INTERNET
STANDARDS,
SECURITY AND
SAFETY COALITION
(IS3C)

MAKING THE INTERNET
MORE SECURE AND SAFER

Internet Standards, Security and Safety Coalition - IS3C

Annual Report for 2021

1. *Introduction*

The Internet Governance Forum's Dynamic Coalition on Internet Standards, Security and Safety (DC-ISSS) held its inaugural meeting at the virtual IGF in 2020. It set out its aim to make online activity and interaction more secure and safer. Online ICT security can be significantly enhanced by more widespread and rapid deployment of existing, security-related Internet standards and best practices. The coalition brings together stakeholders from the technical community and civil society, government policymakers and regulators, and corporate and individual users with the shared goal of agreeing recommendations and guidelines which will achieve this aim.

At the IGF2021 the coalition announced its change of name: the Internet Standards, Security and Safety Coalition with the acronym IS3C and this is how the coalition will be referred to in this annual report.

Internet and ICT security is an issue of major concern that is high on the agenda of governments, industry and individual users. Furthermore, the COVID-19 pandemic has brought into sharp focus the increase in society's dependence on the Internet, on communications technologies and networks, and the necessity of secure and trusted interconnection of individual devices and online applications in all social and economic sectors including health, social welfare, work and finance.

It is widely recognised that many Internet-related products and services are increasingly vulnerable to security threats and the spread of online harms and criminal misuse. However, if relevant security-related standards and best practices are more effectively adopted and deployed worldwide, these risks can be reduced significantly. This will foster greater trust in the Internet and in its related digital technologies and applications, with the result that the positive social and economic benefits of these transformative technologies for sustainable development will be fully realised for communities worldwide.

The IS3C multistakeholder coalition aims to ensure that standards and best practices play their full role in addressing these cybersecurity challenges through establishing the conditions for their wider, more effective and more rapid adoption by key decision-takers throughout the supply chain in both the public and private sectors. This can be achieved only if there is a shared commitment by stakeholders worldwide in a new strategic comprehensive approach to standards implementation.

During 2021 the leadership team took important steps in finalising the organisation and modalities of IS3C's work by ensuring that its governance is transparent and accountable to its members. A series of important outreach activities were undertaken during the year including presentations to government bodies, Internet organisations, national and regional IGFs, Internet standards and cybersecurity groups and briefings for individual stakeholders. These activities are presented in more detail below.

The UN Secretary-General's Roadmap for Digital Cooperation has made clear the expectation that the IGF's dynamic coalitions will play an important role in contributing to the IGF's outcomes. If this is to be realised in a comprehensive and meaningful way, it is important to consider how these outcomes - including those of the dynamic coalitions such as IS3C - are received by stakeholders worldwide and brought to the attention of the UN Member States and its institutions and agencies.

The IS3C leadership team has participated actively in meetings of the IGF's Dynamic Coalition Coordination Group (DCCG) when these aims were discussed. The leadership team's consultations with the UN Department of Economics and Social Affairs (UNDESA) and with the Secretary-General's Office of the Envoy for Technology will also be important in determining the steps on how IS3C's policy recommendations, toolkits and best practice guidance should be communicated as IGF outcomes to policymakers and be disseminated to decision-takers worldwide. These discussions will continue in 2022 and the coalition's members will be consulted accordingly.

1.1 *IS3C's Leadership*

The IS3C leadership team comprises:

Wout de Natris - Coordinator (De Natris Consult, the Netherlands)

Mark Carvell - Senior Policy Advisor (Independent Internet governance consultant, UK)

and the following working group Chairs and Vice-Chairs:

WG1: Security by design - Internet of Things

Chair: Yuri Kargapolov (Head of Research and Scientific Office, State University of Intelligent Technologies and Telecommunications, Ukraine)

Vice chair: Lim, May-Ann (Director of the Fair Tech Institute, Singapore) was succeeded in June 2021 by Sávyo Vinicius de Morais (IoT Security Specialist at Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, Brazil)

WG 2: Education and skills

Chair: Raymond Mamattah (President of E-Governance and Internet Governance Foundation for Africa - EGIGFA, Ghana)

Vice-chair: Janice Richardson (Director Insight, Australia/Luxembourg)

