February 2013

Cybersecurity Norms

Key Points

- The private sector, with its global supply chain and customer base, can make an important contribution to the emerging discussion of cybersecurity norms.
- As governments continue to develop their views on cyber security and normative behavior in cyber space, creating international public-private partnerships can help ensure the resiliency of critical infrastructures and agility in responding to complex security events in cyber space.

BACKGROUND

"The last two decades have seen the swift and unprecedented growth of the Internet as a social medium; the growing reliance of societies on networked information systems to control critical infrastructures and communications systems essential to modern life; and increasing evidence that governments are seeking to exercise traditional national power through cyber space." [1]

The technology landscape in cyber space is indeed changing rapidly, but agreed-upon standards for state behavior have not kept pace—which in turn raises concern about potential conflicts. (According to the United Nations, more than 30 countries have developed military doctrines related to the use of cyber space and some have developed cyber defense centers.) Developing a global understanding of cybersecurity norms will be critical to the long-term stability, reliability, and security of the Internet and cyber space.

To date, most international discussions on cyber security have taken place among governments through such organizations as the United Nations Government Group of Experts and the Organization for Security and Cooperation in Europe.

However, the technology industry creates and operates most of the infrastructure that enables the Internet today. Industry continues to innovate, build best practices, and set technical cybersecurity norms. These include managing the disclosure of software vulnerabilities, implementing the secure development of software and hardware, swift responses to security incidents, and management of security risk. And during actual cyber incidents, it is the private sector that is critical to effective incident response, often relying on trusted communities of engineers, network operators, and other experts from outside of government.

Global conversations on cyber security would benefit from a private sector perspective that can help governments think through the technical challenges and priorities involved in securing billions of Internet users around the world. Many industry practices could be used as the impetus for public-private partnerships to develop cybersecurity norms, because neither governments nor the private sector can address these challenges alone.

[1] *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, The White House, May 2011.
aka.ms/WhiteHouse-cyberspace

MICROSOFT APPROACH

- Microsoft is committed to supporting discussions on the evolution of cybersecurity norms through partnerships. As governments continue to develop their views on cyber security and normative behavior in cyber space, creating international public-private partnerships can help ensure the resiliency of critical infrastructures and agility in responding to complex security events in cyber space.
- The Microsoft Global Security Strategy and Diplomacy team partners with national governments, industry partners, and nonprofit organizations to contribute to the international discussion of cybersecurity norms.

POLICY CONSIDERATIONS

- **Appropriate forums**. Effective discussions to develop cybersecurity norms take place when governments identify appropriate forums for such discussions. The membership of these forums must include the relevant government stakeholders, have the ability to integrate input from the private sector, and have the expertise necessary to sustain meaningful progress.
- **Public-private partnerships**. To be effective, governments must develop cybersecurity norms in collaboration with the private sector, which owns the majority of today's global networks. Although governments are the primary actors in international negotiations, the private sector can contribute considerable operational experience to help inform their discussions.
- **Focus on consensus**. Governments should focus on areas where achieving consensus in the short term is practical. For example, it may make sense to seek agreement on areas of specific common interest, such as how to deter threats to critical infrastructures, before discussing areas complicated by significant national and cultural differences.

Helpful Resources

Microsoft Global Security Strategy and Diplomacy
www.microsoft.com/security/gssd

Cybersecurity Norms and the Public Private Partnership: Promoting Trust and Security in Cyberspace
aka.ms/norms-public-private

Cybersecurity Norms for a Secure Cyber-Future
aka.ms/Secure-cyber-future

Developments in the Field of Information and Telecommunication in the Context of International Security (UN First Committee)
aka.ms/UN-cyber-security