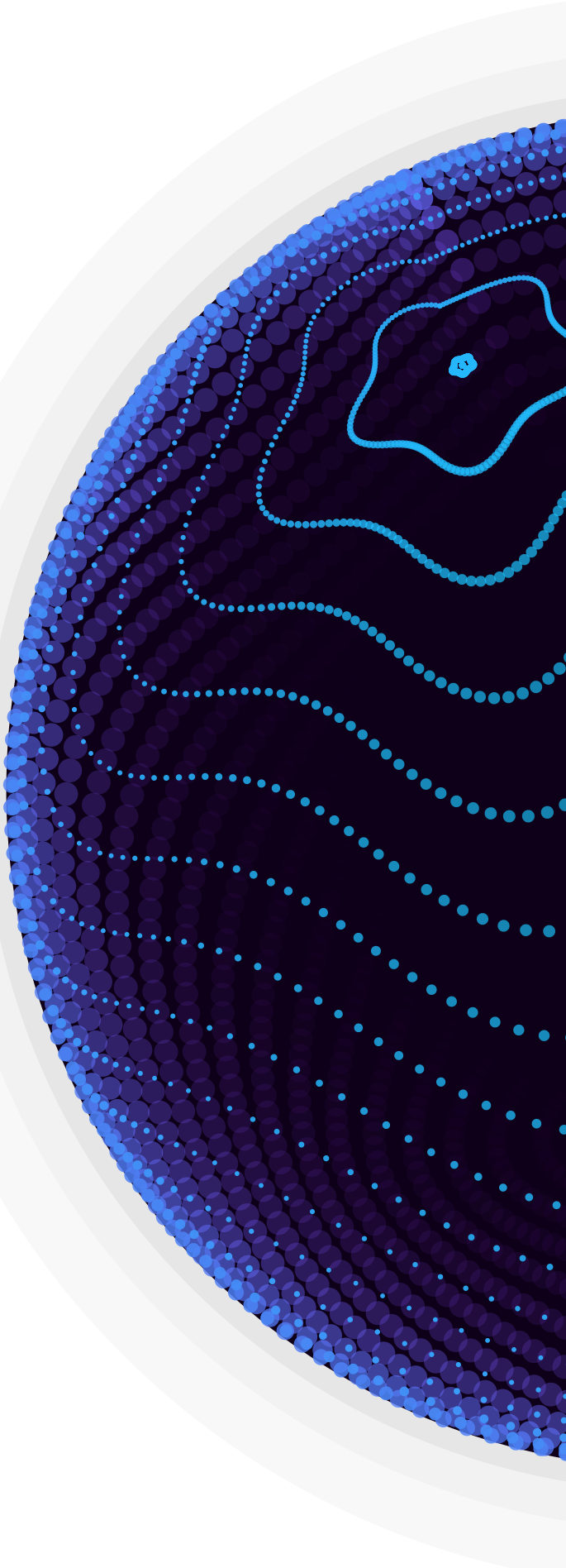
Geneva Dialogue

ON RESPONSIBLE BEHAVIOUR IN CYBERSPACE



GENEVA MANUAL

On Responsible Behaviour in Cyberspace

Implementation of Norms of Responsible Behaviour in Cyberspace by Relevant Non-State Stakeholders

7 December 2023

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Federal Department of Foreign Affairs FDFA

REPUBLIQUE ET CANTON DE GENEVE

DiPLO

EPFL CENTER FOR DIGITAL TRUST

UBS

swisscom

Contents

Executive summary

The Geneva Dialogue on Responsible Behaviour in Cyberspace, established by the Swiss Federal Department of Foreign Affairs and led by DiploFoundation with the support of the Republic and State of Geneva, Center for Digital Trust (C4DT) at EPFL, Swisscom, and UBS, addresses the roles and responsibilities of relevant non-state stakeholders in ensuring the security and stability of cyberspace. Emphasising the principle of 'shared responsibility', the Geneva Dialogue focuses on operationalising the UN cyber norms by the private sector, academia, civil society, and the technical community to contribute to global cyber security and peace. The results are published in the ***Geneva Manual***, the key outcome of the Geneva Dialogue, reflecting contributions from over 50 entities and experts around the world. The Geneva Manual documents stakeholders' understanding of the UN cyber norms, their agreements and disagreements on particular aspects of their implementation, and provides guidance for international collaboration, while outlining the related good practices. Thus the ***Geneva Dialogue makes an important contribution to the international discussions, including in the UN Open-ended working group (OEWG), by advancing the implementation of the agreed norms and promoting responsible behaviour in cyberspace.***

The inaugural edition of the Geneva Manual focuses on the implementation of the two norms related to ICT supply chain security and responsible reporting of ICT vulnerabilities (UN GGE norms 13i and 13j), thus building on earlier results of the Geneva Dialogue to collect good practices by industry and private sector in reducing vulnerabilities in digital products and securing their design and development.

The Geneva Manual highlights the diverse perspectives of non-state stakeholders, emphasising ***the importance of multistakeholder participation in the implementation of norms***. The inaugural edition identifies areas of agreement and divergence among non-state stakeholders. Some of the key messages include:

- *Norms operationalisation:* Geneva Dialogue experts recognise the importance of cyber norms, and outline that practical actions, inclusive policies, and good governance are essential for global approaches to ICT supply chain security, responsible reporting of ICT vulnerabilities, and security of digital products and ICTs.

- *The role of the private sector*: The private sector is understood by the Geneva Dialogue experts to play a major role in the development of secure digital products and ICTs, and reducing ICT vulnerabilities in the supply chain (through adopting security-by-design, and cooperating with others for responsible vulnerability disclosure, among other measures).

- *The role of the civil society*: Non-government organisations play an important role in alerting about exploitation of ICT vulnerabilities for the infringement of human rights and privacy, and put pressure on vendors to ensure more secure products, on policy makers to develop regulations and policies, and on users to demand more secure products and implement safety and security measures. Academic and research organisations contribute with mapping legal, technical and political challenges and solutions, and raising critical questions related to the implementation of the norms.

- *The role of the open-source software (OSS) community*: While the Geneva Dialogue experts agreed, in principle, that OSS developers should not be held accountable for vulnerabilities in their free products, they emphasised the important role the OSS community could play in reducing vulnerabilities throughout the ICT supply chain, through embracing secure development practices, supporting developers in vulnerability identification and

disclosure, and cooperating with other stakeholders in implementing their respective roles.

- *Government leadership*: In order to implement their respective roles and responsibilities outlined in the Geneva Manual, non-state stakeholders expect governments to lead by example in implementing cyber norms, including through creating an inclusive and enabling regulatory and policy environment, but also through enhancing transparency in disclosure and management of ICT vulnerabilities discovered by, or reported to, the public authorities and the security sector.

- *Geopolitical challenges*: To mitigate the challenge that geopolitical tensions and technological competition pose for the implementation of norms – in particular, the norm 13i related to ICT supply chain security – the Geneva Dialogue experts emphasise the need for a global approach to the implementation of norms, not least through the enhanced cooperation among public and regulatory authorities, in order to harmonise their rules, policies, and operations across jurisdictions.

At the same time, the Geneva Manual raises critical questions for future discussions, including but not limited to, the role and responsibility of citizen customers in implementing cyber norms; enhancing accountability of private and state actors exploiting vulnerabilities; and feasibility of developing global rules for ICT supply chain security in the current global context of increasing technological and economic competition between countries.

The Geneva Dialogue will continue discussions on these open questions, and clarify the respective roles and responsibilities of stakeholders in the implementation of the UN framework on responsible behaviour and cyber norms, in particular. Interested stakeholders are invited to contribute to future work of the Geneva Dialogue.

1 Context: What is the Geneva Manual?

In 2004, beginning with the first United Nations Group of Governmental Experts (GGE) on information and communications technology (ICTs), states started debating how to behave in cyberspace. Much has happened since. States agreed that international law applies in cyberspace and have agreed to eleven norms for responsible state behaviour in cyberspace. Meanwhile, outside the UN system, states and regional organisations have developed their own rules and have published numerous confidence building measures (CBMs), as listed in the IGF BPF report. This demonstrates that states indeed see cyberspace as an important asset and, furthermore, a place that should remain peaceful.

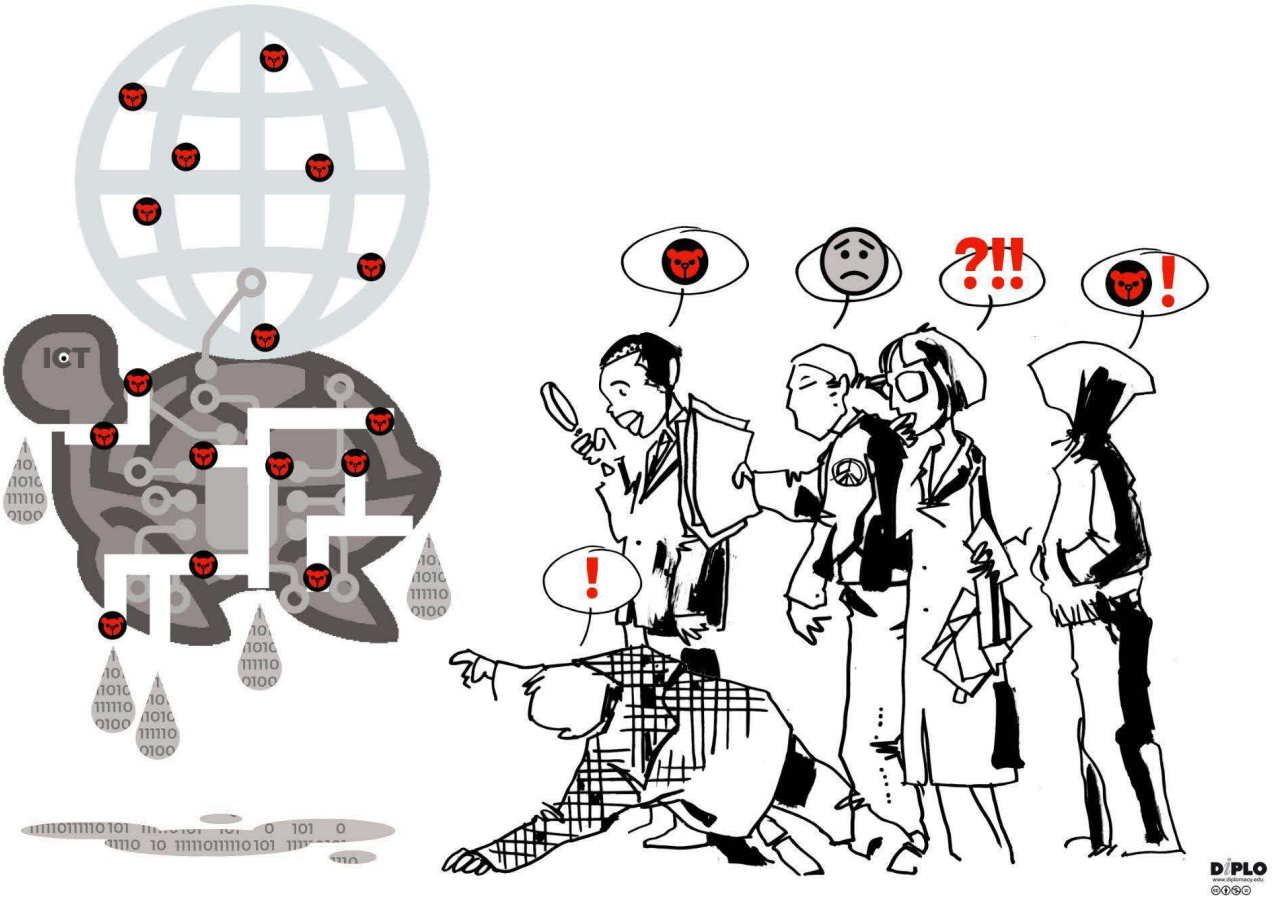
However, the ICT infrastructure that makes the digital space such a unique and valuable place is neither owned or operated by states, nor do states have the sole ability to govern it, due to its transnational nature. In fact, most of the ICT infrastructure is owned and operated by thousands of private companies, which also produce the devices, from traditional computers to medical devices, connecting to, and utilising the internet. In addition, technical community sets the standards and has the hands-on knowledge and expertise on running and securing the ICT environment, while civil society, with its broad understanding of social and economic context, wide networks, and ability to reach out to end-users, plays and can play an important role to enhance citizens' awareness and advocate for their safety and rights.

