IS3C'S CONTRIBUTION TO THE UNITED NATIONS SUSTAINABLE DEVELOPMENT GOALS

INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)

MAKING THE INTERNET MORE SECURE AND SAFER

OCTOBER 2023 VERSION 2.0
INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)
info@is3coalition.org
BY

ABRAHAM FIIFI SELBY (IS3C) & OLÉVIÉ KOUAMI

IS3C'S CONTRIBUTION TO THE UN SUSTAINABLE DEVELOPMENT GOALS

Introduction

The IGF's Dynamic Coalition on Internet Standards, Security, and Safety (IS3C) is a collaborative multi stakeholder initiative with the aim of making the Internet more secure and safer through more effective and rapid deployment of existing Internet standards and related best practices. This paper describes how the coalition's objectives and areas of work contribute to achieving the UN Sustainable Development Goals (SDGs).

IS3C's Objectives

The objectives of the IS3C in the context of the UN SDGs are:

- to promote a secure and resilient Internet infrastructure that supports sustainable development.
- to create greater awareness of the importance of deploying existing global Internet standards that enhance online security, safety, and data privacy.
- to support international cooperation and collaboration to address Internet-related challenges hindering the achievement of the SDGs.

By advancing wider deployment of Internet standards that establish greater online security, safety, and data privacy, IS3C supports the establishment of a digital environment that empowers individuals and communities, fosters innovation, and accelerates progress towards a more sustainable and equitable future. Much of the coalition's work is accordingly directly relevant to achieving several SDGs, as explained in this paper..

ABOUT THE INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)

Effective governance of the Internet is necessarily underpinned by global respect for security standards that build trust in the online environment and contribute to the safety of Internet users. The Dynamic Coalition on Internet Standards, Security and Safety (IS3C) brings together expert stakeholders from all regions 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 related ICT best practices. In this way IS3C will ensure that standards and best practices contribute a greater role in addressing current and evolving cybersecurity risks in the global digital economy.

IS3C's work is undertaken by a series of Working Groups, each with specific expertise in key policy areas of cybersecurity including security by design, cybersecurity skills, procurement, data governance and emerging technologies. The principal aims of the working groups are:
i) to research and analyse gaps in the critical supply and demand factors of cybersecurity.
ii) to identify the best options for the deployment of key standards and best practices to address these gaps.
iii) to publish and disseminate worldwide the outcomes of their work in the form of policy recommendations, practical guidance, and policy toolkits.
iv) to translate the theory of security into the practice of actual deployment, e.g. in capacity-building programmes and training.

ABOUT THE UNITED NATIONS SUSTAINABLE DEVELOPMENT GOALS (SDGs)

The United Nations Sustainable Development Goals (SDGs) are a set of 17 interconnected objectives designed to address some of the most pressing global challenges. These goals were adopted by all United Nations Member States in September 2015 as part of the 2030 Agenda for Sustainable Development. The agenda provides a shared blueprint for peace and prosperity for people and the planet, aiming to be achieved by the year 2030. The SDGs build upon the successes of the Millennium Development Goals (MDGs) while expanding their scope to encompass a broader range of economic, social, and environmental issues.

The goals are interconnected, meaning that progress in one goal can positively impact progress in others. Monitoring and reporting on progress are a crucial part of the agenda to ensure accountability and transparency. They are intended to be universally applicable, meaning that all countries, regardless of their level of development, are expected to work toward achieving them. Governments, inter-governmental organisations, businesses, technical bodies, civil society, and individual citizens all have roles to play in achieving the SDGs. Achieving these goals requires collective global efforts and cooperation to address issues such as poverty, inequality, climate change, environmental degradation, and more, with the aim of creating a more sustainable and equitable world for current and future generations.

THE RELEVANCE OF IS3C's WORK TO THE SDGs

IS3C's aim to make the Internet more secure and safer is relevant to achieving all the SDGs. All economic and social actions in support of sustainable development will to some extent involve the use of the Internet and reliance on its protocols and the devices and applications connected to the Internet. The more secure and reliable communications become, the more likely a positive outcome will be within reach. Trust is one of the most important requirements of effective cooperation and more security and safety in communications provide a more trusted environment for greater cooperation and (economic) development.

It is important that the public core of the Internet[1], namely the central protocols and infrastructure, supports the global public good. Currently, the standards that make the Internet function are under attack, abused and misused 24 hours a day, 365 days a year. This makes recognition of these standards by public and private sector organisations of crucial importance and the need to update them with the latest security requirements, highly relevant to achieving success in achieving the following SDGs.

SDG 3: Digital applications and services increase social well-being, provision of health services, the protection of democratic freedoms and the spread of economic opportunities created by digital and Internet technologies. By addressing the current gaps in the deployment and implementation of cybersecurity technical standards, IS3C contributes to creating a more secure, safe, and trustworthy global online environment so that all the world's citizens can fully enjoy these benefits on an equal basis.

