to others. That is an invitation for our adversaries to exploit our absence. Rather, given the rising tide of challenges we face in cyberspace, now is the time to elevate these issues and strengthen our country's ability to build alliances and continue to lead.

Threats in Cyberspace

A wide range of cyber intrusions and attacks directed at our government, businesses, citizens, and even the core of our democracy itself, have become a daily fixture of our lives. Threat actors are also diverse, including nation states, cybercriminals (both transnational organized groups and individuals) and terrorists, with an increased blurring of the lines between these actors especially when criminals act either at the behest, or with the tacit permission, of nation states. Recent events like the WannaCry ransomware worm illustrate emerging new destructive threats and the involvement of rouge state actors. Poorly or unsecured Internet of Things ("IOT") devices have led to new and powerful botnets and, while IoT holds incredible promise for huge economic and technological advancements, potential security issues could lead to significant harm and injury.

State-sponsored cyber intrusions and theft of information continue to be an economic and national security challenge and state-sponsored attacks pose a significant threat to both U.S. and international security. The Director of National Intelligence in his Worldwide Threat Assessment stated: "Our adversaries are becoming more adept at using cyberspace to threaten our interests and advance their own, and despite improving cyber defenses, nearly all information, communication networks and systems will be at risk for years." Like his predecessors, he listed Russia, China, Iran and North Korea as key state threats to the U.S. and terrorists and criminals as non-state threats. Over the past few years, malicious actors have used cyber means to damage and disrupt critical infrastructure and other networks, making a long time fear of such attacks a reality. And, while the U.S. has long focused on potential state sponsored attacks on critical infrastructure and the damage caused by the wide-spread theft of commercial information by state actors, it did not foresee the hybrid threat posed by Russia's cyber enabled attempt to undermine and influence the 2016 election that goes to the core of our democracy. This last challenge has played itself out in several other democracies and will be a significant issue in future U.S. elections. In addition, an increasing number of countries are developing cyber offensive capabilities with no clear doctrine for their use, raising the specter of cyber conflict, inadvertent escalation and unanticipated consequences and damage if and when they are used.

All of these challenges are exacerbated by the lack of effective deterrence and appropriate consequences for bad actors in cyberspace.

Criminals and criminal groups are becoming ever more sophisticated and creative in using cyber tools for theft, extortion (including an increase in the use of ransomware) and disruption, as well as using cyber capabilities and networks (including the Dark web) to facilitate both cyber and non-cyber criminal activity. Cybercriminal activity almost always has a significant international dimension — either because it is caused by geographically distributed trans-national criminal groups or because, even where the criminals and their victims are in the same country, smart criminals will route their communications and attacks through several countries to avoid detection and apprehension. Terrorist groups have long used cyberspace to plan, coordinate, inspire their followers, raise funds and recruit followers, and some have expressed interest in developing greater offensive cyber capabilities.

In addition to the above more technically focused threats, there are a number of policy threats and challenges facing the U.S. in cyberspace. Though cyberspace has proven to be a tremendous tool for economic expansion, innovation and social growth, many repressive or non-democratic regimes view the openness of the Internet as an existential threat to their control and stability. Those states try to restrict access on the Internet, use cyber tools to monitor their citizens, and champion the pre-eminence of absolute sovereignty over the free flow of information and international human rights. Moreover, they have sought to replace the current multi-stakeholder system of Internet governance and promote a system of intergovernmental control that would both stifle innovation and undermine Internet freedom and human rights. Other policy challenges include the risk of multiple, conflicting regulatory regimes related to various aspects of cyberspace and the Internet. For example, multiple jurisdictions are considering some sort of regulatory regime involving the Internet of Things. Forced data localization and cybersecurity regulatory regimes that appear to be more focused on "indigenous innovation" and market protectionism rather than security pose additional economic and security challenges for the U.S.

The Role of Diplomacy

Against this sobering backdrop, the need for diplomacy, working in conjunction with other instruments of our national power, is clear. Because cyberspace threats are almost always international, as is the technology itself, an unprecedented level of international coordination, engagement and cooperation is required both to counter those threats and embrace and drive the economic and social opportunities that cyberspace offers for the future. This diplomatic effort must also be cross-cutting because security, economic and human rights issues in cyberspace are often interdependent. In recognition of the need to increase our focus and leadership on international cyber issues, my former office at the State Department was created in the Secretary's Office. The office led on a number of policy and operational issues and coordinated with other offices throughout the building and the interagency on others. Some of the key areas of diplomacy in cyberspace include:

