Internet Society's response to the initial pre-draft report of the OEWG

This submission is in response to the OEWG Chair's letter of March 16 inviting suggestions and comments to the initial pre-draft report of the Open-Ended Working Group on developments in the field of Information and telecommunication in the context of international security (OEWG). We commend Ambassador Lauber for his efforts in the preparation of the report and appreciate the opportunity for non-governmental stakeholders from Civil Society, Technical/Operational Communities and Academia to express views on the report.

The Internet Society (ISOC) is a non-profit organization dedicated to an open, globally connected, secure and trustworthy Internet for everyone. We have 125 Chapters around the world, over 67,000 individual members, 101 organizational members and 10 Special Interest Groups. We are the administrative home for the Internet Engineering Task Force (IETF), a standards development organization whose mission is to make the Internet work better.

Our submission will reflect points in three sections of the initial pre-draft report: Existing and potential threats; Norms of responsible State behavior; and Capacity Building. In this submission we will focus mostly on Internet Security, an important element of the much broader concept of cybersecurity.

Potential Risks and Threats

We believe that the report does not sufficiently consider some major, action-oriented initiatives undertaken by public and private sectors to improve Internet security. It would also be improved by acknowledging the voluntary collaborative approach by which Internet security is achieved. Internet security more broadly relates to the security of network infrastructure, devices connected to it and the technical building blocks from which applications and platforms are built. This is an important point that bears highlighting for two reasons.

First, for greater clarity, the report should ensure that it is clear that security concerns and **potential threats cannot be solved by States alone**. Given the decentralized nature of the Internet's architecture any less will fall short of meeting these challenges adequately. As networks are interconnected and interdependent, one network acting alone can make little difference, even in protecting its own resources. Collaborative security or shared risk management approach where many stakeholders act together is particularly crucial to improving the security, resiliency and trustworthiness of the Internet's architecture while maintaining its openness.[1] A key component of this approach is collective responsibility where Internet participants share a responsibility towards the Internet as a whole. Internet security depends not only on how well participants manage the generic cyber security risks they face, but also, importantly, how they manage security risks that they may pose to others (whether through their action or inaction) – the "outward" risks. Note, see the Collaborative Security Approach.

1 Openness means that anyone may create, use, or deploy the technologies that make the Internet. It is a promise of continued innovation, the ability to share, create, and thrive.

internetsociety.org
@internetsociety

Rue Vallin 2,
Geneva, CH-1202
Switzerland

Tel: +41 22 807 1444
Fax: +41 22 807 1445

11710 Plaza America
Dr., Suite 400,
Reston, VA 20190 USA

Tel: +1 703 439 2120
Fax: +1 703 326 9881

Second, there are several **major initiatives in cybersecurity aimed at securing the Internet's infrastructure which is an important element to capture** in the report in order to provide a shared understanding of efforts being undertaken by public and private sectors towards Internet security. Some of these initiatives are grounded in experience, developed by consensus and evolutionary in outlook. These initiatives are flexible enough to evolve over time**.** We know that technology is going to change and threats will adapt to take advantage of new platforms and protocols. Therefore, these initiatives are developed to be responsive to new challenges. We have enclosed an infographic that provides some examples of initiatives working on improving the Internet's security such as Mutually Agreed Norms for Routing Security (MANRS), a global initiative, that provides crucial fixes to reduce the most common routing threats.

