Date: Tuesday, 26 February 2019
Version: 2
Theme: Security, Safety, Stability and Resilience (draft, tbc)

Narrative Description:

> Security and Safety are prerequisites to economic growth and a healthy digital environment beneficial to all. While security, stability and resilience refer to the systems, the infrastructure and the devices; safety and resilience of the users are also of paramount relevance.
>
> Under this theme potential risks to security and safety will be discussed from various angles with due consideration to how stability and resilience can be achieved. Strategies for protection of both systems and users will be addressed, taking into account a multidisciplinary perspective to potential solutions and the importance of stakeholder collaboration for responding to the growing range of threats to the global Internet and its users.

Link to SDGs: 1, 3, 4, 5, 8, 9, 10, 16

Sub-Theme 1	Illustrative policy questions
Cyber attacks and Cyber security best practice	1. How can technology assessments contribute to the early detection of potential security risks? 2. Cybersecurity concerns have helped drive a rise in protectionism. But are tech nationalism and walled-off networks the right response given it will disrupt the openness the Internet has thrived on? 3. What role can institutional arrangements such as CERTs etc. play? 4. How can cooperation and collaboration on national, regional and global levels help to increase security? 5. What should govern the response of states to state-sponsored cyberattacks? What types of aggression in cyberspace could be considered "armed attacks" and which would fall short? 6. What role do Internet protocols play in the fight against cyber attacks? 7. What legal regulations are already in place but potentially need to be enforced? What legal regulations should be created to address upcoming threats? 8. How can we facilitate awareness and broader participation of the general public on issues of cybersecurity to ensure they are equipped to engage with national politicians on this critical issue? 9. What role should different stakeholders play in cybersecurity capacity building? Which organizations are best suited to lead these efforts?

Sub-Theme 2	Illustrative policy questions
Safety of vulnerable	1. How can risks of contact and content be addressed successfully by new legal and regulatory approaches?

groups	2. What new technical instruments are available to address risks of contact and content?
	3. How can new technology tools and improved social norms contribute to safe and healthier online interactions and increase digital civility?
	4. How can children's rights to participation, access to information, and freedom of speech be preserved and balanced with their right to be protected from violence, exploitation and sexual abuse in the online environment?
	5. How can the resilience of minors be achieved by means of capacity building, media literacy, support and guidance in the digital environment?
	6. What role can the implementation of safety by design as a principle play to achieve increased safety?
	7. How can consumer rights be reinforced?
	8. How to increase consumers' understanding to protect themselves in the age of surveillance capitalism?
	9. What role can the implementation of privacy by design and privacy by default as principles play to achieve increased safety?
	10. How can violence and abuse against women online be addressed?
	11. How can literacy to protect women and girls online be achieved and increased, what programmes and projects would be necessary?

Sub-Theme 3	Illustrative policy questions
Internet ethics and human rights	1. How can trust and accountability be restored?
	2. What role should Internet platforms play in defining the standards for acceptable content in light of freedom of speech? How can we develop globally accepted standards?
	3. Where is the middle ground between increasing demands for proactive content policing by digital platforms and the necessary neutrality and legal certainty for platforms?
	4. What kind of collaboration could be created among Internet platforms and media outlets to fight disinformation and fake news?
	5. Which technical and regulatory instruments can reinforce the fight against CSAM?
	6. How can all forms of inappropriate sexualisation of childhood in digital areas be addressed by effective means?
	7. What are adequate techniques or technologies to fight all forms of online harassment including sexual harassment?
	8. How to make Internet or online life safer for all genders?

(NB: These are illustrative and not top-down – they are provided as examples to give guidance for the community in setting their own policy questions as part of their workshop proposals)