STATEMENT FOR THE RECORD

CHRISTOPHER PAINTER

Coordinator for Cyber Issues

Before the

House Foreign Affairs Committee

Subcommittee on Europe, Eurasia, and Emerging Threats:

Cyber Attacks: An Unprecedented Threat to U.S. National Security

March 21, 2013

Chairman Rohrabacher, Ranking Member Keating, and members of the Subcommittee, thank you for this opportunity to testify on the State Department's role in countering cyber threats. State is not only a key player in the U.S. response to ongoing cyber threat activity, but the lead agency for cyber diplomacy, promoting international cooperation on cyber issues in order to reduce the cyber threat worldwide. I commend the Subcommittee for focusing on this foreign policy imperative and for your support in promoting diplomacy as a tool for improving our nation's cybersecurity – and, by extension, our national security and economic interests.

The United States is a global leader in promoting the tremendous social and economic benefits inherent to cyberspace. As new technologies expand and progress, peoples of all nations seek to take advantage of emerging forms of connectivity. However, as cyberspace has evolved, so too have the threats to its networks and infrastructure. The United States is also a world leader in facilitating and encouraging cooperation among states to counter these increasingly common threats. The State Department plays a leading role in diplomatic efforts to stabilize cyberspace and to advance the vision of an open, interoperable, secure and reliable Internet articulated in the Obama Administration's 2011 *U.S. International Strategy for Cyberspace*.

We currently face several kinds of threats in cyberspace. First, there are operational threats to our cyber networks that, whether state-sponsored or criminal in nature, can potentially harm our security and do substantial harm to our economic interests. One recent example of this type of threat is the Distributed Denial of Service attacks that have targeted the U.S. financial sector. In these attacks, an attacker harnesses thousands of computers worldwide to use as a 'botnet' in an attempt to disrupt service by overloading systems with requests. To mitigate these kinds of threats, the State Department works closely with the Department of Homeland Security (DHS) and other agencies to share technical data with international partners. The United States has shared information related to the recent attacks with over 100 countries for use in mitigating the impact of similar attacks. Sharing this information not only helps counter the immediate threat, but also promotes international cooperation and transparency that will strengthen international collaboration to help prevent future attacks.

Another kind of threat that has been making news lately is large-scale cyber intrusion for purposes of stealing intellectual property, trade secrets, proprietary technology, and sensitive business information from the private sector. The Administration takes these threats seriously,

and last month, President Obama released the Administration's Strategy on Mitigating the Theft of U.S. Trade Secrets, which identified sustained and coordinated diplomatic engagement regarding trade secret theft and economic espionage as a critical element of the Administration's overall approach to such activities.

National Security Advisor Tom Donilon recently said, "increasingly, U.S. businesses are speaking out about their serious concerns about sophisticated, targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China on an unprecedented scale." The State Department has consistently raised our concerns about cyber intrusions with senior Chinese officials, including military officials, and we will continue to do so.

We are seeking meaningful, constructive dialogue with China on these issues. As National Security Advisor Donilon stated, "we need China to engage with us in a constructive direct dialogue." I welcome recent Chinese official statements that suggest a willingness to expand dialogue and discussion, and we have been engaging with China about that type of dialogue. The United States and China must work together to address this problem.

It is crucial that we continue to elevate cyber issues throughout our international engagements to promote global cooperation, to ensure that states take the threats seriously, to build consensus on the norms of responsible conduct in cyberspace that enhance international cyber security, and to address the recent malicious activity that has received extensive media coverage.

We face challenges within the international policy realm as well. Cyber issues are on the agenda in every major international forum and it is imperative that we engage diplomatically in these venues. Some states seem to view the dynamism and innovation of the Internet as a threat to the stability of their regimes. They reject the successful multi-stakeholder model of Internet governance that includes a role for states, civil society, and industry in favor of top-down intergovernmental control that enables state control and regulation of content. The "International Code of Conduct for Information Security" tabled at the UN General Assembly in 2011 by Russia, China, and other countries, is an example of this former approach. This proposal opens the door to greater government control over the Internet, including censorship by states of Internet content. It would limit freedom of expression online in order to promote political stability, a position at odds with existing international human rights instruments. The United States, by contrast, is committed both to a multistakeholder model that gives all appropriate stakeholders in the Internet the ability to participate in its evolution, and to a global consensus in which existing international law forms the basis for responsible behavior, including for protecting human rights online and the conduct of hostilities in cyberspace.