SDG 8: Only if there is greater security, safety and trust online can digital and Internet technologies contribute to inclusive and sustainable economic growth and the creation of new opportunities for employment. IS3C's work to address significant gaps in the deployment of cybersecurity standards contributes to achieving this important objective.

SDG 9: IS3C's work to achieve a more resilient and secure digital infrastructure through wider, more effective and more rapid deployment of relevant technical standards, serves ultimately to promote sustainable industrialisation and to foster innovation.

[1] 'The public core of the internet. An international agenda for internet governance'.(The Hague, WRR report 94, 2015)
https://english.wrr.nl/publications/reports/2015/10/01/the-public-core-of-the-internet

SPECIFIC AREAS OF CURRENT IS3C WORK THAT ARE RELEVANT TO THE SDGS

IS3C WORKING GROUP 1: SECURITY BY DESIGN

The IS3C membership agreed that promoting security by design should be a key objective for the coalition. Security on the Internet of Things (IoT) is crucial not only for technological advancement but also for addressing global challenges and improving people's lives. It was decided therefore that the first phase of WG1's work should focus on security by design of the Internet of Things (IoT) by:

1. reviewing current security related IoT initiatives and practices worldwide.
2. developing a coherent package of global recommendations and guidance for embedding security by design in the development of IoT devices and applications.

The working group's report of its recent research with recommendations for policymakers and cybersecurity guidance for IoT providers and users, was presented at the IGF in Kyoto[2].

In addressing the gap between the theory of cybersecurity and the current reality of ineffective practice and lack of widespread and rapid deployment of key standards, the activities of WG1 are directly relevant to the following SDGs:

SDG 3: Good Health and Well-being: implementing strong security measures in healthcare IoT devices and systems can protect patients' sensitive data and ensure the reliable operation of critical medical equipment, thereby promoting good health and well-being.

SDG 9: Industry, Innovation, and Infrastructure: security standards and best practices for IoT devices and networks can foster innovation and promote the growth of the IoT industry, contributing to infrastructure development.

SDG 11: Sustainable Cities and Communities: by ensuring the security of IoT devices used in smart cities (e.g., for traffic management, waste management, and energy efficiency), can help create safer and more sustainable urban environments.

Following the conclusion of WG1's current focus on IoT, IS3C will undertake research in 2024-25 in security by design relating to other existing and emerging digital technologies which will likewise have significant positive benefits for sustainable development.

IS3C WORKING GROUP 2: EDUCATION AND SKILLS

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 to understand the benefits of security-related Internet standards and ICT best practices. For ICT security to be better understood, it must be integrated into tertiary ICT educational curricula, at all levels. This may result in the structural development of ICT(-related) products and services that include cyber security, Internet standards and ICT best practices.

[2] Working groups website https://is3coalition.org/working-groups/ .

Improving education and skills to increase cybersecurity for the individual and the cybersecurity sector will therefore contribute directly to SDG 3 on social well-being and access to reliable and sustainable healthcare, to SDG 8 on inclusive and sustainable growth and to SDG 9 on sustainable industrialisation and innovation.

WG2's work will also contribute indirectly to SDGs 1, 4, 5, 10 and 16. In particular, enhancing the digital skills of citizens, especially in developing countries, will help level the economic playing field (SDG 1) and as more citizens and services embrace digital technology, cybersecurity will become more crucial than ever, and the ensuing employment opportunities will help eliminate disparities as a broader population can benefit regardless of gender or physical capacity (SDGs 4 and 5). Furthermore, improved cyber skills, and better cybersecurity and data validation mechanisms should contribute to increasing access to quality lifelong educational opportunities for all (SDG 4).

Secure networks and a better skilled population are essential in eliminating many forms of discrimination and exploitation that are currently increasing rather than diminishing, according to Europol (SDG 5).

SDG 10 relating to equal opportunities and SDG 16 on institutional strengthening are also dependent to some degree on the security of the digital infrastructure and more especially the digital skills of all sectors of the population worldwide.

IS3C WORKING GROUP 3: PROCUREMENT AND SUPPLY CHAIN MANAGEMENT

The focus of the third IS3C working group is on the opportunity to promote the business case for cybersecurity through the inclusion of security-related technical standards in public sector procurement contracts and in supply chain management practice in the private sector. The outcomes of the work undertaken in 2023 to develop actionable and practicable policy recommendations and guidance to ensure that public sector procurement and private sector supply chain best practice and related professional training considers Internet security and safety requirements, was presented at the IGF in Kyoto[3].

In potentially contributing to infrastructural capacity building in the Global South, this work is directly relevant to SDGs 3 and 9, and indirectly to SDG 16 regarding increasing the effectiveness and resilience of institutional capacity in the public sector.

