



UN Internet Governance Forum's Internet Standards, Security and Safety Coalition (IS3C)

2024 Annual Report

The Internet Standards, Security and Safety Dynamic Coalition (IS3C) was launched during the virtual Internet Governance Forum in 2020 with the aim of bringing together expert stakeholders from the technical community, civil society, government policymakers, regulators, and corporate and individual adopters, with the shared goal of making online activity more secure and safer by achieving more widespread and rapid deployment of existing security-related Internet standards and ICT best practices.

Nine working groups have been created since 2020 to take forward the coalition's work in analysing existing policies worldwide and researching the challenges and barriers relating to the deployment of security-related Internet standards. In the past two years IS3C has published three reports: on education and skills in tertiary cybersecurity education (2022); security by design and the Internet of Things (2023); and public sector procurement of ICTs (2023). IS3C has also published a tool containing the most important cybersecurity standards (2023).

Updates on the coalition's recent work and future action plans were presented at the IGF in Riyadh in December 2024. This report sees to the whole IGF cycle from Kyoto to Riyadh.

Section 1: Progress reports on the IS3C Working Groups

In this overview we present an update on the activities of IS3C's working groups in 2024.

WG1 security by design - Internet of Things (IoT) and WG 3 Procurement and Supply Chain Management

WG1 leaders:

Nicolas Fiumarelli, Chair - Uruguay

Sam Goundar, Vice-chair - Vietnam

WG 3 leaders:

Liz Orembo, Chair - Kenya

Frank Ogochukwu, Vice-chair - Nigeria



These two working groups have continued to monitor new policy documents relevant to their specific areas of government policy, regulation and best practice. This will lead to preparation of updates in 2025 of their previous reports on these issues. In addition, they have formulated action plans which aim to promote their recommendations in capacity building programmes and a series of informational webinars to be held during 2025-26. Both WGs were actively engaged in ensuring funding for their programmes. Unfortunately grants were not allotted to them in 2024. The work will be carried out after funding is secured.

WG 2 Education and Skills

Leaders:

Awo Aidam Amenyah, Chair - Ghana

Janice Richardson, Vice-chair - Luxembourg / Australia

The research undertaken by WG 2 2022 in 66 countries showed that there is global consensus on the existence of a significant gap between the skills taught in the cybersecurity curricula of tertiary education institutions and the skills required by industry. The consequence of this is that students do not graduate with the skills necessary to meet the challenging needs of the sector.

IS3C's report published in 2022 and presented at the IGF in Addis Ababa made several recommendations on how to overcome this growing gap in the cybersecurity supply chain. In Kyoto the centrepiece of IS3C's action plan was presented, to translate these recommendations into action by establishing a cybersecurity hub which will contribute to developing a more skilled and diverse cybersecurity workforce through improved collaboration between the technical, industry, tertiary educational and social sectors. At the IGF in Riyadh the working group showed a video which explained the concept of the cybersecurity hub. This was produced by the Pixel Blue Academy of Edmonton in Canada. IS3C expressed its gratitude to Tony Grillo, Buchanan Kohl and their students for their valuable work on this project. The video can be accessed at:

<https://is3coalition.org/cybersecurity-hub/>

WG 4 Communications and strategy

Leaders:

Raymond Mammatah, chair - Ghana

Selby Abraham, vice-chair - Ghana

WG4 handles IS3C's internal communications including the maintenance and updating of the coalition's website - <https://is3coalition.org> - which is carried out by webmaster and Vice-chair Selby Abraham.



WG 5 Internet Security Standards

Leader:

Wout de Natris-van der Borgh - The Netherlands

WG5 was created in 2023 to draw up a reference list of key Internet security standards (including the most important interoperability-related Internet standards) that will assist ICT procurement decisions. This was reported and presented at the IGF in Kyoto as the final output of this working group. The WG's activities stopped in January 2024.

WG 6 Data Governance

This working group was inactive in 2024.

WG 7 Consumer Protection

This working group has been in the process of development in 2024 in consultation with leading experts and consumer organisations. It is expected to launch in 2025.

WG 8 DNSSEC and RPKI Deployment

Leaders:

David Huberman, Chair - United States

Bastiaan Goslings, Vice-chair - The Netherlands

WG8's aim in 2024 was to develop a narrative that can be drawn on to convince corporate leaders and decision-takers of the necessity to deploy the DNSSEC (Domain Name System Security Extensions) and RPKI (Resource Public Key Infrastructure) Internet standards and to make these standards an integral part of their ICT procurement policy.

The project was announced at the Kyoto IGF in 2023. In 2024 a team of international experts reached consensus on how to formulate the non-technical case that technical staff can draw on to convince decision-takers to deploy these critical protocols or have them deployed through their procurement decisions. They are of a varying nature and cover security requirements, regulatory compliance, data protection controls, commercial benefits, and ethical considerations. The report and narrative tool were presented at the IGF in Riyadh and can be downloaded at:

<https://is3coalition.org/docs/how-to-convince-your-boss-to-deploy-dnssec-and-rpki/>

It stands to reason that these arguments can be used for other security-related Internet standards and ICT best practices as well.

