Policy recommendations

International cybersecurity norms

The opportunity

As the transformational power of cloud computing comes into focus, there are growing concerns about the rise of cyberspace as a battlefield for cyberconflicts and a conduit for attacks launched by governments and their proxies. As a result, there is increasing urgency to develop and implement cybersecurity norms that provide clear international expectations for preventing and managing conflicts in cyberspace.

Establishing international cybersecurity norms is an essential step in protecting international and national security, maintaining trust in technology, and protecting the stability of the connected global economy.

The challenge

Until recently, most work to develop cybersecurity norms has focused on conceptual discussions about the rights and responsibilities of nations. Now the movement is towards more concrete proposals for cybersecurity norms. This is especially evident as policymakers, advocates from the public and private sector, academia, and civil society propose a wide range of more specific ideas for how to address the challenges raised by the exploitation of technology for conflict.

Many of these proposals recognize that nations should not permit malicious cyberactivity to be launched from within their borders, and that critical infrastructure should not be considered valid targets in times of peace. So far there has been only limited progress. In addition, not enough attention has been paid to the critical need for the public and private sectors to work together to protect technology systems and infrastructure from attack.

Policy recommendations

The process for developing and implementing international cybersecurity norms continues to evolve as technology advances, stakeholders change, the implications of potential policies are explored, and new forums for discussion emerge. Fundamentally, however, the success of cybersecurity norms will be determined by how they are implemented and when and how violators are held accountable. This means it is critical for governments to be proactive and collaborative in contributing to and evaluating cybersecurity norms and determining how to make them effective and enforceable. Governments can most effectively achieve these goals if they take into account the following recommendations:

Increase efforts toward agreement on globally accepted cybersecurity norms. While there are signs of alignment around a small number of cybersecurity norms, the urgency to move forward remains. Nations must understand the potential outcomes of their actions in cyberspace and continue to work to agree to norms for improving defenses and limiting conflict and offensive operations. If we are to avoid the potentially catastrophic effects of cyberwarfare, continuous engagement is essential.

Provide avenues for private-sector input and involvement. Input from the global ICT industry is critical to ensuring that the language of cybersecurity norms accurately reflects the realities of defending technology users at global scale. It is important to establish appropriate venues and clear processes for the private sector to contribute. In addition, industry is in the best position to utilize information about tactics, techniques, procedures, and indicators of compromise to strengthen defenses for technology users worldwide.

Explore the opportunities and challenges associated with using an independent body to assist with attribution and verification. The successful development of cybersecurity norms will require new forms of cooperation and new mechanisms for dealing with politically sensitive allegations such as attribution. Governments and the private sector need a forum where they can provide evidence to support technical attribution and obtain validation through rigorous peer review. One model that has worked is the nuclear and chemical warfare realms. This provides a model for future cybernorms verification.

Evidence and further reading:

United Nations Group of Governmental Experts Report: "Developments in the Field of Information and Telecommunications in the Context of International Security"

Microsoft Proposed Norms: "International Cybersecurity Norms: Reducing Conflict in an Internet Dependent World"

Microsoft White Paper: "From Articulation to Implementation: Enabling Progress on Cybersecurity Norms"

Microsoft White Paper: "Governments and APT: The Need for Norms"

For links to these and other resources, please visit:
http://www.microsoft.com/cloudforgood