WG3: Procurement, supply chain management and the business case

Chair: Mallory Knodel (Center for Democracy & Technology - CDT, USA)

Vice-chair (interim): Wout de Natris (De Natris Consult. Netherlands)

WG4: Communication

Chair: Raymond Mamattah (President of E-Governance and Internet Governance Foundation for Africa - EGIGFA, Ghana)

Vice-chair: Olévié Kouami (Directeur général chez Le FA de la Téranga, Senegal)

1.2 *IS3C's Supporting Organisations*

The coalition is largely run on a voluntary cooperative basis but inevitably some administrative costs have been incurred. The leadership team express their deep appreciation to the following organisations who supported the IS3C and its work with financial contributions during 2020-2021:

- The Swiss Ministry of Foreign Affairs
- Microsoft
- SIDN
- Platform Internetstandaarden

The following organisations have allocated resources on behalf of the IS3C in 2021 and for ongoing work in 2022

- ecp (platform for the information society, the Netherlands)
- E-Governance and Internet Governance Foundation for Africa (EGIGFA, Ghana)
- Institute of Information and Communication Technologies for Development (INTIC4DEV, Senegal)
- Platform Internetstandaarden (the Netherlands)

1.3 *IS3C's Thematic Working Groups*

Three working groups were established at the IGF in 2020 which in a coordinated work programme will:

1. bring the critical security supply and demand factors together;
2. propose the best options for the deployment of key standards and best practices on both sides, in the form of policy recommendations and practical guidance. These outcomes will be presented as IS3C policy recommendations for dissemination to policymakers and decision-takers worldwide.

The three working groups look at the issue of deployment from separate, specific policy angles:

- WG1: Security by design (SBD). The first sub-group of WG1 looks specifically at SBD in the Internet of Things (IoT);
- WG2: Education and skills;
- WG3: Procurement, supply chain management and the creation of the business case.

The protection of computer systems and networks from information disclosure, disruption, theft and damage to their hardware, software, or electronic data, is widely discussed and a large number of cybersecurity initiatives and programmes worldwide are run by various stakeholders communities, quite often in isolation from other similar initiatives. At the same time more and more online vulnerabilities are exploited by criminals.

As a consequence, a gap has developed between the theory of security and the daily occurrence and practice of insecurity online. This is a gap that has to be closed in order for online activities to become generally more secure and safer.

Many cybersecurity initiatives concern mitigation of threats. Computer Security Incident Response Teams, botnet mitigation programmes, Security Operation Centers, etc., generally focus on alerts of threats and the reporting of incidents in order to develop responses. They deal to a lesser extent with prevention. However, prevention needs to become the second pillar of defence because apart from human errors of judgement, the causes of many incidents are flaws in the security, design and development of network products, devices and services. These flaws are exploited in order to inflict harm or conduct criminal activity.

This is why the three coalition working groups have the common aim of developing policy recommendations, toolkits and guidelines that will generate a higher level of understanding and knowledge that in turn will lead to the more rapid deployment of Internet security standards and related best practice. The working groups have adopted the same methodology of reviewing current and previous initiatives, collating data on the key issues, analysing the data with the aim of developing proposals for more in-depth research, and engaging stakeholders through presentations and capacity-building workshops. The working groups published their mission statements accordingly including workplans for their research. These are described below.

1.4 *IS3C's Communications*

Internal discussions held in the fourth quarter of 2021 concluded that there was a need for professionalisation of the coalition's communications, the presentation of its work and for establishing its funding arrangements for research and covering administrative costs.

The E-Governance and Internet Governance Foundation for Africa (EGIGFA) and the Institute of Information and Communication Technologies for Development (INTIC4DEV) offered to lead and support the development of the coalition's communications strategy.

A fourth, non-issue, working group was established accordingly: WG4 Communication with its remit to:

1. professionalise the coalition's internal and external communications with a dedicated website, consistent formatting and presentation of its documentation and output;
2. develop a long term strategy for the coalition's awareness-raising worldwide and increasing its diverse stakeholder membership and active participation in the working groups.

Following a consultation of the coalition's membership, WG4 implemented the change the name of the coalition to "Internet Standards, Security and Safety Coalition" with the acronym IS3C" and presented its logo.