These stakeholders are often only spectators to the normative processes by states, yet, in the end, play an important role for the implementation of these diplomatic agreements.

Meanwhile, digital products are ubiquitous and underpin the functioning of modern society. The fact that they can be vulnerable means they can be abused by other actors for malicious purposes. This raises security concerns at various levels – from the security of particular users, to matters of international peace and security. States carry primary responsibility for security of its citizens and infrastructure; however, this responsibility is not absolute, as it is clear that they cannot meet these expectations about cyberspace without engaging with other actors: a cooperation between states, private sector, academia, civil society, and technical community is required to ensure an open, secure, accessible, and peaceful cyberspace.

Norms of responsible behaviour in cyberspace, adopted within the UN and which are further discussed in the UN Open-Ended Working Group (OEWG), give common guidance to what states are expected to do to ensure stability of cyberspace, including the security of digital products. But what are these other actors expected to do to support the implementation of those norms? Where and how can they support states in ensuring the security and stability of cyberspace, along with promoting responsible behaviour in it? What challenges may they face along the way, and how to address them through dialogue with states and other stakeholders?

The Geneva Dialogue on Responsible Behaviour in Cyberspace (Geneva Dialogue) was established by the Swiss Federal Department of Foreign Affairs and led by DiploFoundation with the support of the Republic and State of Geneva, Center for Digital Trust (C4DT) at EPFL, Swisscom, and UBS to analyse the roles and responsibilities of various actors in ensuring the security and stability of cyberspace. In this context, the Geneva Dialogue stems from the principle of 'shared responsibility' and particularly asks how the norms might be best operationalised (or implemented) by relevant actors as a means to contribute to international security and peace.



Concretely, the Geneva Dialogue investigates the consequences of agreed upon norms for relevant non-state stakeholders from the private sector, academia, civil society, and technical community, and tries to clarify their roles and responsibilities. It does not aim to find consensus, but to document agreement or disagreement on the roles and responsibilities as well as concrete steps each stakeholder could take, and the relevant good practices as examples. For this, the Geneva Dialogue has invited over 50 experts and representatives of stakeholders around the world (further referred to as Geneva Dialogue experts throughout the document) to discuss their roles and responsibilities, and the implementation of cyber norms in this context. The results – published in the form of the Geneva Manual – offer possible guidance for the international community in advancing the implementation of the existing norms and establishing good practices. The Geneva Manual also reflects the diverse views of relevant non-state stakeholders and outlines some of the open questions to which the Dialogue has yet to provide answers, but which are important for a better understanding of challenges by states.

The inaugural edition of the Geneva Manual focuses on the two norms related to the supply chain security and responsible reporting of ICT vulnerabilities. In the coming years, the Dialogue will continue discussing the implementation of other norms to expand the Geneva Manual. In section 2, we explain our approach and share more information about the particular norms we focus on.

We invite all interested stakeholders to join us on this path to collect ideas, core challenges, opportunities, and good practices for relevant non-state stakeholders to implement the existing norms, and collectively help make cyberspace more secure and stable. The Geneva Manual remains open to comments and suggestions at *genevadialogue.ch*, and will be continuously updated to reflect the changes driven by the rapid development of technologies.

2 Main concepts

Before we discuss the implementation of norms in cyberspace, let us introduce some of the concepts and terms which will be used throughout the Geneva Manual.

First, we should clarify what the '***norms of responsible behaviour in cyberspace***' are. These norms are a part of the ***UN cyber-stability framework***, created by the UN GGE[1] (mentioned earlier), and later endorsed by all UN Member States to encourage responsible conduct among nations in cyberspace. Besides the non-binding eleven cyber norms, the framework includes three foundational pillars: binding international law; various confidence-building measures, particularly those to strengthen transparency, predictability and stability; and capacity building.

The framework, agreed upon by states, focuses on regulating ***state*** conduct in cyberspace. While it acknowledges the role of various stakeholders, it provides limited guidance on their roles and responsibilities, leaving room for ambiguity regarding their expected actions as well as further work to unpack the norms into coherent practices and actions.

These various ***relevant non-state stakeholders*** include representatives of the private sector and industry, academia, technical community, and civil society.

Despite the voluntary nature of the eleven norms, they are foundational as a part of the framework encouraging states to reduce the risk of cyber conflicts, and promoting stability and cooperation in cyberspace.

UN cyber norms, ASPI

[1] UNGGE 2013, 2015 and 2021 reports provide the basis for the UN cyber-stability framework.

Given that the norms and framework do not extensively cover the roles and responsibilities of relevant non-state stakeholders, the Geneva Manual aims to bridge this gap by focusing on how such actors can implement cyber norms, as a step to further enhance stability and security in cyberspace.

The inaugural edition of the Geneva Manual begins with two norms concerning supply chain security (#9) and responsible reporting of ICT vulnerabilities (#10). These norms follow the Geneva Dialogue's previous discussions on digital product security and the roles industry and various actors play in ensuring it.

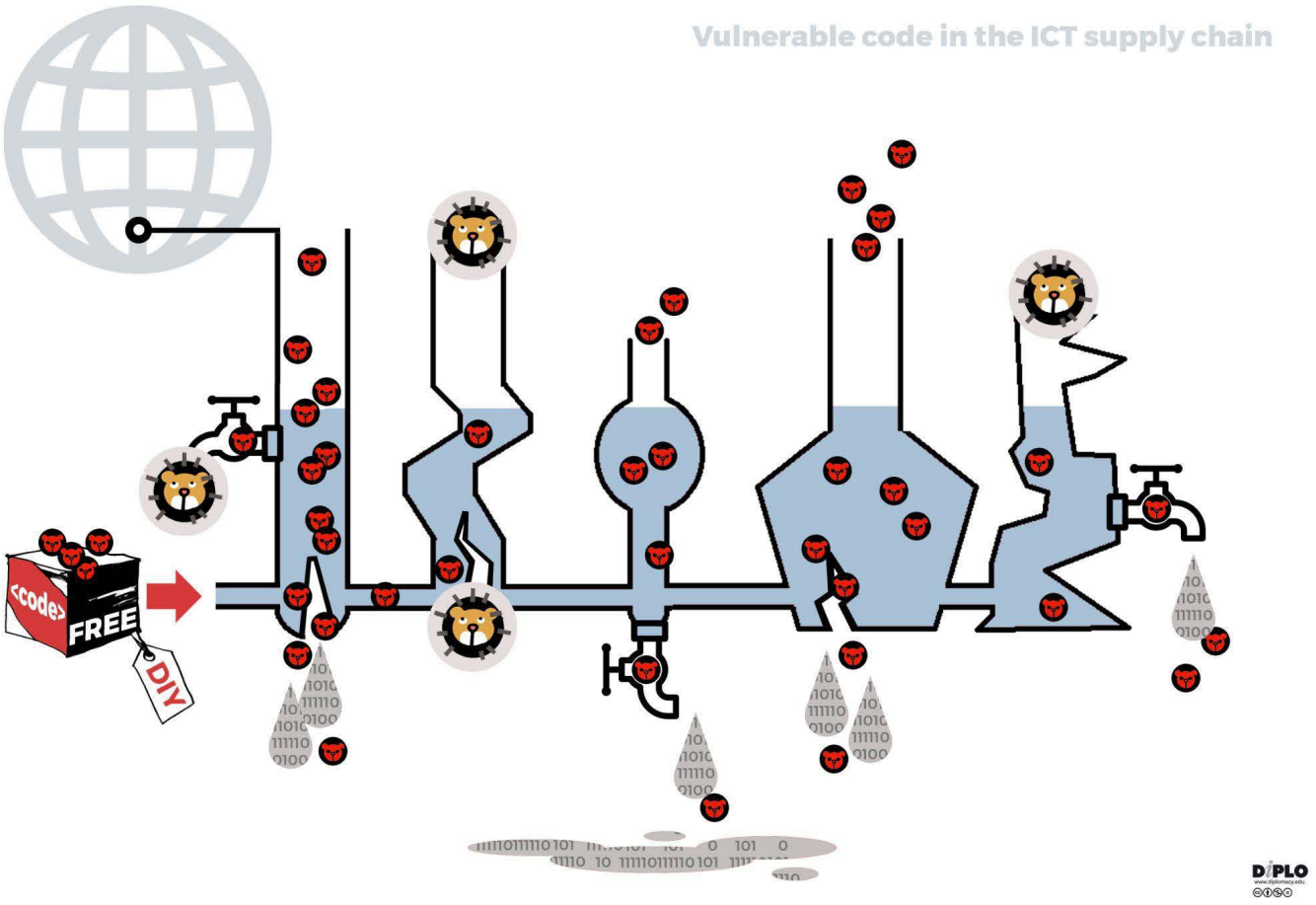
Unpacking these two norms and expectations from relevant non-state stakeholders, the Geneva Manual introduces more specific roles (for example, manufacturers of digital products, code owners, vendors, researchers, etc.). The Geneva Manual uses the term '***digital products***' and understands them as software, hardware, or their combination, and such products are characterised by (i) containing code; (ii) ability to process data; or (iii) ability to communicate/ interconnect. Though they are not necessarily synonyms, for simplicity, the terms 'digital products' and 'ICTs' are used interchangeably in the Geneva Manual.