Building Strategic Partnerships and Engaging Multilaterally

A foundational aspect of cyber diplomacy is building strategic partnerships with other countries around the world to enhance collective action and cooperation against shared threats, assemble like minded coalitions on vital policy issues, share information and national initiatives and to confront bad actors. Over the course of six years, my former office established numerous senior bi-lateral and multi-lateral partnerships and launched numerous "whole of government" cyber dialogues with countries around the world. These include, among many others, Japan, Korea, Germany, France, India, the Nordic and Baltic countries, Brazil, Argentina, Israel, Mexico, Canada, Australia, the UK, New Zealand, Estonia and the EU. These formal and informal dialogues discussed the full range of cyber issues and have resulted in joint statements and, in the case of India, a comprehensive cyber framework. More importantly, they have translated into direct cooperation and common approaches in important multilateral venues. As we seek to advance common values, push back on repressive regimes and look to enhance collective action and deterrence, these partnerships need to be strengthened and expanded.

Nearly every formal and informal multilateral and regional body is now, in some capacity, focusing on cyber issues. These include multiple parts of the United Nations (including the ITU and UNODC), the Organization for Security and Cooperation in Europe ("OSCE"), APEC, ASEAN, the OAS, the G7 and the G20. While these venues offer the opportunity for the U.S. and its partners to advance a common vision of cyberspace or implement important initiatives (as we have, for example, in the OSCE on Cyber Confidence Building Measures), they also pose a challenge when non-democratic countries try to use those organizations to advance their own very different view of cyberspace. So far, working with our partners, the private sector, and civil society, we have generally been successful in advancing our agenda of an open and secure cyberspace and thwarting attempts by repressive regimes to impose state control over the Internet or undermine security or human rights. However, I believe we are at an inflection point, where the debates and decisions made in these forums over the next several years will have a major impact on all of these issues. If we are to advance our vision and defend our core values, the U.S. must continue to engage at a senior level in these many forums.

Enhancing Cooperation, Collective Action, Incident Response and Capacity Building

Diplomacy and diplomatic tools play an important role in directly responding to cyber threats and laying the groundwork for better cooperation and action against future threats. For example, using the network of counterparts we had built with other countries, my former office used diplomatic demarches to seek the assistance of over twenty countries when a persistent Iranian sponsored botnet was targeting U.S. financial institutions. This collective action, where each country used its authorities and tools to help address a shared threat, proved very effective in mitigating the malicious activity. Longer term and high level diplomatic pressure played a key role in addressing widespread trade secret and intellectual property theft by China. This included both working with other countries who were also victimized and a sustained campaign of direct diplomatic engagement by the U.S. This diplomatic campaign helped lead to the negotiation of a landmark agreement with China that made clear that no country should use cyber means to steal the intellectual property of another to benefit its commercial sector. Diplomacy and the State Department also have a vital role in working with DOJ and DHS to facilitate law enforcement and technical cooperation. Part of this facilitation is incident specific and part is working with countries to enhance their capabilities so that they can better work with us to combat threats. For example, my former office worked closely with DOJ to expand the countries who are members of the Budapest Convention on Cybercrime and with DHS in helping countries establish Computer Security Incident Response Teams.

Capacity Building also is important both to enabling better cooperation and in persuading other countries that our vision of cyberspace benefits and should be endorsed by them. My former office worked extensively with DOJ, DHS and others to create and implement ambitious cost-effective capacity building initiatives. These initiatives helped developing countries enhance cybercrime fighting capacity, create national cyber strategies and help create institutional and other mechanisms to protect against cyber threats that, given the global nature of these threats, allow them to not only protect their own networks but assist in the security of ours. We also worked with countries as they developed their cybersecurity policies to ensure that they properly accounted for human rights and economic access concerns. While modest amounts of funding for capacity building pay comparatively large dividends, both in bolstering our own security and in promoting U.S. leadership, unfortunately, funding for these efforts has been dramatically curtailed.

Advancing Strategic Policy and Building a Consensus for Global Cyber Stability

A cornerstone of U.S. cyber diplomacy is promoting and protecting core values such as openness, Internet freedom and multi-stakeholder Internet governance that have all been threatened over the last several years. The U.S. is a founding member of the Freedom Online Coalition and has raised Internet freedom and Internet governance issues in virtually every diplomatic engagement. Diplomacy must also be used to push back on flawed cyber regulatory regimes or policies that serve to fragment the Internet and risk undermining its incredible social and economic potential. We have used diplomatic channels to challenge forced data localization regimes, ill-conceived cyber regulatory approaches and market access restrictions, and have partnered with the Department of Commerce in promoting the NIST Cybersecurity Framework with partners around the world. And, diplomacy plays a vital role in ensuring the long term stability of cyberspace itself in the face of increasing nation state and other threats, so that everyone can enjoy the benefits of cyberspace and so no state has an incentive to engage in disruptive behavior. Though all of these are of these are important issues, all requiring substantial diplomatic international engagement, in the interest of time, I will focus on the last.