1.5 *IS3C's governance*

It was agreed by the members in early 2021 that the coalition should establish a framework of governance that would:

1. ensure stakeholder inclusivity and predictability in the coalition's process for developing concrete outcomes;
2. command the respect of the target policymakers and decision-takers for those outcomes.

Following an online survey and consultations with participating stakeholders in February-March 2021, a governance document was drawn up which confirmed the coalition's open membership through subscription to the mail list, described the step-by-step procedure for reaching consensus-based decisions for finalising recommendations and guidelines, and established the roles and responsibilities of the leadership team including the working group Chairs and Vice-Chairs. The full text is accessible at https://www.intgovforum.org/en/filedepot_download/3737/2536.

1.6 *IS3C's Outreach activities*

The leadership team has made considerable efforts during 2021 to generate active stakeholder support for IS3C through active participation in its working groups and funding to cover the costs of research activities and administrative support. The number of participating experts is steadily rising and the first tranches of financial support have been secured for 2021.

The IS3C Leadership presented its work throughout 2021 to various bodies and stakeholder groups active in the field of Internet governance and cybersecurity, including UN First Committee's Open-ended Working Group (OEWG); the High-Level Panel on Internet Governance chaired by the European Commission (DG-CNECT); the European Commission's Multi Stakeholder Platform on ICT Standardisation; and the African Union Commission's Working Group on Cybersecurity. IS3C leads also actively participated in the Paris Call process.

Presentations and interactive sessions were also held in several national and regional IGFs (NRIs), including the Ukraine, Taiwan, USA and the Netherlands national IGFs, the European regional IGF (EuroDIG) and the Asia Pacific Regional IGF (APrIGF). The Leadership also discussed the IS3C's objectives and modalities with a range of individual organisations and companies

Outreach will continue in 2022 in accordance with its new communications strategy being developed by WG4, in order to promote awareness in all geographical regions, to invite contributions on content and support for developing outcomes through participation in the working groups, and to secure financial support for research activities and to cover essential administrative costs.

1.7 *Funding for IS3C's activities and administration*

IS3C reached an agreement in 2021 with the Dutch platform for the information society called *ecp* under which *ecp* will provide the administrative services and financial handling of all transactions made on behalf of IS3C, including the receiving and sending of invoices. Through its relationship with *ecp,* the coalition has established a basis of financial neutrality with an organisation that is specialised in Internet governance with considerable experience in national and international cooperation. The financial costs incurred by *ecp* are covered by Platform Internetstandaarden.

The efforts to secure financial support for research projects will continue in 2022 under the enhanced strategy for engagement with stakeholders being developed by WG4.

2. *Coalition activities undertaken by WG1, WG2 and WG 3*

2.1 *Working Group 1: Security by Design - Internet of Things (IoT)*

The rapid expansion of the so-called "Internet of Things" (IoT) in social and economic life has created new challenges for ensuring the security and safety of IoT networks, devices and applications. The aims of IS3C's Working Group 1 (WG1) are twofold:

1) *to review current security-related IoT initiatives and practices and assess the degree of readiness of existing technical and management solutions that affect the design of systems with built-in security by default;*
2) *to develop a coherent package of global recommendations and guidance for embedding security by design in the development of IoT devices and applications.*

The objectives, projected outcomes, key tasks, and timeframe for its work plan are set out in its Mission Statement published in June 2021 which is accessible at: https://www.intgovforum.org/en/filedepot_download/3737/2589.

WG1's membership grew in 2021 to include a diverse range of experts from different geographic regions and organisations. Working relationships have also been established with specific initiatives including the IoT CyberSecurity LAC (Latin America and Caribbean) Working Group, which is mapping national initiatives regarding certification, homologation, and regulation of the commercialisation of IoT devices in the region, and ISOC's IoT Special Interests Group (SIG). WG1 is also in discussion with the Tech Accord concerning its work to identify the challenges in designing and implementing secure IoT systems.

In its first phase of work in early 2021, WG1 reviewed existing research materials and collated information about: a) current approaches to IoT standards deployment; and b) local, national and regional experience in the implementation of IoT standards. Analysis of this data concluded that the factors which weaken the security and safety of IoT networks and devices are:

- gaps in the architecture of the IoT;
- competing protocols;
- poor or deficient security specifications;
- lack of effective identification management;
- the general need for a basic trust model in the IoT environment.