In this context, ***manufacturers***, ***vendors, or service providers*** include a company or an entity that produces or provides digital products and services, or ICTs. A ***code owner*** can be a vendor and a manufacturer in cases where they are responsible for developing and maintaining software code embedded in a final digital product; a particular group of code owners are those engaged with producing the open source software (OSS). ***Researchers*** include individuals or organisations who discover vulnerabilities or any other security flaws in digital products with the intention to minimise the security risks for users of such products.

Vulnerability disclosure is an overarching term which the Geneva Manual uses to describe the process of sharing vulnerability information between relevant non-state stakeholders. Vulnerability disclosure can be ***coordinated*** (***CVD***) in cases where several parties need to exchange information in order to mitigate the vulnerability and reduce security risks.[2] ***ICT vulnerability, or vulnerability in digital products,*** implies a weakness or flaw in such products that can potentially be exploited by malicious actors to get unauthorised access to ICT system or infrastructure, and/or lead to unintended system failures.

Manufacturers and their suppliers form the core of a complex network of ***ICT supply chains*** that encompasses various components and products, and involves multiple stages and stakeholders, from the initial design and manufacturing of digital products to their distribution, installation, maintenance, and eventual disposal and recycling. The primary goal of ICT supply chains is to ensure the efficient production, delivery, and support of digital products/ICTs to meet the demands of customers and end users. ICT supply chains, however, bring about a complex web of interdependencies of digital products, and thus also allow for vulnerabilities in some to penetrate throughout the supply chain rendering it insecure.

2 Security of digital products and services: Reducing vulnerabilities and secure design. Industry good practices. Geneva Dialogue report, 2020. https://genevadialogue.ch/wp-content/uploads/Geneva-Dialogue-Industry-Good-Practices-Dec2020.pdf



Organisational customers of digital products include the entities who procure, purchase, and use digital products in their day-to-day operations, as well as provide further digital or non-digital services to other consumers or end-users. Such customers include various organisations of different sizes, with different resources and cybersecurity knowledge to address cyber threats. However, organisational customers should be perceived differently from ***citizen customers of digital products (i.e. end-users)***, who refer to individuals who use digital products and normally do not have any cybersecurity knowledge to address cyberthreats. ***Civil society*** refers to a broad set of non-government organisations including associations representing the interests of end-users, but also the advocacy groups, grassroot organisations, think-thanks, training and awareness raising organisations, and alike.

3 Introduction: Addressing norms related to supply chain security and responsible reporting of ICT vulnerabilities

3.1 The challenge: How to address insecure digital products and enhance cyber-stability?

Once upon a time, a security researcher (i.e. 'white hat hacker') known as @DinaSyn29 discovered a critical vulnerability - which it dubbed 'TeddyBear' - in a Windows desktop client of an instant messaging and VoIP social media platform Networkarium. This vulnerability could allow an attacker to remotely take over a user's system simply by sending a malicious message, and then run a malicious code on it.

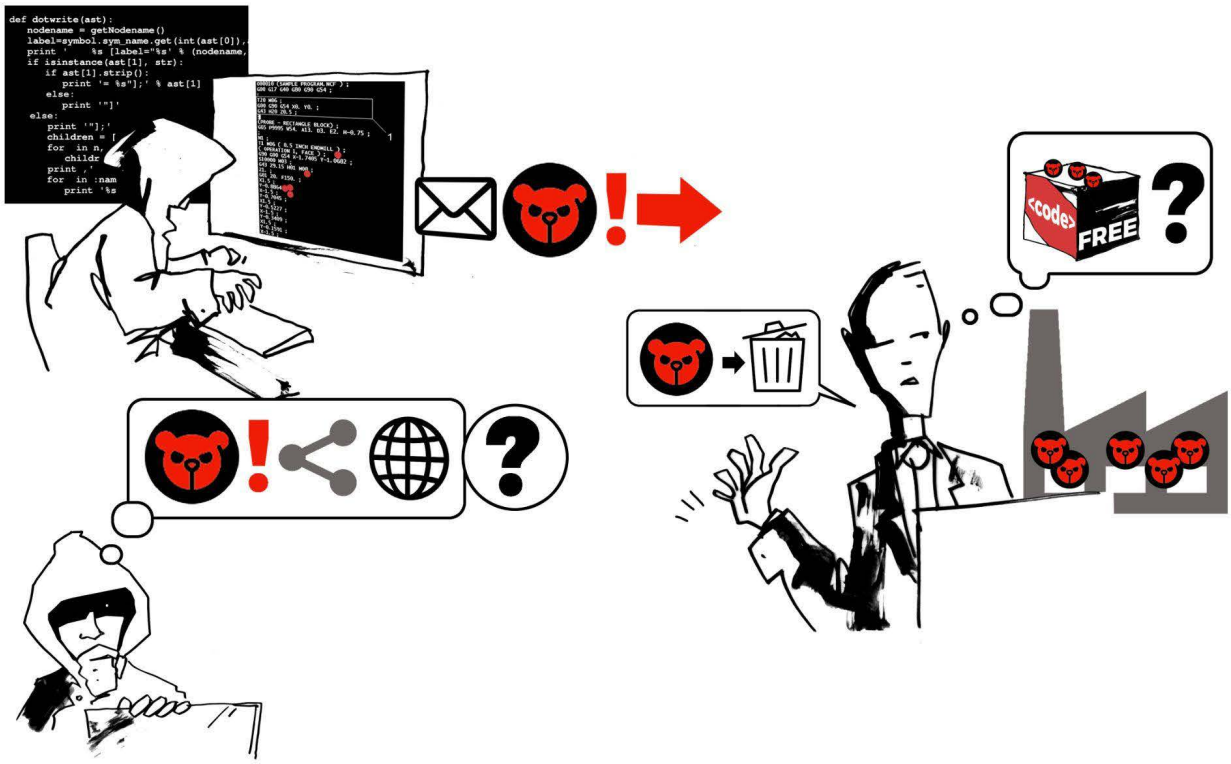
The researcher, following responsible disclosure practices, reported the 'TeddyBear' vulnerability to the Networkarium security team and provided detailed information about the exploit. However, Networkarium initially downplayed the severity of the issue, leading to a disagreement between @DinaSyn29 and the company.

Networkarium argued that the impact of the vulnerability was limited because it required user interaction, such as clicking on a link or opening a message, to be exploited. On the other hand, @DinaSyn29 insisted that the potential for abuse was significant - not least due to general lack of awareness of ordinary users not to open suspicious messages - and that immediate action was necessary to protect users.

In the meantime, the analysis by the Networkarium security team revealed that the vulnerability was 'imported' from a third-party code (a RunTix library), which Networkarium developers embedded into the app's code.The RunTix library containing the discovered vulnerability is part of an open-source project, developed voluntarily by a programmer known as AutumnFlower, which she made available for wider use by anyone for free. The company's security team encountered challenges in developing a patch, as AutumnFlower responded slowly and without much interest, despite acknowledging the vulnerability report disclosed by the Networkarium team.

As the disagreement persisted, @DinaSyn29 was frustrated by what she perceived as the Networkarium's lack of urgency and decided to publicly disclose the vulnerability for everyone to see - complete with proof-of-concept code which would allow anyone to test exploiting the vulnerability - before Networkarium had a chance to release a fix.

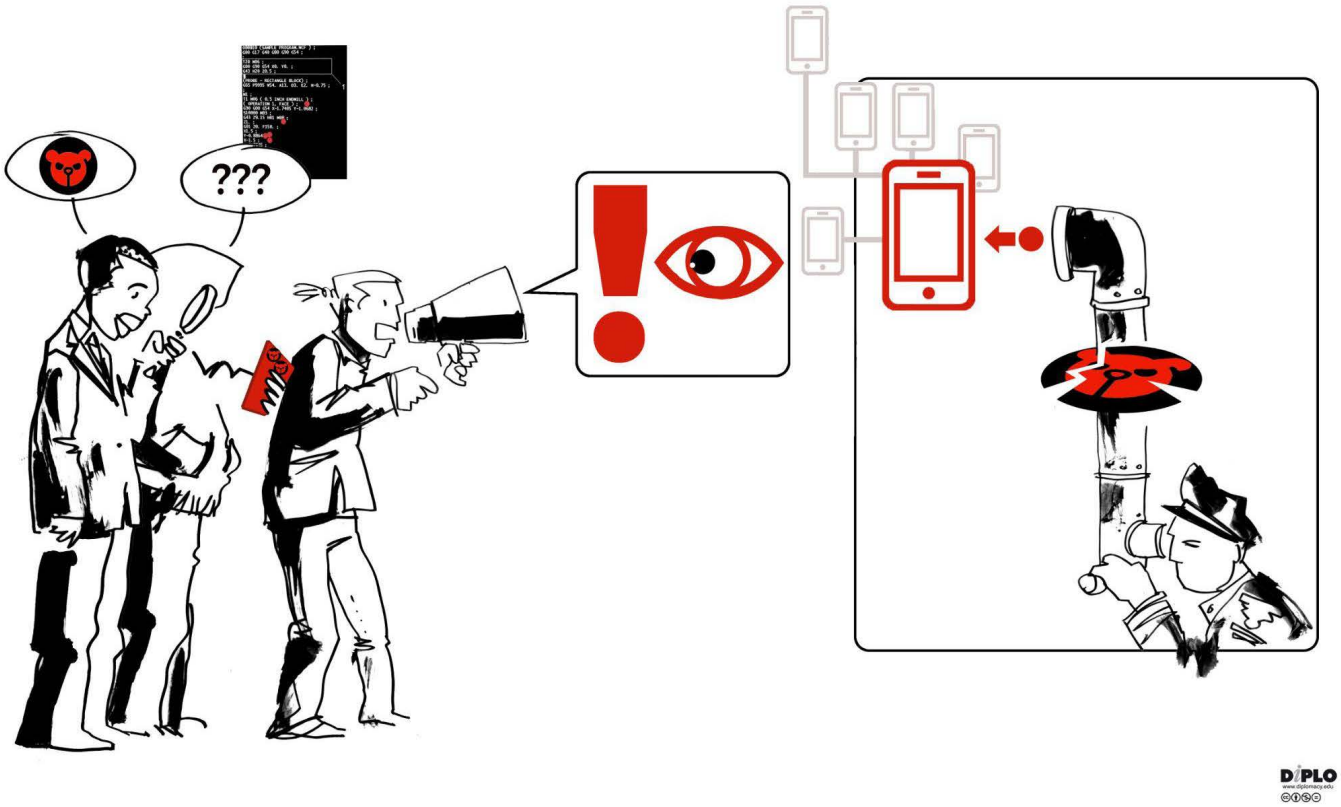
What should be the next steps for Networkarium to respond to this and mitigate the security risks for its users? What should have been done by Networkarium to allow a transparent and responsible vulnerability disclosure process? What lessons-learned can be made here for Networkarium? What should be the next steps for the OSS maintainer to do in this context? What lessons-learned can be made for the open-source community to ensure agility in patching the vulnerable code? What could the researcher have done differently when Networkarium downplayed the relevance of the vulnerability, instead of publicly disclosing it?



