Association for International Affairs
Prague Transatlantic Talks 2014: Facing the Atlantic Cyber Challenge

In recent decades, the world has benefited tremendously from the Internet's rapid growth. In the words of Secretary Kerry, it "has linked us all in a human chain that spans the globe." The Internet has generated new methods of doing business, transformed the ways that individuals communicate, and offered new channels for people to organize and express themselves.

At the same time, we have become increasingly aware that these new benefits do not come without challenges. As we all become more dependent on the Internet, we also become more vulnerable to online threats. Indeed, President Obama has called it the "great irony of our Information Age" that "the very technologies that empower us to create and to build also empower those who would disrupt and destroy." Accordingly, government-sponsored economic theft, threats to critical infrastructure, and of course, the dangers of cybercrime have all risen to the top of the policy agenda. At the same time, the growth of the Internet worldwide has intensified debates on how cyberspace should be governed. And we have also seen increasing efforts by repressive regimes to undermine human rights online because they see the open Internet as a threat to their stability.

These challenges raise an important question. How do we make this prodigious new technology—whose ultimate potential we have still yet to fully grasp—one that all of us can safely depend upon?

The United States has a vision for doing this. It is rooted in the International Strategy for Cyberspace, which the White House released in May 2011. The International Strategy, the first of its kind in the world, articulates the U.S. vision of cyberspace as "a place where the norms of responsible, just, and peaceful conduct among states and people have begun to take hold," and commits to "an international cyberspace policy that empowers the innovation that drives our economy and improves lives here and abroad." Most important, the International Strategy reflects our conviction that if all the nations and people of the world are to reap the tremendous political, economic, and social benefits that cyberspace offers, cyberspace must be open, interoperable, secure, and reliable.

At the same time, we recognize that to achieve our vision, our efforts must be multifaceted. This is not only a technical endeavor. It requires that we develop and stitch together a panoply of institutions, norms, and cooperative mechanisms. It requires, among other things, a concerted diplomatic effort, which is why my office was stood up at the State Department just over three years ago.

Our goal, now as when the International Strategy was released, is to work with that large community of like-minded governments and other stakeholders that support the notion of an open, interoperable, secure, and reliable Internet as the best way to realize the Internet's economic and social benefits.

The State Department is working to promote these principles in six areas:

The first is international security in cyberspace. Some cyber threats have the potential to constitute threats to national security. It is in this arena – of potential large scale threats to national security – where states have an important role to play. The United States has concluded that the international

community needs to strive for a state of "international cyber stability"; a more peaceful environment where all states are able to positively exploit the benefits of cyberspace; where there are benefits to state-to-state cooperation and avoiding conflict and little incentive for states to attack one another. We are pursuing efforts in two areas to achieve this goal.

First, we are working to develop a shared understanding about norms of acceptable state behavior in cyberspace, which will help enhance stability, ground foreign and defense policies, guide international partnerships, and help prevent the misunderstandings that lead to conflict.

In recent years, we have had tangible successes in developing these norms. The 2013 UN Group of Governmental Experts—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. This means that the same international legal principles that have promoted predictability and stability between states during conflict in the kinetic space, such as the UN Charter and the law of armed conflict, apply equally in cyberspace. The group also reached consensus on several other key issues: an affirmation of the applicability of the law of state responsibility to cyberspace, the important role of confidence building measures, and the vital importance of capacity-building to enhance global cooperation in securing cyberspace. And, the Group agreed that the combination of all these efforts support a more secure cyberspace. At the next UNGGE, beginning in July, we intend to build on this important consensus and look more closely at how international law applies to state-on-state conduct in cyberspace during conflict.

Second, our international security work has also focused on the establishment of practical cyber risk reduction and confidence building measures. We have worked to reach agreement on 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 last year, at the ministerial of the Organization for Security and Cooperation in Europe, we achieved an agreement among the 57 participating states for the first ever cyber CBMs for a multinational security organization. These regional measures seek to enhance interstate cooperation, transparency, predictability, and stability. Over the coming year at the OSCE, we will work with the participating states to implement these initial CBMs while also developing additional cooperative measures. And we are also pursuing the development of cyber CBMs in other regional organizations, such as the ASEAN Regional Forum, where there is a great appetite for a regional approach to address common cyber challenges. We envision a future of greater stability and cooperation where all states are connected through these risk-reduction measures.

