Internet Standards, Security and Safety Coalition (IS3C)

<u>Annual Report for 2022</u>

Introduction

The Internet Standards, Security and Safety Coalition (IS3C) is an IGF Dynamic Coalition of stakeholders with the shared goal of making online activity and interaction more secure and safer by achieving more widespread and rapid deployment of existing security-related Internet standards and best practices. Links for further information:

https://www.intgovforum.org/en/content/internet-standards-security-and-safety-coalition-is3c https://is3coalition.org/

The coalition's activities were undertaken by the following working groups in 2022:

WG1: Security by design – Internet of Things

WG2: Education and skills

WG3: Procurement, Supply Chain Management and the Business Case

WG4: Communications

WG5: Prioritising and listing existing, security-related Internet standards and ICT best practices

WG6: Data Governance and Security

The following is a report of their activities in 2022.

Working Group 1 : Security by Design

Chair: Nicolas Fiumarelli

The working group in 2022 followed up the previous year's analysis of gaps in the security in Internet of Things (IoT) devices and network applications, with a worldwide comparative analysis of how IoT security is being addressed in current national regional IoT policies, regulations and best practices. The aim of this research project, which was undertaken by a team of researchers in June-November 2022, was to identify common approaches and solutions for addressing widely recognised gaps in security-related standards. The research team examined regional and national IoT policy documents from 21 countries in five regions. Over 400 good practices relevant to IoT security were identified by the researchers.

The research team also considered consumer policy issues including what procurers of IoT devices and services need to know about the security specifications of IoT devices and applications, and their rights in the event of security being compromised. Current labelling

schemes which have been implemented in some countries were compared with the aim of identifying common approaches and innovative solutions.

WG1 announced that its research will be internally reviewed in December 2022 - January 2023 in preparation for an open consultation of its main findings planned for March 2023. IS3C expects to publish the final report of the research in April 2023. This will include a set of policy recommendations and guidelines, and a compilation of security best practices. IS3C will propose to the IGF Secretariat and the Leadership Panel that the IGF adopt these as IGF outcomes, and promote them for the attention of policy makers and decision-takers in governments and industry worldwide.

Working Group 2 : Education and Skills

Chair: Janice Richardson

A major factor undermining the development of a common culture of cybersecurity is that students graduating from tertiary ICT-related educational programmes often lack the skills that business and society as a whole need in order to understand the benefits of security-related Internet standards and ICT best practices. In order for ICT security to be better understood, it needs to be integrated into tertiary ICT educational curricula. This may result in the structural development of ICT products and services that include cyber security Internet standards and relevant best practices.

Taking forward the previous year's analysis of gaps in tertiary education curricula and vocational training, Working Group 2 carried out a research project in 2022 with the aim of: a) understanding the importance accorded to transversal and professional competences by the cybersecurity sector and by the tertiary education sector; and b) determining their expected level of competence of young people entering the cybersecurity sector.

The research used two methodologies. Firstly, interviews were conducted with cybersecurity experts in over 20 countries in all five regions of the world. This exercise was supplemented by a questionnaire survey that was distributed through Internet governance fora (including the IGF website, the national and regional IGFs) and networks such as the coordination and anti-abuse working groups of the Regional Internet Registry for Europe, the Middle East and parts of Central Asia (RIPE), online platforms such as Twitter and LinkedIn. This resulted in inputs from 66 countries from all regions.

The results of the research confirmed that there are significant gaps between what people learn in formal education about online security and the level of information that is needed by the cybersecurity sector. The research concluded that there is a need for collaboration between the education sector and industry, to ensure that knowledge is compatible with employers' requirements. There is also a need for continuous knowledge-sharing by experts in cybersecurity.

The report of the working group's research, entitled '*Closing the gap between the needs of the cybersecurity industry and the skills of tertiary education graduates*', was published on

on 1 December 2022 and presented at the UN IGF in Addis Ababa by WG 2 representative Teuntje Manders to the Chair of the IGF's Multistakeholder Advisory Group (MAG) Paul Mitchell and to the research's sponsors, Mieke van Heesewijk of SIDN Fonds and Julia Piechna of the Polish National Research Institute NASK.

The report can be accessed on IS3C's website at https://is3coalition.org/docs/study-report-is3c-cybersecurity-skills-gap/.