In its second phase of work, the members conducted a survey to better understand the aims of different stakeholder groups regarding IoT security and collated data on existing IoT security-by-design initiatives, guidelines, current security practice and any relevant regulations. Analysis of the 67 responses received showed that the main concern was about unauthorised access to private IoT data, lack of supporting regulation and insufficiency of cyber protection rules. There were very few concerns about the impact of restrictive regulations.

With regard to identifying the priority policies for improving IoT security-by-design, the survey showed general support for prioritising standardisation and education. A common theme in the responses was concern about the absence of strategies for predicting the behaviour of new security threats to IoT networks, an important consideration for security-by-design strategies of defence against new threats. Most of the initiatives identified by respondents related to developing standards or best practice (56%), technical development tools (36%) and capacity building (31%).

Next steps

WG1's third phase of work in 2022 will focus on the differing assessments of security threats to IoT networks, devices and applications, held by stakeholder constituencies, including suppliers, users and academia. Further outreach to more diverse stakeholder communities will be undertaken. A general goal for the WG is to expand and increase the diversity of the membership through outreach, awareness-raising and personal networking. E.g. outreach to relevant working groups of ICANN and its Office of the Chief Technology Office (OCTO), the Internet Engineering Task Force (IETF) and the Institute of Electrical and Electronics Engineers (IEEE) is also planned for 2022.

To achieve this body of work, WG1 has announced a research proposal that will be made public in February 2022. This will include in-depth categorisation and analysis of IoT certification requirements relating to security, and IoT network capacity-building programmes. The goal is to define a set of global recommendations and guidance for embedding security by design in the development of IoT devices and applications. The report is to be presented at the IGF 2022.

2.2 Working Group 2: Education and skills

The principal aim of Working Group 2 (WG2) is to identify gaps between the knowledge and skills of young graduates entering the cybersecurity sector and the expectations of the organisations that employ them. In its first year, WG2 has been documenting ways that countries and institutions are addressing this challenge and how promoting good practice that could be replicated elsewhere.

WG2's Mission Statement explaining its objectives, projected outcomes, key tasks, and timeframe for its work plan are set out in its Mission Statement published in June 2021 accessible at: https://www.intgovforum.org/en/filedepot_download/3737/2590. This describes the group's focus on examining how tertiary educational curricula, at all levels of education, need to adapt to ensure that school and college-leavers are equipped with sufficient knowledge and understanding of how deploying security-related standards helps individuals and businesses to engage securely and safely in the digital economy.

Because of society's increasing dependence on cyber infrastructure and the major costs to business and society caused by cyberattacks, cybersecurity has become an important and expanding employment sector. The vocational and tertiary education sectors may have attempted to adapt their training and course curricula to meet the demand for expertise in cybersecurity. However, a sample of mainly European stakeholder interviews conducted by WG 2 in the first half of 2021 produced the following, startling conclusions:

- the creative, innovative potential of young people is not being tapped for the benefit of a more secure cyber future;
- industry and government interviewees pointed to a low level of generic skills such as synthesis and analysis necessary for a career in cybersecurity and developing the pipeline of talent required for the increasingly digital society and economy;

- students lacked some core skills such as holistic thinking and the ability to join the dots in complex problem-solving and had poor knowledge of operating systems, systems logic, network protocols and cloud technologies;
- cybersecurity studies should better equip graduates with the ability to draft, strategize and develop a cyber risk mitigation strategy, including the appropriate legal and compliance steps that need to be taken when responding to cyberattacks and reporting them to law enforcement;
- students needed to develop an in-depth understanding of the different types of cyberattacks, the business systems that are most at risk, and the importance of an organisation-wide approach to cybersecurity.

Companies that were contacted by WG2 members during 2021 indicated they were keen to support exploring new approaches to meet the demand for trainees and graduates with more in-depth cybersecurity expertise. Examples of good practice cited by businesses included the establishment of a national hub in Denmark that brought together education and business, and a social engineering approach to recruitment developed in the Netherlands, where gender-balance is also a priority.