Several months ago, a civil society organisation named CyberRights International published an investigation about a surveillance operation on journalists in several countries - malicious actors targeted victims to get access to their mobile phones and stole confidential information like sensitive chats, protected sources, etc. The operation exploited the 'TeddyBear' vulnerability in the Networkarium messaging platform mentioned earlier. In this investigation, CyberRights International teamed up with a cybersecurity company CyberSecurITatus and revealed that a skilled and sophisticated actor - known as APT102, often assumed to be sponsored by the state of Absurdinia - is behind the operation.

Understanding the gravity of the situation, CyberRights International publicly shamed Networkarium for a failure to ensure the security for users, as well as Absurdinia for targeting journalists and posing threat to user privacy and freedom of expression. Global media have widely reported about the case.

The investigation by CyberSecurITatus revealed that attackers used the 'TeddyBear' vulnerability to also breach networks of a much larger company Important Systems Inc. (InSys), which produces hardware and software solutions typically used by energy power plants and industrial facilities. InSys used the messaging platform for internal communications, which allowed the attackers to infect their desktops, and attempt to enter their corporate network. The cybersecurity experts of CyberSecurITatus reported the failed supply chain attack, where attackers tried to compromise the networks of InSys but didn't have much success due to the properly segmented configuration of their internal IT network.



What should be the next steps for Networkarium to respond to this investigation? What can CyberRights International do to promote security for users? What should be the next steps for InSys to respond to this investigation, ensure the security of its products in accordance with the existing UN cyber norms (13i and 13j)?

The NCA - national cybersecurity authority of Utopistan, a country where Networkarium was legally established, became aware of CyberRights International's investigation and the harm caused by Networkarium's insecure service to citizens in the country and worldwide.

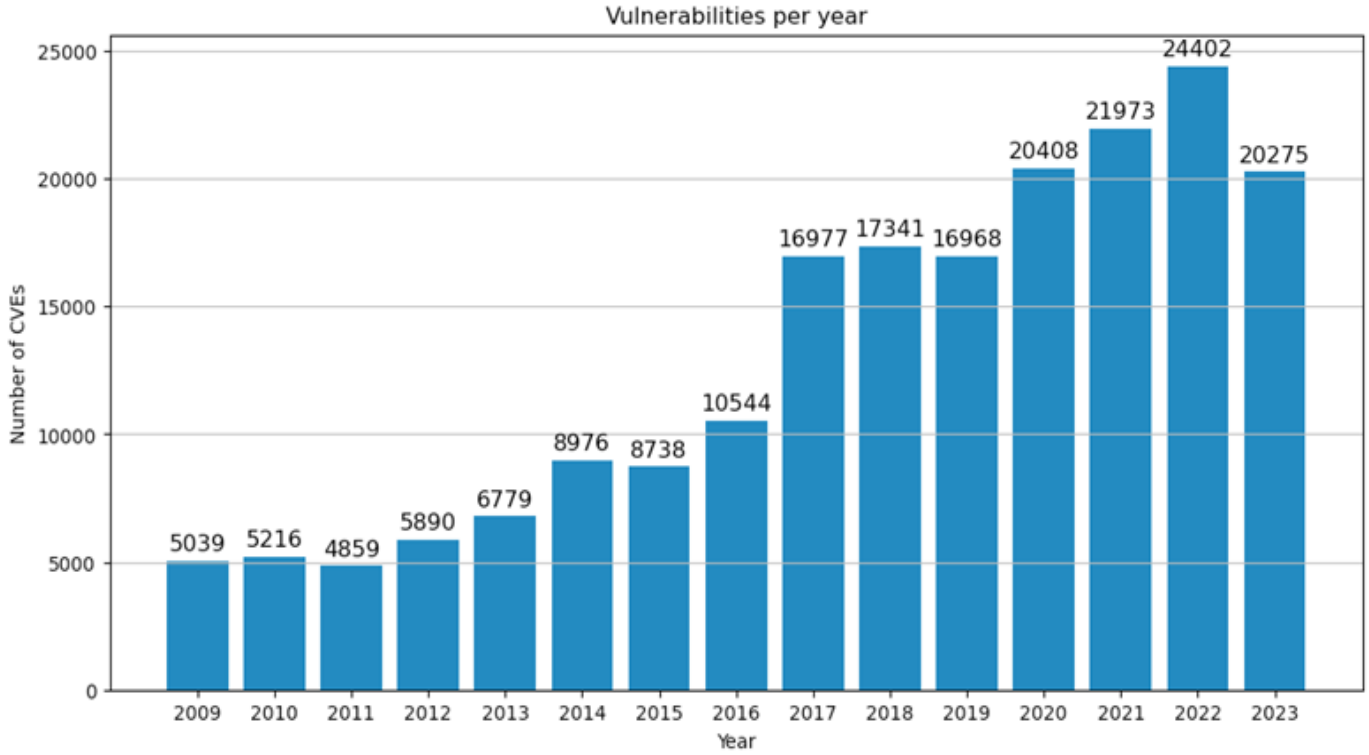
In response, the authority initiated its own investigation into Networkarium's security practices. It was revealed that Networkarium failed to notify both the authority and affected users within 72 hours of discovering the vulnerability, and did not report the unpatched vulnerability to the authority.

What should Networkarium respond to this? What are your thoughts on the decisions made by the national authority?

To mitigate security risks for users, who is expected to do what? What are the next steps?

The story above emphasises that cyberattacks, resulting in security and safety risks for users and causing societal and economic disruptions, most often stem from exploiting vulnerabilities in digital products and a lack of transparency in complex ICT supply chains, which delays the identification of relevant actors responsible for the mitigation of such vulnerabilities. The lack of security in digital products also allows well-resourced threat actors and such attacks to damage global cyber-stability.

> *"In 2022, malicious cyber actors exploited older software vulnerabilities more frequently than recently disclosed vulnerabilities and targeted unpatched, internet-facing systems."*[3]



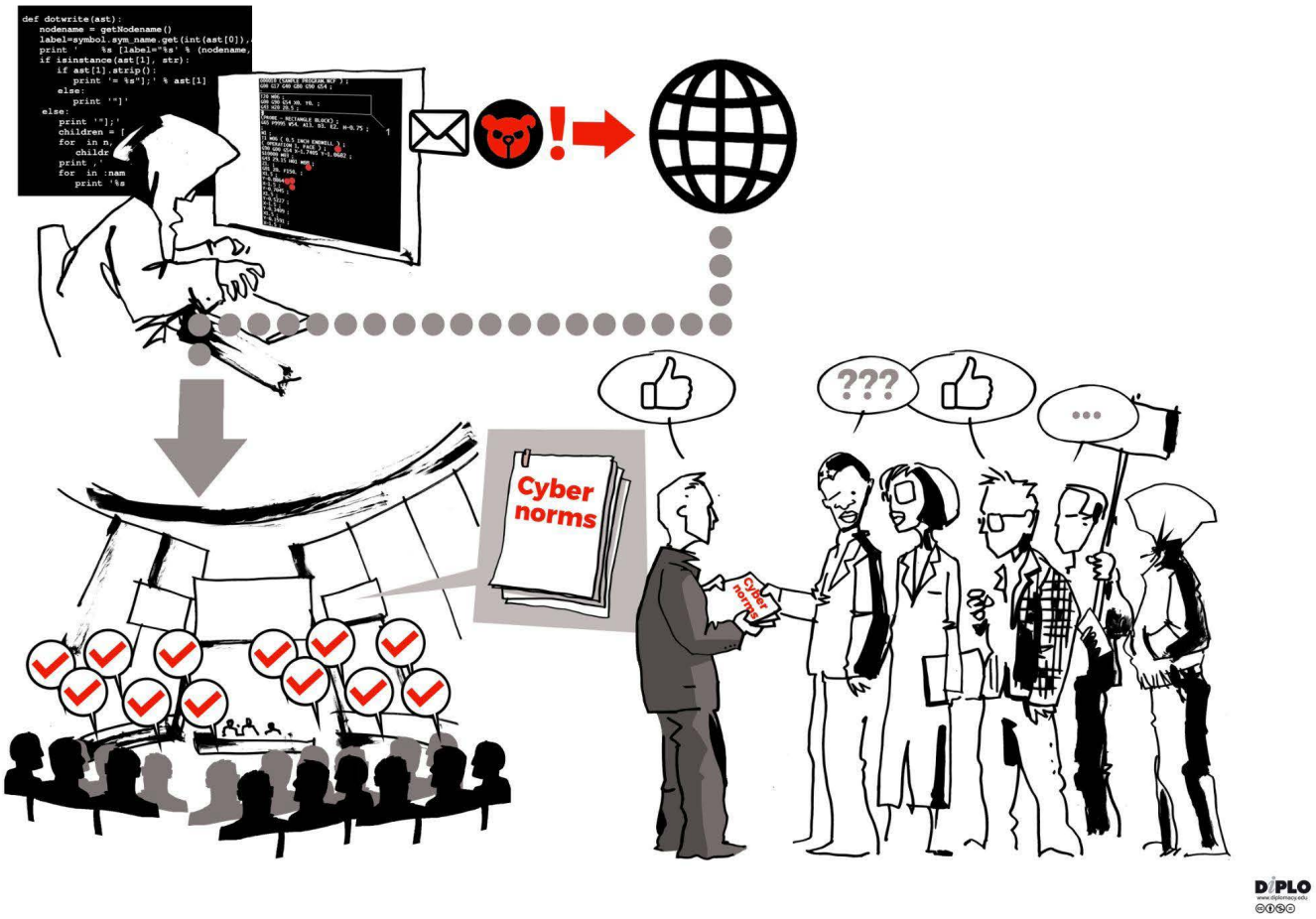
Number of published vulnerabilities per year (CVEs) worldwide (CVE.org)

It should be noted that not all vulnerabilities in digital products necessarily pose a significant threat. The severity of a vulnerability depends on various factors, including the nature of the vulnerability, the context in which the product is used, and the potential impact of exploitation. Additionally, network misconfigurations, characterised by errors or oversights in the configuration and management of network devices, systems, and applications, have been identified as a prevalent source of systemic weaknesses. These misconfigurations can introduce security vulnerabilities, providing opportunities for unauthorised access or other malicious activities, even in organisations that have attained a higher level of cyber maturity.

In order to address this problem, several international processes formulated the cyber norms of responsible behaviour in cyberspace to reduce ICT vulnerabilities and, therefore, security risks for users. For instance, the UN cyber norms**, which have been agreed on and endorsed by all UN Member States**. These include the UN GGE norm 13(i) and 13(j) related to the integrity of the supply chain and security of digital products, and the responsible reporting of vulnerabilities and the related information sharing respectively. These norms, along with others from different regional and multistakeholder forums, call for close cooperation between states and relevant non-state stakeholders.