The second area where we work is Internet Governance. This is the emerging front in the struggle for openness in cyberspace. The United States and many others in the international community support the existing, inclusive multistakeholder model of Internet governance. Other states seek to establish intergovernmental oversight mechanisms for the technical management of Internet resources and operations. The politics of intergovernmental control would upend the currently successful model of governance, leaving non-governmental stakeholders disenfranchised. Any mechanism involving total government control over Internet policy would inevitably enshrine restrictive rules and regulations and help legitimize the kind of censorship and content control exercised by repressive regimes. The United States opposes these efforts to shift Internet governance to a top-down, intergovernmental model. As part of our efforts, we are working to promote more diverse representation by governments and other stakeholders at multi-stakeholder

institutions, building multi-stakeholder capacity to participate in the process, and supporting efforts to further internationalize governance functions. We have also successfully opposed efforts to create a top-down, state-driven, UN-style mechanism for Internet management in venues like the ITU.

I am pleased to note that in recent months there have been a number of important developments in this area. First, in March, the U.S. Government affirmed its commitment to the multi-stakeholder model of Internet governance by formally announcing our intention to transition key domain name functions—known as the IANA functions—to the global multistakeholder community.

Then, last month, the U.S. participated in the NETmundial conference in Sao Paolo, Brazil, a global meeting of governments, entrepreneurs, academics, Internet institutions, civil society activists and users to discuss the future of Internet governance. This conference also represented a success. To the surprise of some, and to the dissatisfaction of the authoritarian regimes who also attended the meeting, a substantial majority of NETmundial's global participants successfully supported freedom and inclusion over government control of the Internet. Standing on equal footing, we agreed on the use of the multistakeholder model for overcoming challenges as our first principle, and outlined other principles Internet governance should embrace.

The third area is promoting Internet Freedom. In the past years, threats to internet freedom have grown, as a look at some of the independent reports out there, like those written by Freedom House or Reporters without Borders, clearly show. In fact, according to data from the OpenNet Initiative, 960 million Internet users live in countries that impose illegitimate restrictions on content—that's 47% of all Internet users. For this reason, it is more important than ever that the U.S. Government continues work to ensure the ability of individuals worldwide to exercise their fundamental freedoms online. This involves: (1) promoting the existing consensus that international human rights obligations and commitments apply to online activity; (2) providing support for individuals facing repression online and bolstering civil society roles in Internet policymaking processes; and (3) encouraging companies to adopt practices and policies that respect human rights online. I am happy to say that we have had some important successes in recent years.

We were part of the core group of supporters of the 2012 UN Human Rights Council resolution 20/8, which affirmed that the rights that people have offline also apply online. The resolution was adopted by consensus and is now the clearest statement from the world's governments in support of Internet freedom.

In addition, we were instrumental in the launch of the Freedom Online Coalition in 2011. This is a group of governments committed to taking concrete action in support of Internet freedom. The group has organized annual conferences to discuss pressing issues, and it also serves as a vehicle for coordinating efforts at international venues where there might be Internet Freedom implications. And the group is continuing to grow; since its launch it has expanded to include 23 governments, from all regions of the world.

Just a few weeks ago, I attended the most recent annual meeting of the Freedom Online Coalition in Tallinn, Estonia. There, the Coalition adopted the Tallinn Agenda, a powerful document in which Coalition members, among other things, dedicated themselves to respecting five principles that help distinguish legitimate practices of states from the illegitimate practices of states that use online tools to repress their people. Those principles are "rule of law, legitimate purpose, non-arbitrariness, effective oversight, and transparency." In addition to enumerating these principles, the Tallinn

Agenda also included reaffirmation of support for an open Internet and multistakeholder governance, as well as commitments to support technologies that enable human rights online and condemn governments that violate those rights.

But for me, one of the highlights of the entire conference was on the first day, when Secretary Kerry gave remarks via live video chat. He closed those remarks by saying that "we need to each stand for an open, secure, and inclusive Internet, and we each must work for the day when we are bound together not only by the humanity that ties us all together, but by the freedoms that for too long have been the province of too few. That's our mission."

The fourth area is combating the serious threat posed by the explosion in cybercrime, a topic near and dear to me from my previous life as a criminal prosecutor with the Department of Justice. Cybercrime is a transnational scourge that has cost the global economy, by some estimates, billions of dollars, and has reduced public trust in the Internet. Some states believe that the answer to the cybercrime phenomena is to promote a new UN treaty, which would take years to negotiate, be unlikely to result in anything of greater utility than the Budapest Cybercrime Convention to which the U.S. and forty other countries are parties, and potentially sideline many ongoing and effective efforts to build international capacity to tackle high-tech crime.