Next steps

In its next phase of research, WG2 intends in the first quarter of 2022 to undertake, with the assistance of the Youth IGF, a further round of interviews with tertiary and vocational establishments in other geographical regions. This research will also include interviews with a more diverse range of business stakeholders. A preparatory step already taken has been outreach to universities in Australia, Morocco and Poland with the aim of:

a) obtaining the views of leading academic experts on the findings of the initial phase of interviews;
b) validating the methodology being adopted by the working group for its continued research.

It is also hoped that this will lead to new partnerships between business and academia that will enhance the ongoing work of the IS3C coalition generally.

The final phase in WG2's work plan in mid-2022 will be to undertake a worldwide stakeholder survey with the aim of consolidating the initial research findings with quantitative data. Open questions in the survey will also encourage respondents to share new ideas and examples of good practice.

The final report setting out WG2's findings and its policy recommendations and guidance for the vocational training and tertiary education sectors will be presented at IGF2022. These outcomes will not only serve to reshape training programmes and educational courses so that they fully meet today's cyber-challenges, but also encourage more young people to consider the cybersecurity sector as an exciting employment opportunity.

2.3 *Working Group 3: Procurement, supply chain management and the creation of the business case*

The aim of Working Group 3 (WG3) is to develop policy recommendations and guidelines relating to the procurement of digital technologies in particular in the public sector and supply chain management decisions in the private sector. The overall aim is to ensure procurement best practice takes fully into account Internet security and safety requirements with reference to key security standards, and that this knowledge and practice is included in procurement training.

WG3's outputs on procurement and supply chain management are therefore expected to be a major contribution to achieving the IS3C's primary goal to make the Internet more secure and safer by being a major driver for more effective and widespread implementation of key security standards and related best practice.

WG3 published its charter and mission statement in June 2021 which is accessible at https://www.intgovforum.org/en/filedepot_download/3737/2588. This explains its objectives, projected outcomes, key tasks, and timeframe for its work plan for developing its outcomes which are summarised in the following table.

Outcome		
Meeting global internet security standards is a ubiquitous baseline requirement in any public or private sector procurement and supply chain management policy.		
Objectives		
1. Full scope of security standards and procurement challenges and opportunities.	2. Relevant and actionable guidance to require security standards in procurement.	3. Guidance influences public and private sector procurement and supply chain management.
Activities		
1.1 Conduct basic desk research to answer "What has been done by others to achieve [this project's outcome]"? 1.2 Develop a decision matrix to narrow in on global institutions within the UN IGF's sphere of influence and impact. 1.3 Collect and document existing procurement and supply chain policies of those institutions, and contacts list. 1.4 Adjust work plan based on findings.	2.1 Circulate a short survey to procurement decision makers on challenges and opportunities in shifting policies. 2.2 Identify areas for improvement in existing procurement and supply chain management policies for internet security standards. 2.3 Develop a guidance document (checklist, issue paper, etc), or suite of materials, fit for purpose. 2.4 Determine areas of future work and adjust workplan.	3.1 Circle back to decision makers with guidance. 3.2 Promote the IS3C and its future work to decision makers. 3.3 Follow up to document outcomes, if any.
Outputs		
Issue paper (2022)	Policy recommendations and guidance documentation (2022-23)	Working group growth (ongoing)

The WG3 work plan consists of two sequential phases of activity: issue mapping and policy guidance, supported by continuous outreach and strategic engagement for securing the necessary inputs from relevant experts and stakeholders. The overall objective of the first two phases is to develop policy recommendations and guidelines for dissemination in the third phase to public sector procurement agencies and supply chain managers in business and the tech sector.

Phase I: Issue mapping (2021-22)

In its first phase of the work, WG3 has been identifying existing guidance for policy makers in a variety of contexts relevant to the procurement of digital technologies, with the aim of identifying:

1. common elements of best practice;
2. shared problems barriers;
3. global and Global South applicability.

A comprehensive overview of current guidance and best practice has been drawn up in a matrix of existing resources broken down by geographical region, institution and sector, and by products and services

Phase II: Guidance and recommendations (2022-23)

Analysis of the background research conducted in the initial phase will inform the second phase of work to develop policy recommendations and resources for decision-takers such as guidelines, toolkits and checklists. These outputs will also help to promote awareness of existing initiatives, processes and best practice which will be described in an accompanying background report.