---

[3] Joint Cybersecurity Advisory (CSA) issues by the NCSC, the US Cybersecurity and Infrastructure Security Agency (CISA), the US National Security Agency (NSA), the US Federal Bureau of Investigation (FBI), the Australian Signals Directorate's Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), the Computer Emergency Response Team New Zealand (CERT NZ) and the New Zealand National Cyber Security Centre (NCSC-NZ), 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-215a



One of the key challenges, however, lies in the implementation of such norms.

The environment in which this cooperation should take place is incredibly complex and uncertain: the threats in cyberspace are heavily influenced by geopolitics; emerging national legal and regulatory frameworks are pressed by national security concerns, and risk additional fragmenting of the global policy environment; traditional existing practices, such as certifications, may not entirely address the need for greater security and safety in the use of ICTs, nor may they be suitable for the various stakeholders, convergence of technologies, and the pace at which the threat landscape changes.

Moreover, the agreed non-binding cyber norms for responsible behaviour are often unfamiliar to relevant non-state stakeholders, or lack the specificity needed to offer practical guidance for their implementation by them. What's more, the norms are designed to primarily support political and diplomatic engagement and therefore may not provide the clear technical and practical guidance required by relevant non-state stakeholders. The current situation is also complicated by the existing limitations that hinder such stakeholders from actively participating and making meaningful contributions to international processes. These processes predominantly centre around the behaviour of states as the primary subjects of international law. Consequently, these limitations restrict opportunities for stakeholders to gain a comprehensive understanding of the present challenges, exchange their own best practices, and benefit from shared experiences in advancing responsible behaviour in cyberspace.

Therefore, in order for the relevant non-state stakeholders – the private sector, academia, civil society, and technical community – to effectively support the implementation of existing norms and contribute to cyber-stability, it is crucial to clarify their needs, roles, and responsibilities. Besides, there is a need to discuss how to approach those stakeholders

who are not interested, unaware or unwilling, to cooperate in enhancing responsible behaviour in cyberspace. Focusing on such actors, the Geneva Dialogue sees as its mission to support such stakeholders involved in global discussions about responsible behaviour in cyberspace, securing digital products and ICT supply chains, and reducing risks from ICT vulnerabilities.

3.2 The approach: How does the Geneva Dialogue address the implementation of norms?

The Geneva Dialogue on Responsible Behaviour in Cyberspace (Geneva Dialogue) is an international process established in 2018 to address the challenge described above and, in particular, map the roles and responsibilities of actors, thus contributing to greater security and stability in cyberspace. It is led by the Swiss Federal Department of Foreign Affairs (FDFA) and implemented by DiploFoundation, with support of the Republic and State of Geneva, Center for Digital Trust (C4DT) at EPFL, Swisscom and UBS.

Asking *how the norms*[4] *might best be operationalised (or implemented) as a means to contribute to international security and stability*, and stemming from the principle of '*shared responsibility*[5]' for an open, secure, stable, accessible, and peaceful cyberspace, the Geneva Dialogue has first focused on the role of the private sector who often owns and/or maintains digital products and ICT systems. After rounds of regular discussions with industry partners, the Geneva Dialogue produced an output report with good practices for reducing vulnerabilities and secure design (November 2020).

Later, the Geneva Dialogue focused on governments' approaches and policies to regulate the security of digital products and covered other actors (such as standardisation and certification bodies) in this regard, to ask a fundamental question on how fragmentation in cybersecurity efforts could be decreased for greater security in cyberspace. For that purpose, the Geneva Dialogue published the policy research, prepared by the Center of Security Studies at ETH Zürich, which analysed various governance approaches to the security of digital products (November 2021).

All of these efforts laid the foundation for clarifying the **roles and responsibilities of relevant non-state stakeholders in implementing cyber norms.** The results are published in **the Geneva Manual, focusing initially on the two norms concerning responsible reporting of ICT vulnerabilities and supply chain security,** to ensure the consistency with the previous work. The Geneva Dialogue will expand its efforts to explore the implementation of other cyber norms in the coming years.

The UN cyber-stability framework, mentioned earlier, negotiated and agreed upon by UN Member States, provides a solid basis for the Geneva Manual: the norms guide on expected outcome in efforts to enhance stability and security in cyberspace. While these UN cyber norms are currently the one and only norms package endorsed by the entire UN Membership, the Geneva Dialogue explored other relevant normative frameworks to build connections, where possible, and avoid duplicative efforts. These normative frameworks include the examples

4 First and foremost, non-binding voluntary UN GGE norms (as agreed by States and endorsed by the UN membership in 2021) are meant here: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/86/PDF/N2107586.pdf?OpenElement. Further in the text, norms and 'cyber' norms are used interchangeably to refer to the UN GGE normative framework.

5 It is clear that states cannot implement agreements made within the UN GGE as well as 2021 UN OEWG report alone, and thus cannot meet their responsibilities without engaging with other actors, while vice versa is applied to other actors and to their responsibilities in cyberspace.

provided by the UN Open-Ended Working Group (OEWG), intergovernmental organisations (such as OSCE, OECD, ASEAN, OAS), and multistakeholder initiatives (such as the Paris Call for Trust and Security in Cyberspace, Global Commission on the Stability of Cyberspace, IGF Best Practice Forum on Cybersecurity, and many others).

The Geneva Manual covers different aspects of the two norms, such as *who* should be involved, *what* they should do, and *why* it matters. It also addresses the *challenges* and *good practices* for putting these norms into action. To gather this information, the Geneva Dialogue conducted regular virtual consultations and side-event discussions between April and November 2023. These discussions involved more than 50 representatives from various stakeholder groups, including the private sector, academia, civil society, and technical community. The findings consist of diverse stakeholder perspectives, good practices, as well as identified challenges in enhancing the security of ICT supply chains and reducing ICT vulnerabilities, thus implementing these cyber norms.

To this end, the Geneva Manual, alongside all previous analytical work produced by the Geneva Dialogue, is a consolidation of multistakeholder and geographically diverse views and opinions by experts, as well as institutions invited by the Swiss FDFA and DiploFoundation.

3.3 The value: Who should read the Geneva Manual and how to use it?

As part of the Swiss Digital Foreign Policy Strategy 2021-24, the Geneva Dialogue pursues its mission – to assist relevant non-state stakeholders who are interested to participate and contribute to global discussions on responsible behaviour in cyberspace and the implementation of relevant norms in this regard. These stakeholders include decision-makers in various organisations representing the private sector, academia, civil society, and technical community, who are interested to help enhance the security of digital products and ICT supply chains, and minimise risks associated with ICT vulnerabilities.

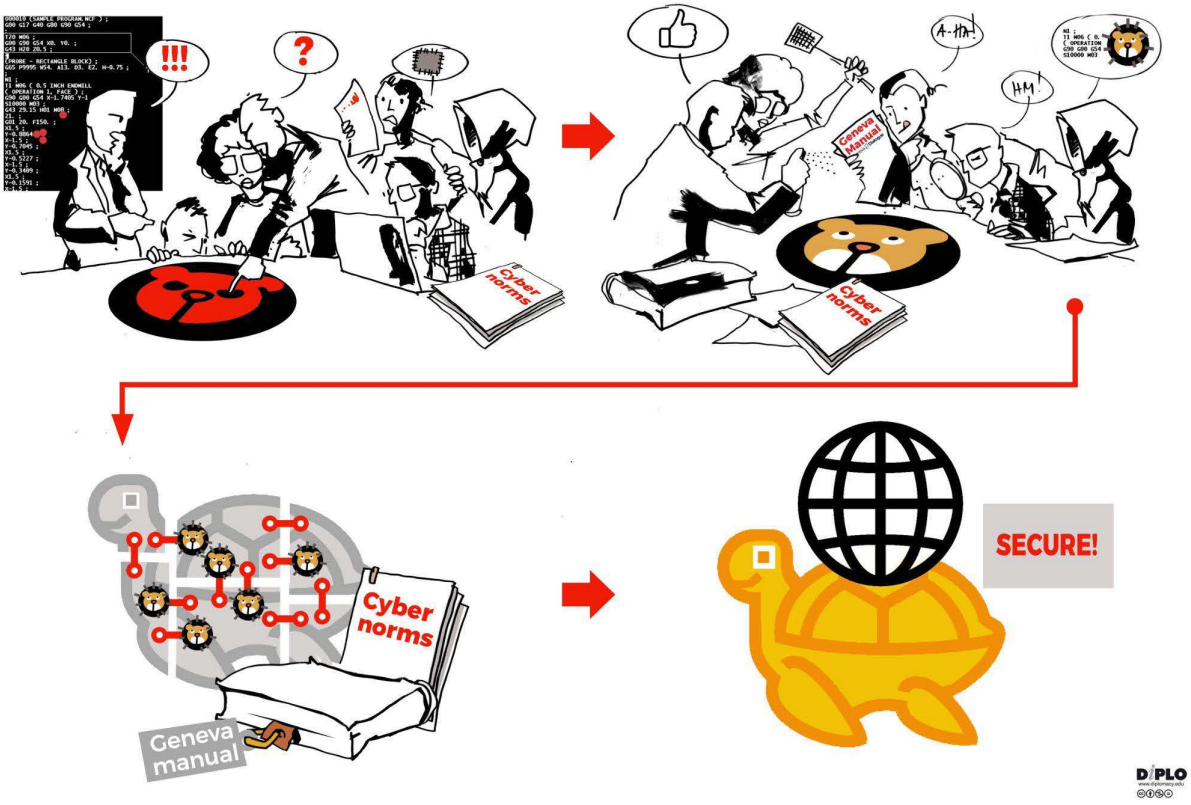
For this purpose, the Geneva Manual as a tangible outcome of the Dialogue, focuses on:

- **empowering such stakeholders** to help them understand their roles and responsibilities, and contribute, in a meaningful way, to processes where the international community discusses how we behave in cyberspace, use and secure digital products and technology, secure supply chains, and make the digital world safer

- **sharing good practices** from different communities and regions to inspire others to follow suit, leading to a safer and more secure digital environment

- **raising awareness** about the importance of international cyber processes to sensitise stakeholders to play a bigger role in such processes

The Geneva Manual emphasises that it is not just implementing norms which is important, but rather proactively taking actions which enhance cybersecurity and stability in cyberspace, particularly by reducing ICT vulnerabilities in digital products and minimising supply chain risks.



The Geneva Manual, therefore, offers an **action-oriented approach to cyber-stability**: through the story introduced at the beginning, it explores the roles (*Who*), responsibilities and actions (*What*), incentives (*Why*), and *challenges*. We also connect actions to norms: in sharing stakeholders' interpretations of norms and drawing a direct line between practical actions and diplomatic arrangements, the Geneva Manual thus facilitates the understanding of the UN cyber-stability framework and its effective implementation.

