# Position paper on cybersecurity developments within the UN context

*FIRST's contribution to the UN Open-ended Working Group on developments in the field of information and telecommunications in the context of international security*

## I. About FIRST

Founded in 1990, the Forum of Incident Response and Security Teams (FIRST) consists of Computer Security Incident response teams (CSIRTs) from more than 500 corporations, government bodies, universities and other institutions across 94 countries. It promotes cooperation among computer security incident response teams, which are sometimes referred to as the "fire brigade" of the internet and are the first ones to respond to major cybersecurity incidents. For more information, visit https://www.first.org.

## II. Major threats to cybersecurity

In the context of internet development, and international security and stability, FIRST sees the following three key areas of challenge ahead:

- **Deepening technical interdependence**

Ever fewer organizations have the ability to run all parts of their technology stack themselves, and increasingly rely on standards and technologies developed and operated by others. In addition, code and data is increasingly shared between organizations. This deepening integration leads to significantly increased potential impact. A security breach or vulnerability in one service, can have unexpected and possibly very large impact in other parts of the internet.

- **Our inability to bring people online in an equal way**

According to the World Bank, in 2005, 15% of the world's population was online, in 2010 that was 28%, and today it is over 50%. Each of those people comes from a different cultural understanding, a different educational perspective, and has different needs.

The next billion people will not use the internet the same way we do today. That raises different and new expectations, and new risks. Security approaches and tools designed for existing models may not meet their needs, creating a digital security divide.

- **Policy can negatively affect the abilities of the technical community**

Security incidents attributed to states have shown that they can have very significant impact. Increasing investment in offensive cyber capabilities, and their use, is an important concern and can lead to destabilizing incidents. This concern is real.

However, there is a risk of setting policy focused on state actors that makes the response to cybercrime, or other, non-state actor conducted operations, a more common threat to the daily online lives of many users, significantly more challenging. We believe it is important that steps to increase international peace and security within the First Committee are designed in a way to not negatively impact the ability of all stakeholders to protect people, who need to be at the core of cybersecurity.

## III. Recommendation to the OEWG participants

FIRST recommends focusing on the following principles for development of future norms:

- **Emphasize partnerships and inclusion**: the internet is operated to a great degree by the private sector, and individual users' interests are in many cases represented by civil society organizations. Governance on a purely multi-lateral basis is unlikely to reflect the wide variety of inputs the internet community can provide. We suggest the development of mechanisms that provide for multi-stakeholder participation to governance processes. We also recommend a "network" approach, with inclusion on both a multi-stakeholder and multi-disciplinary basis.

- **Capacity Building**: any new norms will require significant capacity building, which may include the development of new mechanisms. We strongly encourage states to review the capacity building mechanisms already existent within the community prior to building new ones. Bodies such as the Global Forum on Cyber Expertise, and networks within Civil Society can be a strong partner.

- **Awareness Raising**: norms have no space to exist and be adhered to when the affected parties are unaware. Ongoing awareness raising of the norms development effort is crucial to ensure the right parties get involved.

- **Ensuring CERT/CSIRT Status as Incident responders**: as was the case in the UNGGE 2013 and 2015 consensus reports, norms should continue to advocate and make clear the role of CERT and CSIRT as "incident response teams", and not overload them with activities that may devolve trust within the community; such as attribution or law enforcement work.

We encourage states to consider, in their discussions, the following potential policy decisions to aid in norms implementation:

- **We request all stakeholders to adopt practical measures to create clear indications of the roles and responsibilities of their respective communities**, to increase trust and capacity. As an example, FIRST published a draft Code of Ethics ("ethicsfIRST") for input, which describes the duties of computer security incident responders, including a duty of confidentiality, a duty to respect human rights, and a duty of evidence-based reasoning; increasing trust and transparency.

- **We request states to consider how policies may negatively affect the work of incident responders and security teams**. For instance, we advocate against the criminalization of security expertise. Security teams learn and build expertise from exchanging information on security incidents, defensive and indeed, offensive techniques. Any activities to limit this sharing are typically unhelpful.

- **We request states to build narrow exemptions on domestic and international sanctions implementations to permit for defensive sharing of cybersecurity information.** The internet knows no borders, and a vulnerability exploited in one state today can be used in another tomorrow. We need to ensure the free flow of both requests for assistance, and information on new incidents and techniques, between all incident responders, regardless of where they live.

- **We encourage states to review norms developed in multi-stakeholder communities, such as the Global Commission on the Stability of Cyberspace.** In particular, we believe the norm to "protect the public core of the internet" to have significant potential value in greatly reducing the impact of security incidents.

## IV. More information

FIRST looks forward to further contributing to the processes unfolding in the UN, including both the Open Ended Working Group (OEWG) and the Group of Government Experts (GGE). We remain available to provide any support as requested by these bodies and their participants, and will continue to provide input as is possible within these frameworks.

For more information, any interested parties can contact Maarten Van Horenbeeck via e-mail at maarten@first.org or phone at +1 206 499 4028.