As countries around the globe are developing, and in some cases using, cyber offensive and other capabilities, the lack of any clear consensus on acceptable state behavior in cyberspace poses substantial risks to the many benefits it offers. To address this, the U.S. has led the development and promotion of a strategic framework of cyber stability that includes (1) global affirmation of the applicability of international law to state activity in cyberspace; (2) the development of voluntary, non-binding peacetime norms of acceptable state behavior; and (3) the development and use of practical confidence building measures (CBMs) that serve to reduce the risk of misperception and escalation in cyberspace. The U.S., led by my former office, has had great success in promoting and achieving acceptance of this framework in forums around the world including in the Group of Governmental Experts (UN GGE) on international cyber security (a series of expert forums in the United Nations), NATO and the Organization for Security and Cooperation in Europe. In the 2013 UN GGE report, countries, including the U.S., China and Russia, reached a landmark consensus that international law, including the U.N. Charter, applies in cyberspace. That means that cyberspace is not a "free fire" zone where no rules apply but is grounded in the same rules as the physical world. In 2015, the UN GGE recommended voluntary, norms of responsible state behavior including several peacetime norms that the U.S. has advocated. These voluntary, non-binding norms included states refraining from attacking the critical infrastructure of another state, states refraining from attacking Computer Security Incident Response Teams, and states cooperating with requests for assistance in certain cyber attacks. The agreement on a theft of trade secret norm that the U.S. reached with China was adopted by the G20 and by other country bi-lateral agreements with China. The U.S. also made substantial progress in the OSCE in taking forward and implementing cyber CBMs.

While all of this represents significant progress in achieving global cyber stability, there is much more to be done and the head winds are stiff. The 2016 UN GGE ended in a stalemate, some authoritarian regimes are aggressively promoting their own vision of cyberspace that restricts openness, and some regimes are resisting necessary efforts to assess exactly how international law applies to cyberspace. There is an urgent need to build a broader consensus among countries on the norms we have put forth, much work required to implement them, and significant effort ahead on further articulating how international law applies to cyberspace. This again will require a sustained high level and well resourced effort by the State Department not only with large multilateral organizations, but also with smaller groups of countries and in regional venues.

Of course, discussion of norms and cyber stability are not just the province of governments — though governments are in a unique position to implement them. There has been great work done in thinking through these issues by the private sector and civil society. I currently serve as a Commissioner on the Global Commission for the Stability of Cyberspace, an international initiative that was formed to help foster stability and advance a global multi stakeholder engagement on these issues. That group recently proposed a Call to Protect the Public Core of the Internet. It is an appeal for a new global norm to apply to both state and non-state actors to refrain from activity that intentionally and substantially damages the general accessibility or integrity of the Internet itself. The Commission is engaging with governments and other stakeholders on this proposed norm now and is considering other cyber stability measures to be proposed in the future. Other companies and organizations are active and have performed good work in this area as well.

Like nearly everything in cyberspace, public private partnerships are important in cyber diplomacy. Our policies are better and have a stronger chance of success when the government interacts with civil society and the private sector and it is important for the Department to work with these groups across the full range of cyber issues in a coordinated manner.

Deterrence

While the U.S. has made significant progress (with much more to do) in building an international consensus on what constitutes responsible state behavior in cyberspace, that work is largely irrelevant if there are no consequences for those who violate that consensus. We simply have not done a very good job of deterring malicious actors — particularly nation state actors. There are many reasons for this including difficulties with attribution, a limited tool set of potential consequences, and difficulties sharing information with partner countries. Nevertheless, at the heart of deterrence is the threat of a credible and timely response to the transgressor. Failure to act in a credible or timely way creates its own norm of inaction and signals to the adversary that their actions are acceptable — or at the very least cost free. For example, the lack a sufficiently strong, timely and continuing response to Russian interference with our electoral process virtually guarantees that they will attempt to interfere again, both in the U.S. and in other democratic countries. We must do better.