4 Implementation of norms to secure supply chains and encourage responsible reporting of ICT vulnerabilities

*In dealing with a critical vulnerability, **who** is expected to do **what** in order to minimise security risks?*

To answer this question, the international community fortunately has the framework we previously introduced. This framework helps us define the expectations for achieving cyber-stability. As mentioned earlier, the framework includes non-binding norms, among other elements, with two particular norms of special relevance for our discussion about ICT vulnerabilities and supply chain risks:

13i "States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions."

13j "States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure."

UN GGE reports

However, these norms are by default abstract and general in scope – and voluntary in nature. Who should read them – and how?

4.1 Unpacking the two norms: What did States specifically agree about, and do other stakeholders concur?

While not legally binding, both norms are seen as a collective understanding confirmed by all UN Member States on how to ensure a safer digital landscape. In 2021, States confirmed the eleven cyber norms, as part of the cyber-stability framework, and agreed upon the implementation points for each of them. However, a deeper contemplation of concrete suggestions and steps opens numerous questions.

In particular, when discussing norm 13i (related to supply chain security), States agreed upon the broad measures such as putting in place, at the national level, transparent and impartial frameworks and mechanisms for supply chain risk management to more narrowly define ones, (e.g. putting in place measures that prohibit the introduction of harmful hidden functions and the exploitation of vulnerabilities in ICT products). The 2021 UN GGE report clarifies that States are primary responsible actors for implementing this norm. However, at the same time, ***states agreed that the private sector and civil society should assume a relevant role in the process***. What can be concrete responsibilities for these stakeholders? The norm does not clarify this issue further.

With regard to norm 13j (related to responsible reporting of ICT vulnerabilities), the language remains less detailed and specific. The norm promotes a necessity for 'timely discovery and responsible disclosure and reporting of ICT vulnerabilities'. The norm also mentions that states could consider developing impartial legal frameworks, policies, and programmes on vulnerability handling; develop guidance and incentives, and protect researchers and penetration testers. These measures would find broad support across cybersecurity experts, users, and other stakeholders; however, details are critical – ***what do 'impartial legal frameworks' mean? How will states protect researchers and penetration testers? And what would 'responsible reporting' entail? To whom should vulnerabilities be reported to ensure responsible reporting?*** The norm does not clarify this either.

Discussions with the Geneva Dialogue experts have highlighted that these questions are just as important and on the minds of stakeholders. They have raised additional concerns, such as how to tackle the ***current geopolitical challenges arising from technological competition between countries and the different rules and regulations*** in this field. These challenges and risks of conflicting rules and laws in this field across countries can present hurdles for researchers and industry players trying to collaborate across borders to put these norms into action.

The role of governments in the implementation of these norms raised another concern, especially in regards to the states who have advanced cyber capabilities to stockpile vulnerabilities for their cyber offensive and defensive programs. ***How to build trust between relevant non-state stakeholders and governments to implement these norms and encourage responsible vulnerability disclosure? How to facilitate information exchange to implement these norms between states and relevant non-state stakeholders, as well as between different states?***

The Geneva Dialogue experts have also expressed concerns about the implementation of the norm 13i on supply chain security. In particular, it has been noted that the ICT supply chains now involve multiple stakeholders, and that ***no single entity has complete control over them***. The complexity of these supply chains, with various participants and cross-border data flows, makes achieving optimal security challenging. Each organisation makes security decisions based on its resources and capabilities, which may not align with the security needs of others. The ***absence of universally accepted methods for conducting evidence-based security assessments*** in supply chain security poses challenges for organisations of different sizes. They must make security choices and decide which digital products and suppliers can be trusted. All these decisions often have an immediate impact on the security of customers and users. In this context, the Geneva Dialogue experts stressed the ***need for globally accepted rules and standards for supply chain security***, promoting security by design and default in digital products. ***However, is it possible to develop such rules today, and is there an appropriate international platform for facilitating these discussions?***

While norms set expectations, translating them into practical actions is of the essence. The Geneva Dialogue experts supported translating the norms as non-binding diplomatic agreements into more tangible processes, policies, and regulations. The key questions are ***how to develop such policies and regulations, and where to establish them. What should be the fundamental principles guiding the creation of such policies and regulations to effectively implement the essence of the norms?***

With many open questions, the consultations with the Geneva Dialogue experts showed that ***relevant non-state stakeholders support the norms negotiated by states:*** if properly implemented, they can help significantly increase the security and stability in cyberspace. But the 'devil is in the details' and the key caveats are about 'if' and 'properly implemented' – what would this mean in practice?

With the Geneva Manual, we launch a global conversation on how the norms implementation for the security of cyberspace can become a reality or, where it is already a reality, what can be improved. Based on the idea that achieving effective cybersecurity requires continuous cooperation and commitment from all involved parties, we have outlined suggestions as to 'who should do what.' Below we explore different roles within various stakeholder groups and delve into what each role can include, and could contribute to. This involves understanding the expectations, motivations, incentives, and challenges faced by these groups. Through the regular discussions with the Geneva Dialogue experts, we also discovered some good practices that can inspire others in the international community to play their part in promoting cyber-stability.

4.2 Implementation of the two norms: Roles and responsibilities to achieve cyber-stability

In the event of an ICT incident resulting from the exploitation of a vulnerability in a digital product, what actions should be taken by whom to prevent the recurrence of such incidents?

How will the national policy maker or a cybersecurity agency work to ensure security and safety for users, while preventing security risks from becoming worse?

As an ICT vendor or manufacturer, what steps would you take to keep your customers – especially those in critical sectors – confident and trusting your services while avoiding unnecessary government scrutiny? What challenges may you face in doing so?

Can the researchers and academics do anything to analyse emerging risks and good and bad practices, or increase knowledge and understanding of the technical and social challenges?

As a customer (e.g. an organisation/company) of the digital product/ICTs which could be affected by a vulnerability, what measures would you adopt to minimise the risks for your operations and negative impact, if any, for your stakeholders and users? What obstacles may you come across in this process?

What can civil society organisations (e.g. consumer protection organisations and advocacy groups) do to improve the overall awareness and impact the policy environment that ensures prevention, protects citizens, and holds parties accountable for mistakes?

The questions above are intentionally simple. We wish to focus on one crucial aspect: if there is an urgent risk in the digital world, who should take the lead in fixing it? Is it the person or organisation or institution with technical expertise or political influence, or the one using the technology?

We often say that cybersecurity is a team effort, but how can we ensure that such a 'team' works together *effectively*? To address this, we collected the views of the Geneva Dialogue experts: these multistakeholder inputs helped us analyse where roles start and end, which drivers are needed to incentivise responsible behaviour across relevant non-state stakeholders, and which challenges remain unsolved, therefore requiring further attention of the international community.

Role: Manufacturer and/or supplier of digital products

Who	The role refers to a company or entity that produces or provides digital/ICT products and services, including software, hardware or a system configuration. The role applies to small and medium-sized manufacturers and suppliers as well; however, not all suggested steps below are implementable by them, and certain prioritisation may be needed.
Stakeholder group	The private sector
What	As a result of consultations with the Geneva Dialogue experts, manufacturers have been named as the ones who are expected to have the primary responsibility to address ICT supply chain risks and risks from vulnerabilities in digital products to ensure the security and safety for customers and users. In particular, this responsibility, as collective expectations from users of digital products, entails the following: 1. Implementing security by design practices in the development of digital products throughout their lifecycle and supply chain in line with international standards and recognized security good practices 2. Conducting security risk assessments of suppliers and digital products, including software from third parties and open-source components 3. Evaluating and regularly updating an inventory of supplier relationships, contracts, and any products those suppliers provide 4. Maintaining, regularly updating, and providing upon request information about the composition of its products, including those about integrated third-party and open-source components (known as Software Bill of Materials (SBOM) and/or Hardware Bill of Materials (HBOM) 5. Indicating the expected product lifecycle during which users can expect security updates and security support 6. Implementing vulnerability disclosure and management processes, i.e. responding to vulnerability reports and coordinating actions, where needed, with relevant parties (e.g. national authorities, CERT/CSIRT, researchers, other vendors, OSS community) to remediate vulnerabilities (researchers' expectations from manufacturers) 7. Utilising standardised formats for vulnerability exchange (e.g. VEX) to allow automatisation and quicker response to identify a product or products that are affected by a known vulnerability or vulnerabilities 8. In case of discovered and reported vulnerabilities in open-source software, conducting timely communication with the OSS development team and notifying them about the vulnerability or fix (OSS community's expectations from manufacturers) 9. Building specialised security teams and developing effective organisational structures to promptly address vulnerabilities and security threats (researchers' expectations from manufacturers) 10. Proactively informing affected customers and users, and national authorities, where required, as a first priority, about the released patch 11. Assisting customers to help ensure that their products are deployed in a secure manner and communicating to the customers how to continually ensure the security of their digital products in deployment

	12. Utilising certification and standardisation bodies, as well as industry and trade associations to team up with other manufacturers, technical communities, and relevant civil society organisations and academia to develop interoperable global rules and standards for supply chain security 13. Having an up-to-date software maintenance plan that includes alternative software components which can be used if an OSS developer fails to respond or patch vulnerable libraries
Why	The key incentives include: **1. Regulatory pressure and liability for software security** The Geneva Dialogue experts have discussed the need for governments and policymakers to step in and set standards to ensure the security and safety of digital products. They have been debating the elements of a legal framework that would be widely accepted but, so far, there was no agreement among stakeholders on how to strike the right balance. Some of them have called for stronger accountability when companies failed to address vulnerabilities promptly. However, there is a consensus that it would be unrealistic to expect 100% security and hold manufacturers responsible for the existence of vulnerabilities themselves, as technology is rapidly evolving and the threat landscape is constantly changing. To improve security in digital products and help consumers make better choices, experts agree that standardisation, certification and labelling schemes are of the essence. Standardisation is an important tool to raise the cybersecurity bar in organisations and products. Technical standards, defined by consensus-building and inclusiveness, provide a minimum set of requirements that help organisations achieve their cybersecurity goals, with an impact on the global ecosystem. Once the cybersecurity standards are agreed, the demonstration of the conformity to these standards is also strategic; for instance, to comply with relevant legislations and regulations, but also generally to give trust within the market (i.e. to customers).These measures can stimulate stronger security in digital products, address the information gaps, and empower users to make more informed purchases. However, the focus of regulation should not only be on the end product. Instead, the emphasis should be on defining and assessing robust cybersecurity processes. For instance, rather than mandating manufacturers to produce products completely free of vulnerabilities, regulations should require them to establish strong cybersecurity processes that continuously test products and promptly address any vulnerabilities discovered or reported. This way, the emphasis is on building a proactive and effective security approach. **2. Pressure from customers and users to adhere to security standards** The Geneva Dialogue experts who represent manufacturers of digital products stressed that their customers and users are the main drivers who request greater security in products. To meet such customer demands, manufacturers are compelled to perform compliance checks and ensure that their products adhere to industry security standards. Failing to do so could lead to a loss of customer trust and, in some cases, legal liabilities (in the event of security breaches or vulnerabilities, for example). If a digital product is found to be insecure and leads to data breaches or other security incidents, the manufacturer can face legal consequences, reputational damage, and financial losses.