IS3C warmly thanks the WG chairs and the experts for their dedication and time on this project which is now concluded. IS3C also acknowledges the sponsors who made the work



possible, ICANN and RIPE NCC. The IS3C leadership team will continue in 2025 to promote awareness of this important tool through its ongoing outreach communications and delivery of presentations at relevant fora and meetings.

WG 9 Emerging Technologies

Leaders:

Elif Kiesow Cortez, Chair - The Netherlands / Turkey

Maarten Botterman, Vice-chair - The Netherlands

WG9 was originally conceived in 2022 as intending to analyse and research security aspects of AI and quantum technologies. However, having reviewed in 2024 the growing number of existing and emerging global initiatives relating to AI, the leadership agreed WG9 to develop its focus in 2025 primarily on post quantum issues.

Section 2: IS3C's Four Point Plan and Projects in 2025

IS3C announced at the IGF in Riyadh the following four point future plan for cybersecurity cooperation and capacity building in line with the goals of the UN Global Digital Compact and its contribution to sustainable development in all the world's regions.

- 1) Establishing a global Cybersecurity Hub as an online forum for experts from the technology and education sectors to increase cybersecurity skills content in tertiary school curricula and professional training programmes. A workshop will be organised in 2025 where the purpose and operation of the hub will be explained. IS3C will work actively to attract active support for the hub and secure the necessary funding for its launch and operation.
- 2) Recommendations for security best practice in the Internet of things and post-quantum cryptography, supported by capacity building training programmes. In a collaborative project, WGs 1 and 9 will undertake research into the current state of policy of both technology applications, including the impact post quantum computing will have on society, policy, politics, etc. The report will be presented at the IGF in Oslo in June 2025.
- 3) Rolling out a toolkit for public and private procurement agencies that specify how contracts with suppliers should build in specific security requirements for devices and network services.
- 4) Defining the potential role of consumer protection organisations in the security of users' devices and network applications. Contact with consumer organisations and consumer protection agencies was made and this led to a workshop at the IGF in Riyadh that considered consumer perspectives relating to cybersecurity. It was agreed to continue the discussions in 2025 to consider if a working group for consumer protection (WG7) with a



membership of consumer and ICT experts from all regions can be created. Work with consumer advocacy organisations is dependent on positively judged grant applications.

Section 3: Review of IS3C's Governance

So far IS3C's work has focused on research and the ensuing tools and recommendations. Since the Kyoto IGF in 2023, it has also focused on putting the theory of its reports to practice, i.e. moving from research and analysis to capacity building. This makes it important therefore to look at the way this multistakeholder global coalition of experts is structured and organised. Securing sufficient funding will become even more important because setting up capacity building programmes needs a different kind of expertise and funding. The current informal organisation and funding model of IS3C will likely be a hindrance for the development of IS3C's aims for capacity building.

For this reason, following initial discussions and consultations by the leadership team during 2024, IS3C is currently considering the options of applying to become a working group under the Internet Society's Dutch chapter and to become a not for profit foundation. The membership will be consulted on these options at its first General Meeting in 2025.

Section 4: Engagement in International fora and Processes

IS3C's outreach and external engagement activities in 2024 included interactive presentations at the European regional IGF EuroDIG in Vilnius in June 2024 when it organised a day 0 event and contributed to other relevant workshops with reports and updates of the coalition's work.

At the IGF in Riyadh IS3C organised a day 0 event on its decision making tool (WG8) and on consumer protection. In our joint workshop with DC IoT we presented our work on IoT security by design and announced our upcoming work in WG 1 and 9 (see above). Individual members participated in diverse workshops.

IS3C was also active in the consultation process of the UN Global Digital Compact (GDC) during 2024, advocating in particular the GDC's recognition of the IGF's intersessional work including the dynamic coalitions such as IS3C.

Individual members of the coalition represented IS3C on site and online in the NETmundial+10 meeting in Sao Paulo in April 2024 where they advocated the need for improving the Internet's security and safety, e.g. by deploying security-related Internet standards.

IS3C is an active member of the IGF Dynamic Coalitions Coordination Group (DCCG) where it advocates full recognition of the outcomes of coalitions' year-round work within the IGF ecosystem and a better integration of DCs in the IGF's programming and strategy



development. This work has led to an improved understanding amongst the IGF community of the role and contributions of the Dynamic Coalitions and to suggestions on how to integrate DCs more effectively in the IGF's annual programme. IS3C's leadership has also pursued this aim in contributions to the work of the IGF Multistakeholder Advisory Group's Working Group on Strategy.

IS3C's coordinator Wout de Natris-van der Borght presented the work of IS3C at the Dutch national IGF (NLIGF) in December 2023. Selby Abraham reported on IS3C work and its potential impact on the curricula of tertiary cybersecurity education at both the UK Cybersecurity Week 2024, and a seminar on Cyber Warfare at the University College London School of Public Policy.

Section 5: Links for further information and contacts

You can find more information on IS3C, reports and activities here:

<https://is3coalition.org/> and here:

<https://www.intgovforum.org/content/dynamic-coalition-on-internet-standards-security-and-safety-dc-issc>.

You can join IS3C here:

<http://intgovforum.org/mailman/listinfo/dc-issc> intgovforum.org

Wout de Natris – van der Borght

Mark Carvell

IS3C coordinator

Senior Policy Advisor