IS3C WORKING GROUP 5: PRIORITISING AND LISTING EXISTING SECURITY-RELATED INTERNET STANDARDS AND ICT BEST PRACTICES

In order to become more proactive where prevention of online harms is concerned, public and private sector organisations need to demand the deployment of a wide range of key security-related Internet standards and ICT best practices by developers and manufacturers of Internet devices, services and applications. These standards and practices will need to be deployed because they all contribute to a more secure Internet and greater safety in the use of ICT services, devices, and applications. At the same time dependency on the mitigation of incidents will decline.

IS3C is accordingly drawing up for the use of decision-takers and procurement agencies a list containing the most important and relevant Internet standards and related best practices. This will assist them in determining their

[3] Our report https://is3coalition.org/reports-resources/

specific Internet security and safety requirements and enable procurement agencies to identify which secure ICT products, services and devices they should select, making their organisations and the cyber networks more secure and safer. An initial draft of the list was presented for consultation at IGF 2023 in Kyoto with the aim of finalising it for publication in December 2023. .

The outcomes of WG5[4] will therefore contribute to achieving SDGs 3 and 9 in relation to enhancing social and economic well-being founded on a more secure and resilient digital infrastructure.

IS3C WORKING GROUP 6: DATA GOVERNANCE

Data and related issues and developments in the public sector have become increasingly important in terms of government analysis and operations, academic research, and real- world applicability and acceptance. Data is now integral to every sector and function of government, as essential as physical assets and human resources. Much of the operational activity in government is now data-driven, and many governments would find it difficult, if not impossible, to function effectively without data.

In accordance with a contract with the UN Department of Economic and Social Affairs (UNDESA), WG 6 presented its report on data governance practices for publication at the 2023 IGF[5]. This includes policy recommendations relevant to SDG 3 in creating a more secure, safe and trustworthy global online environment that enhances social well-being and economic opportunities based on secure and free-flowing exchanges of data.

IS3C WORKING GROUP 8: DNSSEC AND RPKI DEPLOYMENT

Two of the fundamental building blocks of the Internet are the domain name system (DNS) and the system of routing that allows Internet traffic to flow between users' devices and websites. Both routing and the DNS are older technologies from a more innocent age, and neither was designed with any built-in security mechanisms. To achieve greater security in the DNS and the routing system and increase resilience against malicious attacks and risks of large-scale data theft, the engineering community developed two protocols: Domain Name Security Extensions (DNSSEC) and the Resource Public Key Infrastructure (RPKI).

WG8 focusses on outreach and engagement efforts to increase trust in and contribute to the wider deployment of both critical protocols with the aim of enabling public and private sector decision takers to deploy them effectively in their respective organisations. It does by focusing on the narrative that will allow individuals in leadership-positions to decide to procure secure by design.

The outcomes will potentially provide important inputs into achieving SDG 3 in creating a more secure, safe and trustworthy global online environment that enhances social well-being and economic opportunities; SDG 8 with regard to sustainable economic growth; and SDG 9 concerning sustainable and innovative industrialisation based on secure and resilient digital infrastructure.

IS3C WORKING GROUP 9: GOVERNANCE OF EMERGING TECHNOLOGIES: QUANTUM & AI

[4] Working group 4 is responsible for external communication and e.g. this report and IS3C's input in the Global Digital Compact process.
[5] https://is3coalition.org/docs/is3c-contribution-to-un-gdc/

Breakthrough developments in quantum computing and artificial intelligence (AI) have led to recent global policy making efforts and discussions regarding governance issues. The critical security implications of these technologies require further attention of stakeholders as these technologies continue to advance and be commercialised.

The goals of IS3C's new working group on emerging technologies in 2023-24 include:

- raising awareness of the security and safety issues relevant to policy decisions for Quantum and AI technologies.
- investigating emerging issues that would require the attention of stakeholders, with input from the public and private sectors, including the technical community, and from civil society.
- developing policy recommendations and guidelines as IGF outcomes that will assist governments, regulators and private sector entities in policymaking and standard-setting efforts relating to quantum and AI governance.

The outcomes of WG9 on the issues relating to security standards and related practices for quantum and AI technology development will potentially contribute therefore to SDGs 3, 8 and 9 in ensuring the global infrastructure for these transformative technologies is secure, safe and trusted so that it enhances social well-being and economic opportunities and supports national and regional development strategies.

LINKS AND CONTACTS FOR FURTHER INFORMATION ABOUT IS3C

Website: *https://is3coalition.org*
Email: *info@is3coalition.org*

Authors:

Abraham Fiifi Selby (Chair SDG Working Group, IS3C)
Olévié Kouami (Vice Chair – Communications WG, IS3C)
Wout de Natris (Coordinator IS3C)
Editorial assistant: Mark Carvell (Senior Policy Advisor, IS3C)