International cybersecurity norms

Microsoft Policy Papers

The case for international cybersecurity norms

Around the world, cloud computing adoption is on the rise. People are recognizing that cloud services offer enormous value and agility and can unlock vast potential for innovation. However, at the same time, there are growing concerns about the rise of cyberspace as the battlefield and as a conduit for other attacks launched by governments and their proxies. There is a growing realization that new technologies' usage and growth depend on the stability of the online environment and on users' trust in the security of cyberspace.

As a result, there are growing demands for the development of cybersecurity norms to provide a clear set of international expectations regarding "rules of the road" for nation states engaged in cyber conflict. Establishing international cybersecurity norms is an essential step in protecting national security in the modern world, maintaining trust in services provided online, and ultimately ensuring the continued prosperity of the modern economy. However, until recently, most of the global dialogue on cybersecurity norms has taken form of conceptual discussions about the rights and responsibilities of nations.

Today the movement is toward more concrete proposals for cybersecurity norms. Policy makers, experts, and advocates from governments, the private sector, academia, and civil society are putting forward a wide range of specific ideas for how to address the challenges raised by cyber conflict, particularly how to address the potential exploitation of commercial information technology (IT) systems. While these proposals vary, many recognize that nations should not permit malicious cyber activity to be launched from within their borders, and that critical infrastructure should not be perceived as a target in times of peace. So far, however, proposals have yielded few concrete results and critically have failed to fully acknowledge and realize the need for the public and private sectors to work together to protect technology systems and infrastructure from attack.

The development and implementation of international cybersecurity norms has not been, and is not going to be, a clean or linear process. The relevant stakeholders, implications of potential policies, and indeed, the very technologies themselves are still evolving. The fora that established themselves as forward-leaning on this topic have emerged organically, sometimes on a regional, sometimes on a bi-lateral or multilateral basis. However, critical to the success and impact of any cybersecurity norms will be their implementation and to what degree violators are held accountable. Therefore, governments need to proactively engage and be both collaborative and flexible when they contribute to and evaluate emerging cybersecurity norms, and when they determine how to make them effective and enforceable.

Governments should consider the following recommendations as they embark on this path:

- Increase efforts towards agreement on globally accepted cybersecurity norms. While the international community should be encouraged by the increasing alignment around a small number of cybersecurity norms, it is important not to become complacent. Nations need to understand the potential outcomes of their actions online and work to reach agreement around norms for improving defenses, as well as those focused on limiting conflict or offensive operations. Only continuous engagement in this arena will help the world avoid escalations and limit the potential for catastrophic impacts in, through or to cyberspace.
- Engage collaboratively with the private sector. Input from the global technology industry and also academia, and civil society is critical to ensuring that cybersecurity norms accurately reflect the practical realities of defending technology users at global scale. Governments should therefore work collaboratively

with the private sector to help ensure that the norms that are developed can also be implemented. It is therefore important that appropriate venues are established with a clear process for contributing to norms development and implementation, particularly with regard to the technical elements of attributing acts to actors.

- 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 to effectively deal with potentially politically charged challenges, such as those of attribution. A forum, where governments and the private sector can provide evidence to support technical attribution and obtain some level of validation through rigorous peer review, represents a model that has worked previously in other sectors. It is critical that any organization that emerges is structured in a way that promotes global acceptance.

However, norms are not just for governments. Technology users in enterprises and at the consumer level have expectations of the IT industry as well. In this regard, it is important to recognize that the IT industry is not monolithic; not every provider of IT services can be bound by the same rules. Global IT providers, who make global, mass-market products must focus exclusively on protecting users, in order to protect their customers and be successful in the global marketplace. They cannot participate in offensive activities and help one customer attack another. By contrast, there are companies that work for a single government and may be involved in providing IT support for military operations, even helping to build cyber weapons. Clearly, such companies, which take sides in geopolitical conflicts, will be in a different position to global, mass-market suppliers, and may be beyond the purview of these norms.

As governments commit increasing resources to offensive cyber capabilities, the global IT industry must strengthen its resolve, and take active steps to prevent user exploitation through adherence to industry norms. Most notably, companies must be clear that they will neither permit backdoors in products nor withhold patches, either of which would leave technology users exposed. They will also have to address attacks, whatever their source, to protect customers. These industry norms are meant to increase confidence in the global IT supply chain, and to send a clear message to governments that global IT providers will not help exploit IT users, but will rather help protect them.

Helpful resources

From Articulation to Implementation: Enabling Progress on Cybersecurity Norms:

https://mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cybersecurity-Norms_vFinal.pdf

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