Working Group 3: Procurement, Supply Chain Management and the Business Case

Chair: Mallory Knodel

The coalition's planned work on examining procurement as a driver for widespread adoption of security-related standards was put on hold in 2022 pending receipt of funding support for research activity. At the IGF WG3 could announce that it received a research grant for 2023, to undertake a global comparison of best practices in government and industry procurement of ICTs. It is expected that this research will pave the way for a set of recommended best practices that promote adoption of security-related standards amongst suppliers of equipment and network services. It will also examine how professional training for procurement should take into greater account internet security and safety requirements.

Working Group 4: Communications

Chair: Raymond Mamattah

IS3C's working group for communication launched the coalition's website in the summer of 2022: www.is3coalition.org and is responsible for its maintenance and updating. WG4 also manages the membership's internal communications and external presentations. External communications with other initiatives is also a responsibility of this working group.

A sub-group was formed in October to develop IS3C's response relating to cybersecurity for submission to the UN Secretary-General's Envoy on Technology's consultation on the scope of the proposed Global Digital Compact (GDC). Dr. Allison Wylde leads this work in consultation with IS3C's working groups and IS3C expects to submit its response in March 2023.

Working Group 5: Prioritising and listing existing, security-related Internet standards and ICT best practices

Chair: Wout de Natris

There was *s*ome preliminary consideration in 2022 of possible candidates for IS3C's list of priority standards which will be developed in 2023. At the IGF WG5 could announce that it received a research grant for 2023 and that it will convene an international panel of experts in 2023 to develop a toolkit for government procurement agencies and private sector buyers of digital products, services or devices. This will include:

- A list of the most important existing, security-related Internet standards and related best practices, within to be selected categories, that will be a guide for procuring secure by design devices, services and applications;

- An overview of all security-related Internet standards and best practices.

Working Group 6: Data Governance and Security

Chair: Louise-Marie Hurel

WG6 conducts research into developments in the public sector that have become increasingly important in terms of government analysis and operations, academic research, and real world applicability and acceptance. Data has become as important for every economic sector and functional activity of government as physical assets and human resources. While governments are more connected, they are equally exposed to new and emerging threats. Cyberattacks and incidents such as data leaks highlight the complexity of the challenge in determining what kinds of responses (including regulatory ones) are adequate for securing data more effectively.

Working Group 6 was established in the fall of 2022 with the aim of supporting a global review of data security, identifying emerging trends, and best practices in this area. The working group will place in the coming two months and directly engage in a mapping exercise and the develop recommendations for data security framework. The working group plans in early 2023 to map data security frameworks and regulations worldwide with the aim of developing recommendations for how governments should respond to data security challenges.

New areas of IS3C's work expected to launch in 2023

IS3C undertook ongoing stakeholder consultations during 2022 on future areas of work for the coalition and it was reported at the IGF in Addis Ababa that expressions of interest had been received concerning the following issues:

- post-quantum encryption;

- governance strategies for emerging technologies such as AI and quantum technology;

- consumer protection;

- advocacy barriers to the deployment of three specific security-related standards: DNSSEC, RPKI and IPv6.

Overall Management of IS3C's business

IS3C organised three general meetings in 2022 including one at the UN IGF in Addis Ababa. The number of IS3C subscribers who are members of the coalition as at 31 December 2022 was 129. IS3C's website has over 2.000 subscribers.

All the IS3C working groups active in 2022 organised individual management and planning meetings during the year.

Financial Support

In 2022 IS3C received sponsorship funding and in kind support from the following organisations: SIDN, E-Governance and Internet Governance Foundation for Africa (EGIGFA), Microsoft, SIDN Fonds, NASK, ECP Platform for the Information Society, Platform Internetstandaarden (Dutch Internet Standards Platform), InSight and UN Department of Economic and Social Affairs (DESA).

IGF support activities

IS3C has been an active member of the UN IGF's Dynamic Coalitions Coordination Group (DCCG) and is promoting the means for achieving greater recognition of dynamic coalitions as policy incubators which contribute to the IGF's annual outcomes.

IS3C also advocates more effective integration of all intersessional IGF initiatives, including the dynamic coalitions, in the development of the IGF's multi-year strategy, annual theme-setting, programme development and evolution to "IGF Plus", as recommended by the UN Secretary-General's High-level Panel on Digital Cooperation. This will enhance the international exposure of dynamic coalitions, such as IS3C, and generate a higher level of responsiveness allowing for more input into the DC process, better options towards public consultations and more exposure, so higher participation within DCs.

Wout de Natris

IS3C Coordinator

10 February 2023