Internet Society Approach to Cyber Security Policy

Washington DC, USA; Geneva and Davos, Switzerland – 22 January 2015

The headlines of today regarding hacking, exposure of large quantities of personal data, denial of service attacks, and the continued revelations about pervasive monitoring are deeply disturbing.

The Internet Society believes that with each new cyber-related incident, we risk losing the trust of users who have come to depend on the Internet for many of life's activities. And we believe that we also risk losing the trust of those who have yet to access the benefits of the Internet, thereby discouraging the kind of investment needed to complete the job of connecting everyone in the world.

Public policy can have a positive role to play in meeting the demands of public interest. However, while action is required, all policy initiatives must be both measured and balanced. There is a danger for legitimate policy responses to go too far in addressing security challenges, thereby jeopardizing the very infrastructure that both ties together the global economy and provides the engine for its growth. We are wary of a tendency for government to expand its powers in ways that:

a) may not ultimately be effective; and

b) may further undermine individuals' online privacy.

The technical community has long recognized that the future growth of the Internet hinges on the ability to secure core aspects of Internet infrastructure AND to protect the confidentiality and integrity of the data that flows over it. We continue to play a leading role in these areas.

We note that there have been significant strides made in just the past 18 months within the technical community to secure core aspects of the Internet (such as routing and the Domain Name System) and to empower end users to protect their own information with tools like encryption.

Perspectives on cyber security

Today's cyber security trends are evolving at an overwhelming pace, posing an ever-present threat to our connected world.

At a global and individual level, while everyone talks about "cyber security," it has been our experience that often we do not all mean the same thing. The reality is that because the Internet crosses all sectors of the economy and many aspects of people's lives, we need to recognize the complexity of creating a secure Internet environment.

Security is not achieved by a single treaty or piece of legislation; it is not solved by a single technical fix, nor can it come about because one company or sector of the economy decides security is important. Creating security and trust in the Internet requires different players (within their different responsibilities and roles) to take action, closest to where the issues are occurring. Perspectives on cyber security are far from uniform, for instance:

• Businesses need to safeguard customer information, protect commercial data, or prevent intrusions and damage to their corporate networks.

• Small companies and large companies face very different security issues.

• Users want to be secure and feel threatened about the effects of leakage of personal data.

• Governments have to take into account the concerns of citizens and businesses while also dealing with any national security threats that an Internet attack might pose.

• And, there are differences between developed and developing countries in how they address cyber security. While developed countries might be most focused on securing advanced computing infrastructure or funding cyber security R&D, a developing nation might well be more concerned with developing the technical and policy capacity to deal with online fraud.

It is the legitimate claims of all of these stakeholder groups that explain why it is so difficult to reach consensus on how to define or address cyber security. Any framework for tackling cyber security needs to work from an understanding of the different ways in which the Internet is valuable to its different stakeholders.

The path ahead

From an Internet perspective and in the context of the growing threat vector from hacking, targeted cyber attacks on networks and individuals, and surveillance, the Internet Society’s approach to the development of cyber security policy initiatives is based on the following key considerations:

1. The essential need to ensure international cooperation and cross-border collaboration.

2. The adoption of policies that are based on open technical standards. The Internet would not have had the explosive success it has had if the software that has driven its growth weren't easily adaptable for other purposes on the network. Security solutions that are developed within expert communities—the Internet Engineering Task Force being an example—are more likely to be effective and scalable, and consistent with the Internet's basic principles.

3. The need to develop policies that are flexible enough to evolve over time. We know that the technology is going to change. The solutions need to be responsive to new challenges.

4. The fundamental importance of developing policies using a multi-stakeholder model. This means that effective policies cannot be unilaterally created by government and that all stakeholders must work together.

We believe that within this policy framework, the core critical values of basic privacy protections and the freedom of speech cannot be overlooked.

And finally, as a reflection of the Internet Society's continued commitment to ensuring that the "Internet is for everyone," this approach requires a willingness of those who are developing policy to truly listen to those who are affected by and who design and implement their decisions.