Cybersecurity: Searching for a Common Understanding

27 February 2013

Panellists

- Laurent Bernat, Policy Analyst, Organisation for Economic Co-operation and Development (OECD)
- Liesyl Franz, Office of the Co-ordinator of Cyber Issues at the U.S. State Department
- Malcolm Hutty, President, EuroISPA
- Cornelia Kutterer, Director of Regulatory Policy for Microsoft EMEA
- Derek O'Halloran, Head of Information Technology Industries, World Economic Forum USA
- Patrick Ryan, Public Policy & Government Relations Counsel for Free Expression and International Relations, Google
- Matthew Shears, Center for Democracy and Technology (CDT)
- Moctar Yedaly, Head of the Department of Communications and Post at the African Union

Moderator: Christine Runnegar, Senior Policy Advisor, Internet Society

Remote Moderator: Luca Belli, Doctorant en Droit Public CERSA, Université Panthéon-Assas, Sorbonne University

1. **Summary of presentation and/or debate:**

Please note: this was an information and perspective sharing exercise. The points set out below are a summary of some of the views expressed by the participants on key issues.

Is there a difference between conventional international security and security in "cyberspace"?

Yes and no. A key difference is attribution: it is much more difficult to identify who is attacking you in cyberspace. Established legal principles apply in cyberspace. Many of the same challenges apply. We need confidence to use cyberspace for prosperity.

How would you define "cybersecurity"?

- It is a very popular term today. There are many facets.
- There were a diversity of views at WCIT. If we cannot agree on what cybersecurity is, it becomes increasingly difficult to address with policy measures.
- Policy measures that are premised on stopping bad things, rather than protecting what is valued, provide no guide as to how far those measures should go.
- If we are not careful, the spectre of cyber threats can be used as a vehicle for control of networks and how they are used.
- We need to integrate strategies for cybersecurity with strategies for other goals, such as digital growth.

- It is important to have rigour in definitions and break cybersecurity down into its component pieces.

Some definitions:

- Cybersecurity is not one issue and is not necessarily a helpful term. People use the term to talk about various harms that, in other contexts, we treat as distinct: warfare, crime, terrorism, activism, (corporate) espionage etc. If we take the cyber element away, we would not expect a single conversation, body or governance mechanism to solve all of these issues, so why should we expect this just because they are perpetuated through digital means?
- How you manage security risks in the Internet economy in a way that fosters economic and social prosperity (and that does not inhibit economic and social development).
- Protecting that which you value rather than stopping that which you oppose (i.e. incorporate what you are trying to protect into your concept of security).
- It is about building trust and confidence in cyberspace using a mix of policy, law and regulation.
- In many situations, this is not such a useful term. A better overarching term is "cyber-resilience". It captures the idea that you embed your strategy within your view of that which you are trying to protect or achieve.
- There are important linguistic and cultural aspects too, since "security" in many languages implies only physical security, and adding terms like "robustness" do not always translate well.
- "It is a journey not a destination".
- Perhaps we do not want to constrain cybersecurity to a static definition, but rather as a state with desired characteristics that provide guidance and have the flexibility for the ever-evolving environment.
- A number of nations equate cybersecurity with "information security", but the term "information security" often implies censorship as an additional measure.

What are the dynamics of cyber-threats and cyber-risks? What are new/most prominent threats that nations face, and the international community as well?

- The volume of data and how we share data
- The Internet has become indispensible to our daily life
- Some profound changes have led to a new landscape that we still do not fully understand. For example: services and facilities range across jurisdictions, making it more difficult for traditional mechanisms based around the nation state to operate; cloud services (outside of your direct control; reliance on third-parties; challenging to verify the level of protection the services provide); "de-perimeterisation"; Bring Your Own Device (BYOD) culture.
- Threat of mistaken policy – problems caused by bad choices

Threats and risks are very different. Approaching cybersecurity from the risk perspective, rather than an threat perspective, is more holistic and is a more constructive approach for developing policy; because naturally, there are benefits to taking risks that need to be factored in.

Approaches will need to differ depending on the threat vectors. For example, one approach to target cyber criminal activity is to disrupt the business models underpinning that activity.

In addressing cybersecurity as a global community, what are we doing well and what needs improvement?

- There is insufficient cross-border and cross-stakeholder sharing of information about cyber threats and risks. We need to improve coordination and collaboration.
- We need to have open multi-stakeholder approaches to make informed and nuanced decisions. We also need a dialogue with all stakeholders to reach a common understanding on aspects of cybersecurity and/or on where our disagreement lies. This could lead to the development of a shared set of high-level principles and consensus on acceptable behaviour in cyberspace.
- Competencies and skills need to be enhanced by working together and learning from each other.
- Awareness levels are rising; this is positive.
- We need a more harmonised approach or policy interoperability, but there should be better use of existing legal norms.
- It is important to consider cybersecurity in terms of the value we want to protect, and where possible to choose strategies that enable and empower. We need to challenge the idea that security has to be a trade-off between that which you want to do and having an acceptable level of security. We also need to look for opportunities to mitigate risk through greater empowerment.
- In developing global solutions, we need to keep in mind all the governance arrangements that are available, not just treaties, and that there are cultural and other differences between countries. (Compared to trade we have very little experience in dealing with cybersecurity and, as yet, we do not agree on what should/should not be protected.)
- States do not have to choose between security and freedom of expression.
- We cannot imperil fundamental human rights for the sake of security.
- Cybersecurity is only one aspect of security for development. For example, children need to be safe to go to school to learn.
- We need to engender “cyber optimism”.
- The choice to employ “Resilience by design” and “security by design” need to be decided on a case-by-case basis. Consideration needs to be given to whether this is appropriate, because the constraints could, contrary to expectations, work against what we are trying to protect.
- There is an important role for UNESCO in its educational mandate to educate users about cybersecurity and foster a cultural shift towards shared responsibility.

Recommendations from the session.

"We invite all stakeholders to work together to better understand cyber threats and risks, and through cooperation and mutual assistance to develop policies and strategies that enable innovation, economic growth, and preserve the fundamental principles of the open Internet."