INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)

MAKING THE INTERNET MORE SECURE AND SAFER

IS3C contribution to the Global Digital Compact Consultations with Member States and Stakeholders

Friday 3 February

Thank you for your kind invitation to speak at this important event, my name is Allison Wylde. I hold academic posts with Cardiff University's Centre for Cyber Security Research (CCSR) and with the Business School at Glasgow Cal London. My research focuses on cyber security, in particular I examine the dynamics and processes of trust, trust-building and zero trust in cyber security and AI. I also contribute to the UN IGF BPF Cyber Security.

I support the aims of the Global Digital Compact and its core principles. They offer a roadmap to achieve the goals on an open, free and secure digital future for all.

I support the proposed scope of the compact's thematic areas, in particular data protection, the regulation of AI and of course, trust and trust-building - these areas are central to my research interests.

Thank you again and I appreciate the opportunity for the academic community to contribute to the development of the compact.

I am a member of the U.N. Internet Governance Forum's multistakeholder Dynamic Coalition called IS3C -Internet Standards, Security and Safety Coalition- established to examine how a more effective and rapid implementation of existing cybersecurity standards will lead to greater security and trust online.

IS3C was established three years ago. It's reports can be accessed on the U.N. IGF website and our own[1]. IS3C's current areas of work are 1) Security by design for the Internet of Things; 2) Education and skills, 3) procurement and supply chain management and 4) Data governance and security.

Severe incidents in the digital realm occur constantly, with high-impact ransomware incidents such as Solar Winds, Colonial Pipeline and Maersk but also impacts government and public institutions including hospitals and schools. They suffered severe effects, not just data loss. This, however, is just the tip of the iceberg: SME's and citizens also suffer and the impacts can be devastating.

IS3C looks at internet security from a different perspective with the aim of preventing harm through the prevention of incidents, e.g. through security-by-design for ICT services, products and devices.

It is our belief that the internet and ICTs can become considerably more secure and safer when governments and larger organisations demand security by design when procuring. Our work is a call-to-action that will provide the world at large with the recommendations, guidelines and toolkits allowing them to do so.

Many important security-related internet standards and ICT best practices have been in existence for years but have not been sufficiently widely adopted by industry and consumers. For example, security standards are generally not specified as requirements in public and private sector procurement contracts for devices and network applications.

[1] https://is3coalition.org/

Likewise the critical necessity for secure passwords, emails and domain names is not widely understood.

Secure routing on the internet, and the application of security by design principles in the development and manufacturing IoT devices, websites, software development and hosting are also key areas where a more consistent approach to adoption of relevant standards is required in order to achieve a greater level of security, safety and resilience on a worldwide basis.

IS3C's current work focuses on comparing policy at the global level concerning: cybersecurity education and skills; the Internet of Things; procurement and supply chain management of governments and industry and; data security and governance. IS3C is also compiling a list of the most important internet standards and ICT best practices that will be part of a toolkit of guidance for policymakers and decision-takers in procurement. Proposals for examining emerging technologies such as quantum computing and AI and for consumer protection are under consideration as potential future areas of work for the coalition.

OUR MESSAGES FOR THE GDC:

1. Create an eight thematic track on cybersecurity;
2. THE IS3C coalition looks forward to contributing to the development and implementation of the Compact's core principles and commitments to action;
3. The academic community, working alongside civil society, the private sector, the tech community, governments and regulators, can leverage important research that could help the successful take-up and implementation of the Compact's commitments to action on security and trust.