Diplomacy can and should play a vital role in this effort. Diplomacy is of course one of the key tools in the tool set of response options that also include law enforcement actions, economic sanctions, cyber and kinetic responses. We must continue to employ diplomacy effectively and work to enhance all of our existing response options. We must also work with our like-minded partners and other stakeholders to creatively develop new tools that can be imposed swiftly and be reversible in order to change an adversaries' behavior — expanding the tool set and communicating, as transparently as possible, the likely costs that will be imposed for bad behavior. And, we must enhance collective action. Although the U.S. always reserves the option to act alone if it must, deterrence and legitimacy is better served when several countries band together against a bad actor. There is much diplomatic work to do in forming such an agile coalition of like-minded countries who can call out bad behavior and collectively impose costs on our adversaries. Such a coalition should flexible and can involve different countries and different actions depending on the actor, but creating it, and solving information sharing and other issues, will require a significant diplomatic effort.

Incorporating Foreign Policy Concerns into Broader Policy and Operational Decisions

Foreign policy considerations also play an important role in sensitive operational, military, law enforcement and other decisions and policies related to cyberspace and technology. It is vital for the State Department to have a senior voice at the interagency table for this range of issues to ensure that our actions and policies fully account for potential foreign policy concerns and to make sure we are pursuing the most effective course.

Creating an Effective Structure for Cyber Diplomacy

Although I have only briefly touched on the many areas of critical cyber policy in my discussion today, it is abundantly clear that diplomacy plays an indispensable role in keeping our country safe, promoting global cyber stability and promoting and defending economic interests and human rights in the digital world. It is also clear that there is a tremendous amount of work to be done and that senior, sustained and cross-cutting diplomatic leadership is imperative. Given the centrality and growing importance of these issues, and the leadership role the U.S. and the State Department had established, it was unfortunate that the Department chose to essentially eliminate my former position, downgrade these issues to a lower level, and fold my former office into an ill-fitting and overly narrow reporting chain that has a primary focuses on economic issues alone. Regardless of the qualifications or title of the person who takes on this portfolio, there is a huge difference, both within the Department and in dealing with interagency and foreign counterparts, between reporting to the Secretary (working with the Deputy, Under Secretaries and Assistant Secretaries across the Department), and being placed several rungs down the ladder reporting to a singe functionally focused Assistant Secretary. That organizational structure also hampers the ability to coordinate across the many important cyber issues that I have discussed today— including core security and human rights matters — that don't fit within a single functional mandate. Indeed, while economic issues are very important, everyone is to some extent a prisoner of their perspective, and its hard to see how issues around sensitive cyber operations, deterrence, norms of state behavior, fighting cybercrime, terrorist use of the Internet, responding to significant cyber incidents or even Internet freedom issues can be given full voice and consideration in that setting. Even if this organizational structure for cyber issues is only temporary, as was stated by the Deputy Secretary several months ago, it sends the wrong message to our adversaries, who seek to exploit any perceived lack of U.S. leadership, and to our allies, who are left to wonder about our continuing commitment.

For the U.S to lead and continue to make significant progress on cyber diplomacy, organizational structure and resources are important. The position leading these efforts must be high-level, with broad cross-cutting and coordinating authority and it must report through a neutral reporting chain that allows full consideration of the broad range of issues in cyberspace. Of course, especially as cyber issues continue to gain prominence and are intertwined with physical world issues, other functional offices and their expertise will have an important role to play, and not every issue involving cyberspace or the Internet needs to be placed fully in one office. However, an effective cyber office and the person leading it needs to have clear coordinating authority over the broad range of cyber issues throughout the Department. Given the enormity and increasing importance of its mission, such an office also needs robust personnel, operating and capacity building (foreign assistance) resources. Over a six year period, I worked to build a well staffed and resourced office that, even at its height, was struggling to keep up with the constant and increasing demands of the dynamic cyber portfolio. Now, because of the hiring freeze, cost cutting and potential reorganization, I understand that my former office is operating at a significantly reduced strength, and that its foreign assistance budget has been virtually zeroed out. Finally, for cyber diplomacy to succeed, these issues need to be a real and publicly stated priority for the Secretary, and the person leading these efforts should have access to the Secretary and Deputy Secretary when needed.

The Cyber Diplomacy Act of 2017

Accordingly, I am pleased that this Committee proposed, and the House of Representatives passed, the bi-partisan Cyber Diplomacy Act of 2017. Over my lengthy career, I have found that these issues have almost always been treated in a bi-partisan manner and I am happy to see that reflected in this important legislation. The Cyber Diplomacy Act appropriately makes clear that international cyber issues and cyber diplomacy are a national policy priority. The "findings" section of the Act and the section on implementation reflect the broad range of cyber issues in play and gives appropriate emphasis to security, human rights and economic issues. It also appropriately recognizes the importance of cyber stability and responsible norms of state behavior in cyberspace.

