INTERNATIONAL SECURITY

GOALS AND PRIORITIES

- Seek common understanding on cyber issues and activities of critical national and international significance
- Promote international stability, transparency, and confidence in cyberspace
- Promote the growing international consensus on the applicability of existing international law to cyberspace
- Establish and implement bilateral and regional cyber confidence building and transparency measures to reduce the risk of conflict
- Promote cooperative international partnerships to mitigate and deter cyber threats

"The basic rules of international law apply in cyberspace. We also support a set of additional principles that, if observed, can contribute substantially to conflict prevention and stability in time of peace. First, no country should conduct or knowingly support online activity that intentionally damages or impedes the use of another country's critical infrastructure. Second, no country should seek either to prevent emergency teams from responding to a cybersecurity incident, or allow its own teams to cause harm. Third, no country should conduct or support cyber-enabled theft of intellectual property, trade secrets, or other confidential business information for commercial gain. Fourth, every country should mitigate malicious cyber activity emanating from its soil, and they should do so in a transparent, accountable and cooperative way. And fifth, every country should do what it can to help states that are victimized by a cyberattack.

— Secretary Kerry, An Open and Secure Internet: We Must Have Both, Korea University, Seoul, Republic of Korea, May 18 2015.

CONTEXT

More than 100 states are developing military cyberspace capabilities—a prospect that is increasingly viewed as threatening both our national security and international security. Key aspects of cyber tools—such as the difficulty of attributing an attack to its perpetrators or sponsors and the dual-use nature of the technology—are seen by many as inherently destabilizing. While emphasizing that existing international law applies to state behavior in cyberspace, the Department of State has pioneered the promotion of a framework of shared norms based on concepts drawn from existing international law to guide state behavior in peacetime, and the promotion of practical confidence building measures to reduce risk, with the objective of establishing a coalition of states in support of that framework.

CYBER DIPLOMACY

Norms of State Behavior in Cyberspace

The United States has promoted shared understandings of appropriate state cyber behavior bilaterally and in numerous international venues, including the Group of Seven (G7), the Organization for Security and Cooperation in Europe (OSCE), and the United Nations (UN) General Assembly. At these venues, the United States has sought to achieve common understanding on cyber issues of critical national and international significance, in

particular that: states should promote international stability, transparency, and confidence in cyberspace; existing international law applies to state behavior with regard to the use of cyberspace; and the international community should help build the cybersecurity capacity of less-developed states. In 2013, the UN Group of Governmental Experts (GGE)—a group that included representatives from China, Germany, India, Japan, Russia, and other cyber powers—agreed to a consensus report that was a landmark achievement. The 2013 GGE Report included a clear affirmation that international law, and especially the UN Charter, is applicable in cyberspace. In addition, the group agreed that confidence-building measures, such as high-level communication and timely information sharing, can enhance trust and assurance among states and help reduce the risk of conflict by increasing predictability and reducing misperception. The Group also agreed on the vital importance of capacity-building to enhance global cooperation in securing cyberspace and reaffirmed the importance of an open and accessible cyberspace, as it enables economic and social development. And, the Group agreed that the combination of all these efforts supports a more secure cyberspace.

This year, the UN GGE took a step forward in its report by highlighting that the UN Charter applies in its entirety, thereby affirming the applicability of the inherent right to self-defense as recognized in Article 51 of the Charter, and noting the applicability of the law of armed conflict's fundamental principles of humanity, necessity, proportionality, and distinction. In addition, the experts recommended a number of voluntary norms designed for peacetime. These included several norms long championed by the United States, such as the protection of critical infrastructure, the protection of computer incident response teams, and cooperation between states in responding to appropriate requests in mitigating malicious cyber activity emanating from their territory. Another recommended norm calls on states to seek to prevent the proliferation of cyber tools that can be used for malicious purposes. All of these measures, if observed, can contribute substantially to conflict prevention and stability in times of peace.

The United States is continuing to elaborate on these concepts especially regarding key areas of risk that are of concern to all states. We are working internationally to build agreement on norms of responsible behavior that apply to the everyday challenges of cyber disruptions, cyber-enabled theft, and cyber attacks that fall below the threshold of the use of force. We have used existing, relevant principles and concepts with support in the international community to articulate cyber norms of appropriate state behavior during peacetime that apply to these types of risks in cyberspace.

CYBER CONFIDENCE BUILDING MEASURES

In addition to our norms-focused work at the UN GGE, the United States has pursued regional agreement on cyber confidence building measures (CBMs). In 2013, we had success at the OSCE in establishing a set of 11 practical, regional CBMs focused on transparency measures, including the sharing of national strategies and points of contact. The CBMs also leverage the OSCE as a communication platform for participating States to seek information or assistance when cyber activity appearing to emanate from other states becomes a national security concern. The United States is pursuing similar work in the Association of South East Asian Nations (ASEAN) Regional Forum (ARF).

Some countries have posed significant challenges to our efforts as they try to win support for their vision of a more state-centric, restrictive cyberspace. While it is clear that we will continue to have a different position from such countries on issues such as the role of states in Internet governance and how states approach regulation of the online activities of their citizens, we believe that constructive engagement will contribute to greater international cyber stability and improved bilateral understanding of our approaches, intentions, and actions in cyberspace.

Office of the Coordinator For Cyber Issues (S/CCI)
United States Department of State

DESIGNED AND PRINTED BY A/GIS/GPS
AUGUST 2015