Phase III: Outreach and participation

The third phase of WG3's work will build on the networking with stakeholders in the first two phases with the aim of identifying key contacts amongst decision takers and influencers in the public sector procurement and supply chain management in all geographical regions.

This work will provide the basis for dissemination of IS3C's recommendations and guidance on procurement and supply chain management. Consideration will also be given to using the IGF's global network and the IS3C members' stakeholder networks to assist in awareness raising, establishing sector liaisons worldwide and identifying regional distribution channels for the working group's outputs.

3. IS3C's forward look for 2022-23

The three current IS3C issue-specific working groups will present their outcomes at the next IGF in late 2022 in accordance with the objectives and the next phases of their work plans described in section 2 above.

In support of these outcomes, the coalition intends to produce the following two general outcomes;

1. A list of critical Internet standards and related best practice;
2. A standards and best practice overview document.

A fifth IS3C working group comprising experts in standards from diverse stakeholder communities will be established in 2022 to undertake the work of compiling the list and preparing the overview. These are described in more detail below.

3.1 *IS3C's List of Essential Standards*

The rationale and benefits of this list is twofold. Firstly, most Internet organisations actively promote one standard, e.g. in the domain name community DNSSEC is promoted, for websites the focus lies on the OWASP top 10, RIRs often point to secure routing through RPKI, etc.. However, a person in charge of procurement decisions or supply chain management is often faced with a complex range of various and sometimes competing standards. This complexity of technical information creates a risk of indifference to the necessity of stipulating specific standards that best serve the organisation's security requirements.

To assist in the making of better-informed choices about security requirements, IS3C aims to present at the IGF in 2022 a list containing the most essential, relevant Internet security standards and related best practice, categorised by individual network products, services and devices.

The second benefit of IS3C compiling this list is that standards will no longer be promoted from a single location of standards development. Representatives of relevant cybersecurity interest groups, standards organisations and leading international bodies will be invited to work together in the IS3C multistakeholder coalition to agree a listing of the most urgent standards and relevant best practice. This list will be disseminated as part of a toolkit for public and private policymakers and decision-takers and will also provide a basis for cybersecurity capacity building especially in developing countries which have few resources and limited access to expertise in cybersecurity.

3.2 *IS3C's Standards and Best Practice Overview.*

IS3C intends to present at the end of 2022 a second comprehensive listing that includes all relevant, security-related Internet standards and ICT best practice. Each entry in the listing will be categorised according to network service or device with an explanation of the issue which the standard or best practice aims to resolve and which stakeholders have roles in undertaking the necessary action for deployment.

3.3 *Scope for new IS3C working groups*

The three current thematic working groups on security by design, education and skills, and procurement and supply chain management, lead the coalition's current scope of activities. However, the coalition's remit is expected to evolve and expand with the creation of new issue-specific working groups.

The following issues were identified in the report of the IGF's pilot project on standards published before the coalition's launch in 2020, as potential areas for future research:

- other security by design topics;
- consumer protection testing;
- the need for global testing of ICT products and services, and vulnerability reporting;

- developing a fair system for the "faming, naming and shaming" of the security of specific network devices and services.

With regard to consumer protection generally, some initial soundings have been made by IS3C's leadership team about consumer awareness of Internet security standards and regulatory responses relating to the security of devices. Discussions with consumer bodies will continue in the spring of 2022 with a view to scoping the potential remit of a new working group on consumer protection.

Stakeholders are invited accordingly to submit proposals to the IS3C leadership team for new IS3C workstreams that are relevant to the overarching objective of achieving more rapid and widespread deployment of security-related Internet standards and relevant best practice.

4. *How to contact the IS3C coalition about joining its working groups*

If you are considering joining the IS3C and participating in the deliberations of any of its working groups, please send a message to Wout and Mark at DC-ISSS@intgovforum.org.

Stakeholders can become an IS3C member simply by subscribing to the email list: http://intgovforum.org/mailman/listinfo/dc-isss_intgovforum.org.

Wout de Natris - IS3C Coordinator

Mark Carvell - IS3C Senior Policy Adviser

21 January 2022