Importantly, the Act sets out a strong and appropriate organizational structure for these issues at the State Department. First, it creates, by statute, the Office of Cyber Issues — giving needed permanence to this vital mission. Second, it articulates that the Office and the person heading it should have appropriately broad cross-cutting substantive duties — including leading diplomatic cyberspace efforts "relating to international cybersecurity, internet access, internet freedom, digital economy, cybercrime, deterrence and international responses to cyber threats" and coordinating within the State Department and the interagency cyberspace efforts and other relevant functions. Third, it specifically calls out the need for the position to work with the public and private sector on cyberspace issues. And, fourth, it makes clear that the head of the Office is to be "the principal cyber-policy official within the senior management of the Department of State and advisor to the Secretary of State for cyber issues."

The Act also helpfully prescribes that the head of the Office shall have an ambassadorial rank and be Senate confirmed. While this is important and appropriate given the importance of these issues — and helps with signaling to other governments and for accountability — I believe sufficiently high-level placement within the State Department hierarchy is of at least equal, if not even greater importance. For, example, a Deputy Assistant Secretary, even of ambassadorial rank, does not cary the same clout in the Department, with other governments or with other agencies, or the same access to the Secretary, as someone with an Assistant Secretary or equivalent position. That is especially true because a Deputy Assistant Secretary must normally report through an Assistant Secretary who will almost certainly have a more narrow functional or regional purview. Ideally, given the cross-cutting nature of the issues and the value of signaling the importance and authority of the position both to foreign governments and to interagency colleagues, the official should report directly to the Secretary, as I did, or the Deputy Secretary. The Act does not exclude that possibility, stating instead that the "head of the Office shall report to the Undersecretary of Political Affairs or official holding a higher position at the Department of State." Given, the current reticence to create or maintain additional direct reports to the Secretary, this is a fair compromise. Currently, the only more senior officials at State than the Political Undersecretary, are the Secretary and Deputy Secretary. Also, the Political Undersecretary, who has jurisdiction over all the regional bureaus, provides a neutral reporting chain and a broad perspective that is not stove-piped within any single functional perspective. Moreover, the Political Undersecretary can help with mainstreaming cyber issues throughout the Department and, most importantly, within the regional bureaus and our posts around the world. While I was at State, I worked with the Political Undersecretary who tasked each of the regional assistant secretaries to create comprehensive regional cyber strategies. These strategies not only helped raise the importance of these issues throughout the Department, but also were key building blocks for implementing our programs, working with our posts, and training a cadre of cyber officers in the field. As for level, presumably a direct report to the Political Undersecretary would be cast as an Assistant Secretary equivalent. Moreover, the Act helpfully notes that nothing in the Act prevents the office from being elevated to a full Bureau or the head from being officially designated as an Assistant Secretary — indeed, the Act contains a sense of Congress that this should happen.

The Cyber Diplomacy Act goes a long way toward addressing the urgent international cyber policy issues facing our country, and addressing the structure we need at the State Department to maintain and advance our leadership role. Of course, as I have noted, this effort must also be prioritized in terms of resources and I hope Congress will address this important issue in the future.

Conclusion and Way Forward

Although much has been achieved over the last few years in cyber diplomacy, we are still at the beginning of this journey and there is a long road ahead. The work and the choices we make now and over the next few years will determine whether we can all benefit from this amazing technology, or whether both growing policy and technical threats will undermine its incredible potential. Achieving the future we want will require continued high level attention and a significant, sustained, effort. Diplomacy has and must continue to play a pivotal role — shaping the environment, building cooperation, and working to build coalitions to respond to shared threats — and we must continue to lead the international community. I have only briefly touched on in my testimony the enormity of the work ahead. Much needs to be done to continue to advance stability and norms, bolster deterrence, respond to threats, build partnerships, uphold human rights online, and advance fair economic access and prosperity. Much more needs to be done as well to deal with existing and future hybrid threats — including combined cyber/ influence operation threats that attempt to undermine our democracy. Cyber Diplomacy is the quintessential 21st century issue of our foreign policy — involving aspects of human rights, security and economic policy. It requires cross-cutting leadership that leverages all of our capabilities, across the government, with the private sector and civil society, and with our foreign partners.

Thank you for the opportunity to testify today on this important and timely issue, and thank you for your interest and support for diplomacy in cyberspace. I look forward to your questions.