International Cybersecurity Norms

Microsoft Policy Papers

The case for international cybersecurity norms

As societies expand their digital footprint, increasing connectivity among citizens, businesses, and governments, the world has also seen a concomitant increase in cyber incidents. At times, the attackers' motivations are financial, not unlike criminal behavior in the "physical world." The past several years have shown a new trend. Increasingly, states use the Internet to advance tried and true tenets of intelligence or even military operations: espionage, reconnaissance, and even sabotage. As the pace of activity in cyberspace increases, so does the likelihood of one state misinterpreting the actions of another. Moreover, the risk of a cyber-arms race cannot be discounted.

As more nation states include offensive and defensive cyber capabilities in their intelligence and military planning, there are few international rules to guide or constrain the use of such capabilities. Offensive cyber activities in particular have the potential for unintended consequences including the possible escalation of hostilities from cyberspace to the physical world. In today's internet dependent world this represents an unacceptable risk. It would be naïve to hope that states should fully pull back their military operations from the Internet. Nevertheless, just as there are universally accepted norms of behavior in other realms of conflict, it is no less important to establish norms for cybersecurity. These norms should not only strengthen cybersecurity but also preserve the values of a globally connected society.

As such, norms should define acceptable and unacceptable state behaviors, with the aim of reducing risks, fostering greater predictability, and limiting the potential for the most problematic impacts, including (and in particular) impacts which could result from government activity below the threshold of war. We conceptualize at least two types of norms:

- Norms for improving defenses, which can reduce risk by providing a foundation for national cybersecurity capacity and for domestic, regional, and international organizational structures and approaches that increase understanding between states;
- Norms for limiting conflict or offensive operations, which will serve to reduce conflict, avoid escalations, and limit the potential for catastrophic impacts in, through, or even to cyberspace.

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

Six proposed cybersecurity norms to limit conflict

In light of the growing number of offensive capabilities, Microsoft believes that cybersecurity norms are needed to limit potential conflict in cyberspace and to better define what type of government behaviors in cyberspace should be "out of bounds" so that events don't escalate to warfare. These norms should not only be designed to strengthen cybersecurity but also to preserve the utility of a globally connected society.

We believe that if cybersecurity norms are to be effective, they have to meet four key criteria. First, they must be practicable. They also need to reduce risks of complex cyber events and disruptions that could lead to conflict. In addition, they need to drive behavioral change that is observable and that makes a demonstrable difference in the security of cyberspace for states, enterprises, civil society, and individual stakeholders and users. Finally, effective norms should leverage existing risk-management concepts to help mitigate against escalation, and, if escalation is unavoidable, they should provide useful insight into the potential actions of involved parties.

To help catalyze progress on the development of effective cybersecurity norms, Microsoft proposes six norms to limit conflict. The proposed norms are intended to reduce the possibility that information and communication technology (ICT) products and services could be used, abused, or exploited by nation states as part of offensive operations that result in unacceptable impacts, such undermining trust in ICT; set boundaries for how cyber weapons are developed, contained, and used; and create a meaningful global framework for managing vulnerabilities. We recognize that norms should not be an objective by themselves. Only if implemented, assessed for accountability, and, as appropriate, evolved, can they drive demonstrable changes in behavior.

NORM 1: States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and service.

NORM 2: States should have a clear principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them.

NORM 3: States should exercise restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable.

NORM 4: States should commit to nonproliferation activities related to cyber weapons.

NORM 5: States should limit their engagement in cyber offensive operations to avoid creating a mass event.

NORM 6: States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.

Helpful resources

International cybersecurity norms, reducing conflict in an Internet-dependent world:

http://aka.ms/cybernorms

Government and APTs: The need for norms

http://aka.ms/rethink2