We believe that a cyberspace that rewards innovation, empowers individuals, develops communities, safeguards human rights, and enhances personal privacy will build better governments and strengthen national and international security. The Department of State promotes this vision both by actively working with our closest partners and allies, but also with states that are emerging as global leaders on the cyber stage, developing nations looking for ways to play in the cyber world, and even with states with whom we do not always see eye-to-eye.

The Department of State created my office in 2011 in recognition of the importance of ensuring an organizational focus on cyber policy issues across our international engagements. In my role as Coordinator for Cyber Issues at the Department of State, I coordinate and lead these international engagements. In order to effectively address these challenges, the Administration takes a whole-of-government approach, and the Department of State has worked closely with DHS, Commerce, DOJ, DOD, and other agencies to ensure that our foreign policy positions on cross-cutting cyber issues are fully synchronized. Together, we have sought to achieve the following principles:

1. National Security: Promoting a shared framework of existing norms that are grounded in existing international law.

Many states are developing military cyberspace capabilities—a prospect that has increasing potential to threaten our national security. Key aspects of cyber tools—the challenge of attribution of perpetrators or sponsors of attacks and the dual use nature of the technology—are inherently destabilizing. The State Department has pioneered the promotion of a framework in which States affirm that existing international law, including the law of armed conflict, is the appropriate framework to guide state-on-state behavior in the context of hostilities in cyberspace. We have also proposed transparency and confidence-building measures designed to reduce the risk of miscalculation that could inadvertently lead to conflict. The State Department has taken these concepts to the OSCE, the UN, and the ASEAN Regional Forum. We will continue to work to broaden the group of states who affirm the applicability of existing international law to cyberspace by leveraging our key strategic dialogues and demonstrating to states the benefits of abiding by the norms of conduct based in existing international law.

2. Cybersecurity Due Diligence: Challenge the international community to make cybersecurity a global policy imperative, develop national strategies, and foster transnational cooperation.

Cybersecurity at its core is the idea that each nation must protect its networks and information infrastructure by enhancing its security, reliability, and resiliency. By doing so, global security is enhanced. With our interagency partners, the State Department supports U.S. cybersecurity policy priorities by using our international partnerships; reducing intrusions and disruptions affecting U.S. networks; ensuring robust incident management, resiliency and recovery for information infrastructure; and improving the security of the high-tech supply chain. We also use existing public-private partnerships in support of critical infrastructure protection, international telecommunications, and trade. We complement those partnerships by also collaborating with the private sector on preparation for and participation in global cyber engagement in bilateral, regional, and international fora. A current example is our work with private sector and civil liberties organizations to augment their participation in the October 2013 Seoul Cyber Conference, the follow on to the preceding 2011 London and 2012 Budapest conferences.

The Internet is most rapidly expanding in the developing world, but developing states often lack the capacity to ensure its security. Over the last decade, U.S government international cybersecurity efforts have answered that charge, largely with a focus on helping countries build capacity for domestic cybersecurity. These efforts have been carried out through extensive

bilateral engagements and through concerted, long-term work in the UN, G-8, OAS, OECD. APEC, OSCE and ITU-D. The State Department is now leading the U.S. government in strengthening those efforts, challenging countries to build domestic capacity while simultaneously elevating their view of cybersecurity from a domestic to a global approach, a progression that requires countries to organize effectively and take systematic steps to operate securely in cyberspace, following shared international norms.

My office has supported this transition. We have established interagency capacity building programs to help developing states better protect their cyber and mobile networks, while also emphasizing the importance of protecting fundamental freedoms and promoting affordable access. The first of these programs, in Kenya in July 2011, alerted governments of the East African Community to vulnerabilities and provided tools for securing networks and cooperating internationally. A paired set of programs, in Senegal in September 2012 and Ghana in January 2013, reached fourteen states in West and Central Africa, and launched follow-on engagements to build long-term cyber partnerships in these regions. Programs such as these leverage U.S. government, private sector, and international expertise to help countries take the systematic steps needed to ensure safety and security in cyberspace, which in turn also fosters leaders who can lead and execute compatible capacity building efforts. We understand Ghana intends to craft its own national cyber strategy, and we welcome the continued opportunities to engage with them.

3. Cybercrime: Promote the Budapest Convention and capacity building to help other nations fight cybercrime.

The United States is the clear world leader in combating cybercrime and devotes extensive resources to helping other countries develop their ability to fight it. But unfortunately, cybercrime continues to grow at an exponential rate and most countries are struggling to tackle the challenge. The United States strongly supports the Budapest Cybercrime Convention and uses its structure as a basis for our capacity building efforts. That framework includes three key concepts: (1) ensuring law enforcement agencies have the authorities and tools to fully investigate cybercrime and deal with electronic evidence; (2) enacting substantive cybercrime laws; and (3) creating formal and informal mechanisms like the G-8 24/7 Network to ensure effective and timely international cooperation. We are actively making a renewed push to increase the number of parties to the Budapest Convention, and to increase the membership of the G-8 24/7 Network for law enforcement points of contact. A growing number of states have expressed interest in acceding to the Budapest Convention and we encourage additional cross-border cooperation on combating cybercrime.