	Therefore, the fear of losing customers and facing potential legal consequences acts as a strong indirect incentive and pressure for manufacturers to continuously enhance the security of their products. **3. Market competition** Benchmarking against competitors pushes manufacturers to meet, or exceed, the existing security standards and, thus, this form of peer pressure drives a culture of continuous improvement in security practices. At the same time, interconnected supply chains and business partnerships which create benefits – from accessing valuable information to being authorised to large partners' ecosystems - create certain expectations of a trusted and reliable company, where security becomes one of the key criteria. **4. Security risks** When security breaches happen within the industry, companies closely observe these incidents and their repercussions on the affected organisations. Such incidents serve as cautionary precedents, motivating companies to assess their own security posture and invest in preventive measures to avoid similar vulnerabilities. **5. Reputational risks** A security breach, or revelations of poor security practices that result in security risks for users, can cause significant harm to a company's reputation, undermine customer trust and loyalty, resulting in a decline in business. The fear of being seen as untrustworthy and unreliable in the eyes of stakeholders (including government stakeholders and regulators) and customers pushes manufacturers to build a proven track record of strong security measures and a dedicated focus on cybersecurity.
Challenges	The Geneva Dialogue experts have been asked about factors which prevent manufacturers from implementing the actions above and, therefore, from following the norms. The key challenges include: **1. High costs of required measures** Cybersecurity measures and, in particular, adoption of stricter secure software development practices, require expertise and time. For small and medium enterprises (SMEs), often operating with limited budgets and general IT personnel responsible for all ICT related processes, this can be a tough challenge to meet. **2. Complexity and lack of expertise** The lack of expertise in cybersecurity poses a significant challenge for all organisations when it comes to investing more in their security measures. Implementing effective cybersecurity protocols requires specialised knowledge and skills. This especially affects small companies, as they may not have access to skilled cybersecurity professionals, or find it financially challenging to hire external experts. As a result, they may be hesitant to invest in cybersecurity measures they feel ill-equipped to handle, such as creating and maintaining a vulnerability disclosure program.

Furthermore, successful cybersecurity implementation involves robust asset management, which allows organisations to identify vulnerabilities before they can be exploited. While small organisations with limited resources may effectively manage their assets, medium enterprises might already find it difficult to do so. As organisations grow larger, the task of keeping track of all assets becomes near-impossible.

Furthermore, successful cybersecurity implementation involves robust asset management, which allows organisations to identify vulnerabilities before they can be exploited. While small organisations with limited resources may effectively manage their assets, medium enterprises might already find it difficult to do so. As organisations grow larger, the task of keeping track of all assets becomes near-impossible.

Additionally, many organisations integrate open-source software (OSS) into their systems without fully understanding the potential consequences and risks associated with using code developed outside their organisation. The challenge also lies in having the proper skills and knowledge to conduct necessary security assessments of such components. The one-fits-all approach with centralised assessments can hardly be implemented – security risks are contextualised, as Geneva Dialogue experts noted several times, and manufacturers should rely on the knowledge of their systems and landscape for such security reviews to identify which components could be trusted and would be reliable.

It should be also noted that the lack of expertise in cybersecurity is a universal challenge, which even bigger, more-resourced, organisations may face.

3. **Lack or low awareness of business justification and rationale to implement required security measures**

The Geneva Dialogue experts have shared the widespread issue in many industries which is the difficulty of translating the technical language of vulnerabilities and their impact into terms that CEOs and decision-makers can understand and relate to their business objectives.

One contributing factor to this challenge is that some companies may underestimate the risk of a cybersecurity breach occurring within their organisation, particularly if they haven't experienced such an incident in the past. This perception of low risk can lead to complacency, where companies become less inclined to invest in cybersecurity until they encounter a breach, or face regulatory pressure.

Another aspect is the lack of immediate tangible returns from cybersecurity investments. Unlike investments in product development or marketing, the benefits of cybersecurity may not be immediately apparent. This can make it challenging for some companies to justify the costs for cybersecurity, as they may prioritise activities that yield more immediate revenue. Moreover, investing in cybersecurity involves diverting financial resources from other areas of the business.

4. **Lack of international cooperation and the complex regulatory and policy landscape**

   The lack of international cooperation in setting cybersecurity standards and practices leads to inconsistencies in regulations across different countries and regions. This creates a challenging environment for organisations that operate globally, or have customers and partners in multiple jurisdictions. Adhering to varying cybersecurity requirements can be time-consuming, costly, and logistically demanding.

   At the same time, the constantly evolving and complex regulatory landscape creates uncertainty for organisations. The lack of clarity on future regulations and requirements makes it challenging for companies to plan and allocate resources effectively. This uncertainty can discourage investments in cybersecurity, as companies may hesitate to commit significant resources to initiatives that may become obsolete or non-compliant in the future.

5. **Difficulties to certify and/or conduct a security assessment of a digital product entirely due to the complexity of software composition and use of third-party components**

   To accelerate development and reduce costs, manufacturers often integrate third-party components and libraries into their products. While these components can provide valuable functionality, they also introduce potential security risks. Manufacturers may have limited visibility and control over the security practices of third-party vendors, making it difficult to ensure the overall security of the product.

   At the same time, the lack of standardised and comprehensive certification processes for digital products poses a challenge. Unlike industries with well-established certification frameworks (e.g. safety certifications for physical products), the certification of digital products' security is often less standardised and more complex. The absence of clear guidelines can make it difficult for manufacturers to determine what security measures are necessary, and what level of security should be achieved.

6. **The limitations of technical approaches to address trust issues related to ICT supply chain security**

   These limitations include issues related to trust in suppliers and considerations surrounding the country of origin of the various components used in the product. The technical community and industry are aware of these challenges and recognise the necessity for criteria that encompass both political and technical factors. They see the potential for creating globally interoperable criteria that can effectively evaluate and mitigate supply chain risks. However, creating globally interoperable criteria that effectively address these multifaceted concerns is a challenging task that requires trust and political will from various stakeholders, including governments.

	7. The emerging trend of governments mandating vulnerability reporting directly to them, rather than to the vendors While the intention behind these regulations may be to enhance cybersecurity and create a centralised repository of vulnerabilities, there are inherent risks involved. Collecting all vulnerabilities from various companies into a government database raises concerns about the security and confidentiality of such sensitive information. The potential for data breaches or unauthorised access to such a database could expose critical vulnerabilities, putting not only the companies at risk, but also the users of their products. Another challenge lies in the lack of trust between the private and public sectors. Manufacturers may be hesitant to report vulnerabilities, particularly those which are not patched yet, directly to the government, fearing that the information could be mishandled, misused, or not adequately addressed. This lack of trust can lead to underreporting of vulnerabilities, leaving potential security loopholes unaddressed. Moreover, governments' involvement in vulnerability evaluation and reporting can be influenced by self-interest and national security concerns. In some cases, there may be a tendency to prioritise certain vulnerabilities over others based on national interests, potentially leading to the non-disclosure of critical vulnerabilities that affect the security of digital products.
Good practices[6]	Geneva Dialogue Output report with a collection of industry good practices to reduce vulnerabilities and secure design of digital products and services Software Bill of Materials (SBOM) and Hardware Bill of Materials (HBOM) as a practice to maintain an inventory, a list of ingredients that make up software or hardware components, as well as a practice to share this inventory documentation with upstream and/or downstream customers Vulnerability Exploitability eXchange (VEX) as a practice to maintain an attestation, a form of a security advisory that indicates whether a product or products are affected by a known vulnerability or vulnerabilities OSS Vulnerability Guide a resource to assist organisations in creating and maintaining vulnerability disclosure programs FIRST Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure as a resource to assist organisations in improving multi-party vulnerability coordination across different stakeholder communities and minimising the security risks in vulnerability disclosure ISO vulnerability disclosure and handling standards (ISO/IEC 29147 and ISO/IEC 30111) that assist manufacturers and focus on bilateral disclosure for vulnerabilities in their digital products OpenSSF Guide for Evaluating OSS as a resource to support software developers, before using OSS dependencies or tools, to evaluate them for security and sustainability GitHub Secret Scanning as a tool which prevents OSS developers (and contributors) from pushing code with a detected secret GitHub Guide to implementing a coordinated vulnerability disclosure process for open source projects

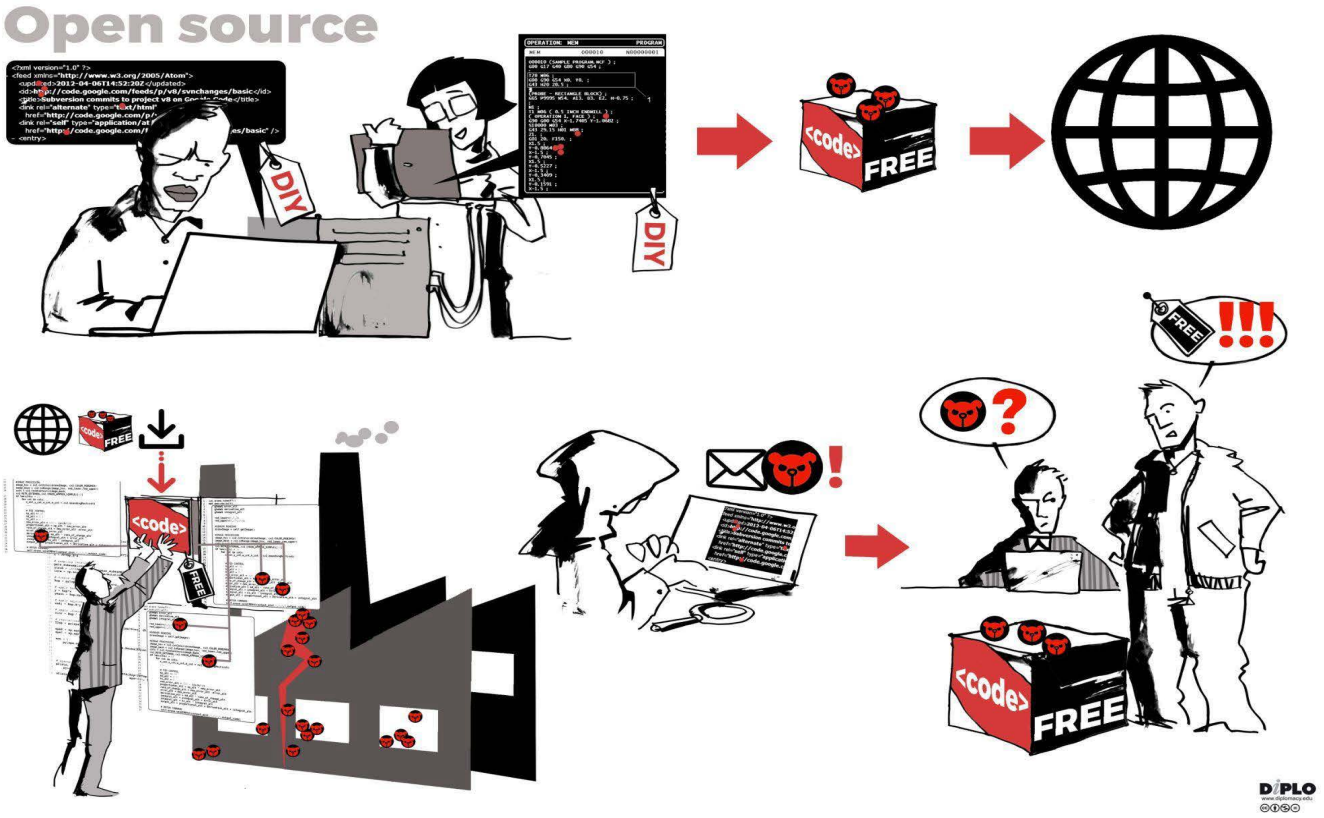
[6] Please note that these practices, also further in the Geneva Manual, are not exhaustive and that the Geneva Dialogue will continue including more good practices to inspire others in the international community to implement the norms.