We believe the Budapest Convention provides a strong basis for our fight against cybercrime, while also protecting fundamental human rights. It identifies the three elements needed for effective cybercrime legislation, namely: (1) strong and harmonious substantive cybercrime laws; (2) comprehensive investigative tools for addressing high-tech crime and conducting digital forensics; and (3) effective mechanisms for both formal and informal international cooperation, like the G-8 24/7 Network.

Diplomatically, promoting accession to the Budapest Convention and participation in the G-8 24/7 Network is a key priority for the U.S. We are heartened to see regionally diverse countries like Japan, Australia, the Dominican Republic, Mauritius, and Panama becoming parties to the Convention in the last two years, with many more countries – including Senegal, Colombia, Costa Rica, Morocco, and Israel in the process of joining.

The U.S. Government is also committed to strengthening international cooperation in the fight against cybercrime by modernizing the mutual legal assistance treaty process. In January, the President highlighted improving the MLAT process as a priority for his administration for fiscal year 2015. He committed to devoting the resources necessary to improve the process while maintaining high privacy standards. We hope the US Congress will fund this initiative. At the same time, our foreign partners need to do their part to help improve the process, by developing experts and specialists and empowering their people to work with us so we can help them navigate the MLAT process and meet US legal standards.

But we also recognize that many countries need help with this fight, and so we are strongly supporting capacity building efforts to enhance states' ability to fight cybercrime and address the exponential growth in digital evidence in all criminal investigations. The State Department is working with our interagency partners such as the Departments of Justice and Commerce, as well as the private sector and key international partners and institutions to eliminate cybercrime havens wherever they may exist.

We firmly believe that the battle against transnational cybercrime is one we can and will win.

The fifth area is ensuring that nations perform their cybersecurity due diligence. Here, working closely with DHS as well as the rest of the interagency, we are strengthening relationships with other countries as we cooperate on cybersecurity issues of mutual concern. This includes efforts to enhance collaboration on network defense, incident management and recovery, and supporting the development of those capabilities where needed. It also involves enhancing participation in and strengthening of existing regional and global cybersecurity fora.

- For example, the State Department has been a big supporter of greater international CERT-to-CERT cooperation and CERT experts are often a part of our international delegations.

- We also use our diplomatic channels to support the Administration's information sharing efforts, helping to draw the attention of foreign policy makers to the need for cooperation on specific cybersecurity threats of serious concern. For instance in the 2012-2013 timeframe, when the public-facing websites of US financial institutions suffered botnet attacks from infected computers around the world, the United States reached out, using both technical and diplomatic channels, to share information and obtain assistance.

- At the same time, as noted, the U.S. Government works in partnership with countries to develop their capacities to carry out effective due diligence. Through this work, we have developed an innovative and holistic approach to cyber capacity-building that focuses on five areas: (1) Development of national cyber strategies; (2) increasing public-private partnerships to manage cyber risk and share knowledge; (3) deterring cybercrime by updating criminal laws, procedures, and policies; (4) developing incident management capabilities, such as CERTs; and (5) building a culture of cybersecurity. Using this model, the U.S. Government has provided a number of regionally-based capacity building training sessions. For example, in the last few years we have held three workshops in eastern and western sub-Saharan Africa, and we are currently planning a fourth workshop to be held next month in Botswana for member states of the Southern African Development Community.

The final area is State's work to promote the Internet, and cyberspace more generally, as an engine of economic growth. The Internet has proven to be a major catalyst for economic development around the world. The State Department is supporting efforts to bridge the digital divide so that an open, interoperable, secure and reliable Internet can be an engine for growth in even the poorest regions of the world. The State Department has provided support both through its diplomatic efforts and its support for the Alliance for Affordable Internet, a coordinated public-private-civil society voice advocating policy and regulatory best practices for expanding affordable access to the Internet. Moreover, USAID has also taken a lead in providing technical assistance and capacity building through its Global Broadband and Innovation Program and through its Mobile Solutions team in the Global Development Lab.

So, to sum up, the United States has a vision for achieving an open, interoperable, secure, and reliable Internet. We believe that achieving this vision requires efforts on a number of different fronts and that diplomatic efforts will be central to our success. As the International Strategy puts it, "international collaboration is more than a best practice; it is a first principle."