Additionally, here are several examples of policy initiatives and regional security frameworks developed through collaborative processes that yield informed outputs for effective implementation:

- Internet Infrastructure Security Guidelines for Africa (AIIS): A joint initiative of the Internet Society and the Commission of the African Union. This initiative also formed the African Union Cyber Security Expert Group (AUCSEG) that served as an advisory role to AUC on matters related to cybersecurity, cybercrime, online privacy and data protection as well as digital policy related issue.
- Global Commission on the Stability of Cyberspace (GCSC): which proposed a set of norms and guiding principles, such as the Call to protect the public core [https://cyberstability.org/research/call-to-protect/] - a good example of recognizing the shared responsibility of state and non-state actors in securing the Internet.
- Global Forum on Cyber Expertise (GFCE)- a global platform connecting various stakeholders through initiatives like global good practices [https://www.thegfce.com/good-practices] and, with partners the Cybil knowledge platform for cyber capacity building https://cybilportal.org/
- OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security
- APEC Framework for Securing the Digital Economy

Taking a strong stance on cybersecurity means making a firm commitment to minimize risks and counter threats posed by bad actors by adopting a **collaborative approach** that encourages inclusiveness and a range of expertise particularly from the technical, operational and research communities.

Norms, rules and principles for responsible State behavior

We agree that **voluntary non-binding norms are essential** in maintaining responsible State behavior and that the Norms in the 2015 UN GEE consensus report provide an important foundation in which to build international security and peace. We support the suggestion in the report for "*upgrading*" and further elaboration of norms. In particular, "*that the general availability or integrity of the public core of the Internet should be protected.*" This element should be elaborated further on the norm on the Protection of Critical Infrastructure in order to include the principle to protect the public core developed by the Global Commission on the Stability of Cyberspace (GCSC) and adopted by the Paris Peace Call on Security and Trust.

The Internet's public core encapsulates the Internet routing, naming and numbering systems (the Domain Name System), security and identity cryptography mechanisms, and communications cables.

These are the core functions that make the Internet work and should be safeguarded to ensure that the Internet remains an enabling technology that has global reach and integrity.

We encourage the OEWG to take due cognizance of the values of the GCSC Norm to Protect the Public Core, which emphasizes the need for both state and non-state actors to refrain from allowing any activity that could intentionally or substantially damage the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace.

Capacity Building

We agree that capacity building is an important contributor to a more secure and stable ICT environment for all. We recognize that **capacity building is a responsibility for all stakeholders** and given our global dependency per definition a cross border activity. In that context it is important to recognize that capacity building can be enhanced not only by including local civil society, academic institutions, the technical/operational community, and private sector actors but also by looking at regional and global actors in those stakeholder communities.

For example, there are regional and functional operator communities such as **regional network operator groups** (AfNOG, NANOG, APNOG, MENOG, etc.) that share their knowledge, experience, provide skills transfer and problem solving to grow the capacity of local and regional technical expertise. Some of the trainings which vary by region include network security, CERT training and information security. These operator communities also help with deployment of new technologies and encourage the use and implementation of best practices.

Other examples include **the Regional Internet Registries (RIRs)** which provide a range of trainings and workshops such as network security, DNS/Domain Name System Security Extension (DNSSEC), IPv6 security training and best practices and implementation of RPKI. The RIRs include the Africa Regional Internet Registry (AfriNIC), the Asia Pacific Network Information Centre (APNIC), the American Registry for Internet Numbers (ARIN), the Latin American and Caribbean Internet Addresses Registry (LACNIC) and the RIPE Network Coordination Centre (RIPE NCC).

With respect to coordination in capacity building efforts, we recommend the OEWG assess whether there are other platforms available outside of the UN which already have a coordinating role. Duplication of effort with existing initiatives, such as the Global Forum on Cyber Expertise, an existing multistakeholder platform, should be avoided. Further, as mentioned above, new initiatives will develop to address new challenges sometimes these will be outside of the view of any coordinating body, this should be seen as a positive feature.

To summarize the above, to address risks and threats in cyberspace adequately in order to build international security it is important to recognize in the pre-draft report that **Internet security is a shared responsibility by States and stakeholders and the collaborative security approach is crucial** in improving the security and resiliency of the Internet. Furthermore, the values in the GCSC norm on protection of the public core is integral to the UN GGE norm on the protection of critical Infrastructure and capacity building is enhanced through wide range of stakeholders from Civil Society, Technical/Operational inclusion, Academia and Private Sector actors.