IS3C: achievements and plans

The UN Internet Governance Forum's Dynamic Coalition on Internet Standards, Security and Safety Coalition (IS3C) was launched at the virtual IGF in 2020. Its goal is both simple and complex: to achieve the widespread, rapid deployment of existing, security-related Internet standards and relevant ICT good practices in order to make online activity and interaction more secure and safer. In just three years this multistakeholder coalition of experts has grown to comprise eight working groups, with remits to produce reports, recommendations, guidelines and toolkits that will contribute to making the digital world more secure and safer. You can read here what was achieved and learn of our plans for 2024 and beyond, including the development of an IGF Cybersecurity Hub which will bring industry and tertiary cyber security education representatives together to collaborate in addressing gaps in professional cybersecurity skills.

Main recommendations of IS3C's reports

IS3C working groups have produced three reports during the last 12 months on security by design for the Internet of Things (WG 1), on cybersecurity education and skills (WG 2), and on procurement and supply chain management as drivers for the adoption of security-related standards (WG 3) IS3C has also published a paper on how its work contributes to achieving the UN's Sustainable Development Goals (WG 4). All these reports can be found on our website at www.is3coalition.org and the tools for implementing the Working Groups' recommendations will become available in the coming months (WGs 5 and 8). A report on data governance (WG 6) will be published shortly.

WG 1's research compared IoT policy documents from 18 countries and found over 440 best practices and variations. The analysis of these concluded that there is a need for greater coordination between countries on policy and best practice, and also on taxonomy. These findings and other recommendations are described in more detail in WG1's report which was published during the IGF in Kyoto.

WG 2 published its initial report on education and skills during the previous IGF in Addis Ababa in 2022. Its key recommendation was to bring together stakeholders in the cyber sector to address the gaps in knowledge and skills in general and more specifically relating to cybersecurity standards and related ICT practices that students have when they enter the cybersecurity sector.

WG 3's report compared public sector procurement documents and practices in various countries and found that most documents did not mention cybersecurity and if they did they did not refer to standards. Its recommendations for addressing this opportunity for procurement contracts to drive the implementation of security standards are set out in its report.

The overarching issue of standards recognition

One major overarching issue stands out from this body of work: open source Internet standards and related ICT best practices are generally not recognized by governments and as a result they are omitted from almost all governmental publications and tools.

This is surprising, given the fact that these standards are what makes all modern communications work and are integral to the core of the Internet which governments consider as an essential public good that should not be vulnerable to attack. The focus in debates about cybersecurity, aside from mitigation of incidents and threats, is usually on the physical components of the Internet's infrastructure, i.e. the servers and undersea cables, etc, not on the technical standards relating to security and safety of Internet users. These standards include the Internet Protocol, email protocol, routing protocol, transport protocol and the domain name system. Without them all Internet communication would be impossible. They all have two things in common: a) they are the global standards and b) they were made in the early days of the Internet's development and evolution when, as "the father of the Internet", Vint Cerf points out, ensuring the security and safety of Internet users was not a major concern or objective. This is largely because it was not envisaged at that time that "the Internet would become the global super information highway we know today" that has the potential to connect the entire population of the world with a myriad range of applications that create both unprecedented opportunities and new risks and threats to personal and corporate security and welfare.

The technical community has since then recognised the need to augment and update these protocols in order to fix their deficiencies and flaws. The Internet industry and manufacturers have to deploy this new generation of standards but as IS3C's research shows, this does not consistently and effectively happen and Internet users worldwide continue to be exposed to unnecessary threats and attacks.

IS3C members believe that if more public and private sector organisations were to require the deployment of these important security standards when procuring their ICTs or renegotiating existing contracts with suppliers, the world would become far more secure and safer. Formal recognition of the critical importance of these protocols appears to be a serious challenge for governments in particular, as shown by IS3C's analysis of their procurement practice. Hence we provide the following solution: It suffices when all large organisations, public and private, from now on demand them when procuring. Currently, there is no incentive for the ICT industry to deploy these protocols: in fact there are only negative incentives because there is little to no demand. The organisations who currently do deploy these protocols in their Internet devices and network applications, incur higher costs, making them more expensive than those who do not. Furthermore, they do so knowing that they are still insufficiently protected as long as other entities in their networks do not deploy them as well.

This means that there is a significant first mover disadvantage and a lack of a level playing field in the market for more secure devices and applications. IS3C believes that the widespread adoption of a security-focussed procurement practice will drive demand for more

secure products and this will address the cost disincentives. IS3C therefore recommends all organisations to start procuring devices and applications that are secure by design by requiring standards to be implemented in the products they purchase whether it be in hosting or email services, or the acquisition of a website or a tool with an ICT component such as a printer or an Internet-connected coffee machine.

This is the reason why IS3C has asked a team of independent experts to develop two toolkits that would provide both public and private sector organisations with guidance when procuring. First, a list of the 23 most important open source standards. This will be published in December 2023. This list is intended for use as a reference point by any organisation wanting to procure devices and applications that are secure by design. Secondly, a narrative tool on security standards is being written, which we believe will empower technology officers and technical advisers in administrations and companies with the arguments they need to convince their boards and senior executives either to deploy these standards or to procure them even if it means incurring higher costs for the organisation.

New areas of IS3C work in 2024

IS3C announced the plans for its future work programme at the 2023 IGF in Kyoto. This comprises two workstreams. The first is a new working group focusing on emerging technologies (WG 9). It will start on artificial intelligence with the aim of carrying out a global comparison of policy initiatives at the national, regional and international level. If sufficient funding is found, this work will be presented at the 2024 IGF in Riyadh.

IS3C also plans to start work on consumer advocacy and consumer protection in 2024, as well as on responsible disclosure.

The Cyber Security Hub

The second body of work focuses on the bigger challenge. IS3C's goal is to have the Internet standards and related ICT best practices deployed on a global scale. To move from theory to practice, IS3C announced the concept of a new Cybersecurity Hub under the aegis of the UN IGF at the 2023 EuroDIG regional IGF meeting in Tampere and at the IGF in Kyoto. The goal is to bring cybersecurity experts together in this hub, in order to work together to develop solutions and enhance the capacity to solve the challenge of greater online security. The first area of focus will be on education and skills, in order to close the gap between the offer in tertiary cyber security curricula and the demand from industry and society as a whole. The goal is to present the first outcome of this work at the IGF in Riyadh.

Open invitation

As an open invitation to you, we point out that anyone with an interest in driving ICT security forward, can approach us to suggest a new working group. There's one caveat, it has to be within the scope of IS3C. Just reach out and we will take it from there.

Support

IS3C's aims for achieving greater online security and safety cannot be achieved without the support and commitment of stakeholders, in all regions, through their active participation in the coalition's working groups, contributing their expertise and experience to the development of policy recommendations, guidelines and toolkits. We also need your support for and recognition of the reports at the global level. Without such support the outputs of IS3C's working groups will lack the necessary credentials and credibility for their outcomes to be recognised, endorsed and reach a decisive level of influence. Financial support is also necessary for the conduct of the coalition's research projects and development of capacity building programmes. This will facilitate the hiring of expert consultants to lead the research and development and cover essential administrative costs.

Haarlem, 23 November 2023

Wout de Natris — Coordinator

Mark Carvell — Senior policy advisor

IS3C: Making the Internet more secure and safer