

Legal Aspects of Internet Governance: International Cooperation on Cyber Security

Defining the Problem

Cyber Security is commonly defined as the protection of data and systems, especially those connected to the Internet. While useful in many circles, that definition is narrow and a broader perspective is appropriate for ongoing discussions, especially when considering non-technical issues like the law. Rather than offer an alternative definition, I suggest that the following five qualities be considered in any broad discussion of Cyber Security:

Security	Degree of protection from danger, damage, loss, criminal activity
Stability	Consistency, ability to maintain or restore equilibrium
Resilience	Flexibility, ability to recover from and/or adjust to environmental changes
Reliability	Ability to function as expected under stress
Continuity	Lack of interruption/disconnection

Specifying Solutions

Additionally, we need to consider time, and the requirement that these qualities be supported both in the short- and long-term. Short-term in Internet terms, is measured not in days or weeks but in seconds and minutes. Long-term is not weeks or months but years and generations. The policies and systems we put in place today need to enable rapid if not instantaneous response, yet remain effective for decades to come. They themselves must demonstrate the qualities they are designed to support.

Protecting systems and data on the Internet requires rapid response to complex situations. Those responses are difficult enough when the problem is local or contained within a sovereign border. Data breaches, spam, phishing, or malware attacks that cross national boundaries present significant challenges, yet the requirement for rapid response remains unchanged if we are to support the qualities above. It is essential that we find ways to facilitate rapid response while at the same time protect individual rights.

Implementing Solutions

Our current policies and systems are straining to meet our needs. Data breaches, cyber crime, and malware attacks are on the rise. Some point to these and other “failures” as indicative of a structural deficiency with the overall Internet

Governance model and are calling for change. While change can be beneficial, let's first work within the system before replacing it; evolution before revolution.

Cyber Security, or lack thereof, is a multi-stakeholder, 21st century problem. We should employ 21st century solution problem solving, building on historical models, like volunteer fire-fighting¹, where the fire-fighters freely cross borders; be they public/private or sovereign. For these first responders to be effective, we must ensure that our formal legal frameworks are supportive of collaborative, ad hoc action.

Do our current mechanisms encourage individuals and institutions to offer assistance or are they designed primarily to codify acceptable use/behavior and formal, treaty-based enforcement mechanisms? Remember, that cyber security is not limited to criminal activity, but also encompasses (by my definition) danger, damage, and loss. These can occur either within the law or outside the law, but in either case require attention and action to mitigate impact. In the case of criminal activity, there is the added possibility of an enforcement action, but this alone frequently is not a sufficient response.

Call to Action

What can you do?

- Participate - in fora such as this
- Collaborate - government, business, individuals
- Advocate - in your sphere of influence
- Don't equivocate – encourage expanded use of Internet models

Together we can improve both our individual and collective Cyber Security. There are technical/operational actions, some very simple, that we can take today without the need for further discussion. There is also a need for continued conversation if we are to develop both the formal, treaty-based and ad hoc, collaborative mechanisms required to facilitate Internet first responder activities. Let us continue the dialog and develop innovative Internet-ready and Internet-scale solutions to these complex and vexing issues.

Conclusion

The Internet community has demonstrated an ability to provide a stable, reliable, resilient platform that has facilitated advancements far beyond its original "design goals". It is my firm belief that its unqualified success is in large measure a direct result of the underlying principles employed during its development; openness, inclusivity, collaboration, experimentation, and voluntary adoption. Adherence to these principles has brought us the Internet today and our adherence to them tomorrow will ensure continuity as the Internet evolves to whatever it will be for our children and grandchildren.

¹ Suggested by Vint Cerf during session.