4. Internet governance and public policy: Protect and promote inclusive global Internet governance mechanisms and ensure our vision of an open and interoperable Internet.

The Internet is currently managed by multi-stakeholder entities that reflect its dynamic, innovative nature, such as technical and standards bodies like the Internet Engineering Task Force and the Internet Corporation for Assigned names and Numbers. Public policy conferences like the Internet Governance Forum also play a vital role in shaping the Internet in a multi-stakeholder setting. This preferred architecture is under threat from those countries who seek a top-down, state-driven, UN-style mechanism for Internet management. The U.S. remains steadfast in our support for these existing, multi-stakeholder organizations. We also recognize

that their legitimacy is derived both from their efficiency and effectiveness and from a global perception that they are independent, transparent, and non-political institutions. The U.S. must continue to vocally support these institutions, provide constructive contributions as necessary, and encourage our friends and allies to do the same.

5. Internet Freedom: Promote respect for human rights, including freedom of expression online, and more fully integrate Internet freedom policy within broader cyber foreign policy goals.

In the wake of the Arab Spring and in light of increased global access to the Internet, a wider range of countries are pursuing policies that diminish protections for those freedoms of expression, assembly and association that are enshrined in the Universal Declaration of Human Rights. Countries pursue such policies through new domestic laws and regulations, through resolutions and agreements in international and multilateral institutions, and through targeting individual citizens peacefully exercising their rights online. As the State Department continues to respond to the largest Internet Freedom offenders, we have been deeply involved in the creation of the Freedom Online Coalition. The Coalition provides a forum for nineteen like-minded governments from five continents to coordinate efforts to advance Internet freedom. The Coalition works with civil society and the private sector in a multi-stakeholder process to support the ability of individuals to exercise their human rights and fundamental freedoms online. I view the Freedom Online Coalition as a great venue for addressing Internet Freedom and human rights issues with our partners. It can also be a useful venue to consider broader cyber policy concerns that have an Internet Freedom nexus. These fundamental freedoms that form the core of our Internet Freedom policy are also the foundational principles for our cyber policies writ large.

The Department of State works closely with the interagency to further these five principles in an array of international engagements. The U.S. engages on cyber issues with a multitude of states, bilaterally and in regional groups. For example, we are working with our European allies, both with the European Union and in NATO. The European Commission recently launched their cybersecurity strategy, and at last year's Chicago Summit, NATO leaders reaffirmed their commitment to improve the Alliance's cyber defenses. We coordinate very closely with our partners around the world and in the last year alone, we have launched dedicated cyber whole-of-government senior policy dialogues with India, Brazil, South Africa, South Korea, Japan, and Germany to share perspectives and build a consensus view on the future of cyberspace. We continue to seek deeper engagement with countries like Russia and China who may have a different world view but with whom we need to find ways to develop stronger relationships. Through these engagements, we leverage the widespread global public support for an open Internet to champion the multi-stakeholder model with emerging global leaders.

The U.S. government has challenged and persuaded other states to focus on cybersecurity as a critical policy issue. That work goes back many years and includes several UN resolutions on cybersecurity and capacity building. My office was the first of its kind in a foreign affairs agency, and since its creation, many countries have created similar positions and offices in their own foreign ministries as they recognize cyber as a new foreign policy imperative.

The State Department has effectively mainstreamed rapidly-developing cyber policy issues across our regional and functional bureaus, and integrated cyber within our international engagements. We have created internal coordination mechanisms to draw from a range of expertise in the formulation of cohesive and balanced policy. We have also helped our diplomatic posts establish diplomatic cyber points of contact – a corps of cyber attachés if you will – as well as form interagency country teams on cyber issues to communicate globally the U.S. vision of cyberspace and cybersecurity.

The State Department will continue to focus on both the kinds of operational threats you've called us here today to discuss, and on the long-term policy efforts that will help to mitigate them in the long run. In his confirmation hearing, Secretary Kerry cited the importance of "cyber-diplomacy and cyber-negotiations," stressing the need to affirm "rules of the road that help us to be able to cope" with challenges in cyberspace. State is doing just that, working with other nations on efforts that will not only contribute to greater stability and security in cyberspace, but will also protect freedom of expression, ensure opportunity to innovate, and promote economic growth around the world.