	Singapore Cybersecurity Labelling Scheme (CLS) and the separate scheme for medical devices as an approach to enhance the security of consumer Internet of Things (IoT) devices and incentivise manufacturers to invest in the security of their products by helping them stand out from their competitors Singapore Common Criteria Scheme is established to support the info-communications industry with means to evaluate and certify their IT products against the CC standard in Singapore International 'Secure by Design' guidance from 18 countries (national authorities) to support software manufacturers in incorporating security by design and security by default in their design and development programs NIST SP 800-218 Secure Software Development Framework (SSDF) as a guidance for software developers to mitigate the risk of software vulnerabilities in their design and development programs Global Cyber Alliance Cybersecurity Toolkit for Small Business as a resource which provides free and effective tools to support small and medium sized businesses to implement cybersecurity controls OECD Recommendations on Digital Security Risk Management and High-level principles to enhance the Digital Security of Products as guidance for policy-makers to mitigate the digital security risks related to potential supply-chain attacks, as well as to embrace responsibility and duty of care
Messages	• Emerging cybersecurity regulations should avoid requirements to mandate reporting of unpatched vulnerabilities to anyone else but a code owner to minimise the risks of accessing this information by malicious actors. Where code owners do not cooperate, governments can play a role by putting pressure on such vendors to participate in responsible vulnerability disclosure • Governments need to enhance transparency about their vulnerability equities processes (VEP) or government disclosure decision processes. This would include making the information about the scope, involved government agencies, principles that guide the government decision-making in responsible vulnerability disclosure, and oversight mechanisms public. Such measures can help boost trust across the private sector and research community to cooperate with governments in responsible vulnerability disclosure • New regulations concerning digital product security should avoid the one-size-fits-all approach and, instead, tailor their requirements to the unique characteristics of each product category, such as cloud services and IoT devices, taking into account their distinct use cases, processes, and data handling practices • Governments need to step in to create better incentive programs for organisations to invest more in security of digital products (e.g. with the help of insurance companies) • A neutral and geopolitics-free governance framework is required to globally approach the security of ICT supply chains and security of digital products. Many organisations, as the Geneva Dialogue partners emphasised, need fact-based security assessments of technology, software, and suppliers to reduce security risks

	• The implementation of both norms and, particularly, efforts to address interconnected supply chain risks, require stronger international cooperation. Manufacturers and the private sector actors should be encouraged to participate more in such international discussions, including in the activities of the standardisation bodies and other industry international or regional processes • Addressing the certification challenges in complex multi-component digital products requires a multifaceted approach, including industry-wide collaboration, standardised certification processes, and a commitment to prioritising security throughout the product development lifecycle
Open questions	The Geneva Dialogue experts have emphasised the necessity for more targeted discussions to precisely specify which of the aforementioned steps (or additional ones) are applicable to small and medium-sized organisations. They also highlighted the importance of supporting these organisations, considering their limited resources, in adopting security practices. The question of how to provide such support and tailor it more effectively, especially for organisations within the ICT supply chain so they do not pose a cybersecurity risk, remains an open consideration. Furthermore, there is a recognised need for a more detailed analysis of 'sub-roles' within the manufacturing sector, acknowledging that different sectors, such as telecom or banking, may be subject to varying degrees of regulation and, consequently, differing responsibilities. Addressing the challenge of incentivising manufacturers to invest in cybersecurity during the development of their digital products is complex. While regulation is not always necessary, it relies on customer behaviour and their security demands. The Geneva Dialogue experts, particularly those from the private sector and industry, have expressed their expectations for regulators to play a role in promoting a cybersecurity culture through a 'whole-of-government' and 'whole-of-society' approach. This involves measures such as ensuring and promoting standards for vulnerability exchange, developing government vulnerability disclosure policies, ensuring transparency in how authorities handle vulnerabilities responsibly, and setting a precedent by implementing these norms and cooperating with relevant non-state stakeholders. However, while the Geneva Dialogue experts expressed a desire for a global, neutral, and geopolitics-free governance framework to secure ICT supply chains and digital products, it remains unclear if such a framework can be established at all, given the also growing fragmentation in regulatory efforts across countries. Therefore, tackling the implementation of the norm, specifically 13i, and addressing risks associated with ICT supply chain security in today's context, marked by increasing polarisation and technological competition between jurisdictions, poses a challenge that necessitates international approaches such as the Geneva Dialogue.

Role: Open-source software (OSS) community

If you were the owner of an open-source tool where the vulnerability had been discovered, what actions would you take to minimise the security risks? What difficulties may you encounter in taking such actions?



Who	The role refers to an individual, or a group of individuals, who contribute to the development, improvement, and maintenance of OSS projects. This includes the code owners, as well as repositories and organisations that maintain them. OSS refers to software whose source code is made freely available to the public, allowing anyone to view, modify, and distribute the code. OSS contributors, developers and maintainers are used interchangeably in the Geneva Manual.
Stakeholder group	Technical community
What	Given the wide adoption of OSS in modern ICT products (e.g. 97% of applications leverage open-source code, and 90% of companies are applying or using it in some way according to GitHub) and recently discovered critical vulnerabilities (e.g. Log4Shell), the Geneva Dialogue experts have singled out the open-source community and developers. They have recognised the professional and ethical responsibility of the OSS community to produce as much secure software as possible (and they are expected to follow relative OSS foundation guidelines), but not the legal responsibility to do so. Since the OSS developers and maintainers may not have the resources and capacities to meet all security requirements (and in most cases they work on voluntary basis), the Geneva Dialogue experts emphasised the importance of collaboration between the private sector and the OSS community, as well as mutual support in this regard.

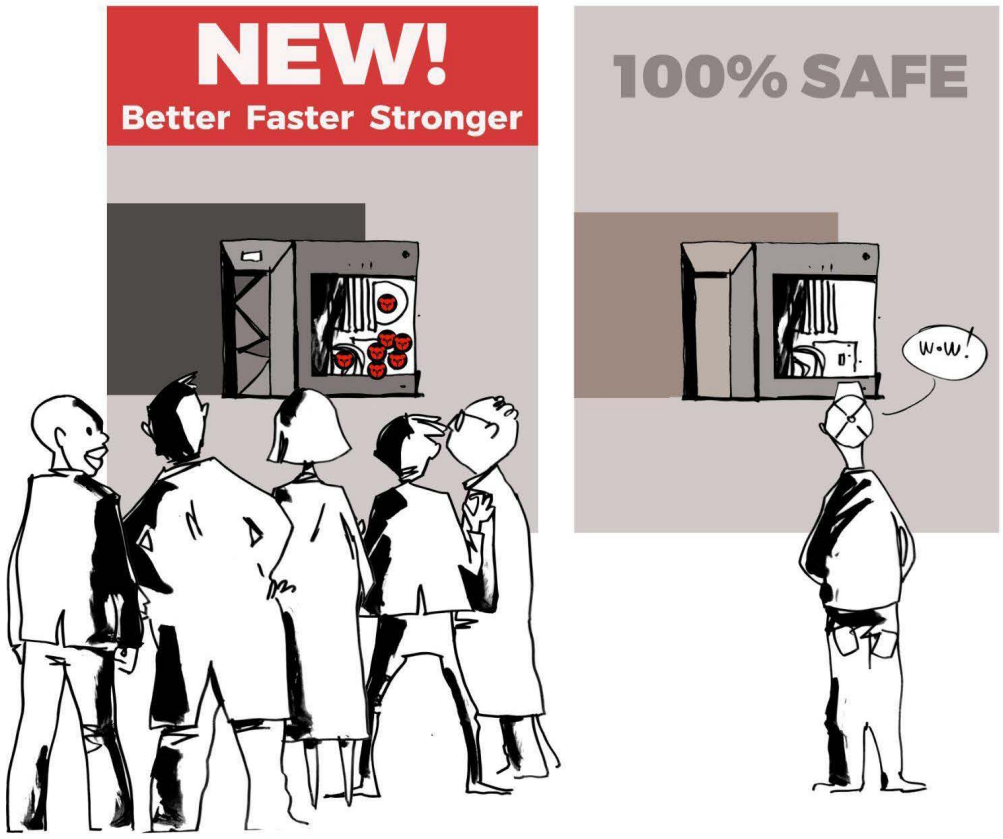
	The Geneva Dialogue experts added that OSS developers and maintainers may need to consider commoditising or making free security assessment tools to uplift the code quality as well as security. In this regard, the role of repositories has been specifically highlighted – they can help OSS contributors with the adoption of security practices for code development as well as support them with vulnerability reporting concerning their repositories.
Why	Some of the incentives for the OSS community to adopt stricter security practices, as well as to follow the two cyber norms, include: 1. **Community reputation** By prioritising security, OSS developers can build a reputation for producing reliable and secure software, which enhances trust among community contributors and users. 2. **Personal and professional growth** By following security practices, OSS developers can make more valuable contributions to software development, thus enhancing their career prospects.
Challenges	**OSS developers face several challenges in producing more secure code** One of the main challenges are the unrealistic expectations often placed on OSS developers, under the assumption that they have the same level of resources as closed-source companies. However, there are certain key differences between the two that impact the way security is handled: 1. **Lack of contractual obligations** Closed-source companies typically have contractual obligations with their customers or users, which may include service level agreements (SLAs) specifying response times and actions in case of security incidents. In contrast, OSS maintainers often work on a voluntary or a community-driven basis, and they may not have the same contractual obligations. This lack of formal obligations can make it difficult to meet specific response times or take immediate actions as expected. 2. **Limited resources for regular testing of software components** Open-source projects, especially smaller ones, may have limited resources, including capacity and funding. Unlike proprietary software companies that may have dedicated teams for security, open-source developers might not have the same level of resources available to focus solely on security-related tasks. In most cases, OSS code-owners are developing and maintaining the code on a voluntary basis. 3. **Complexity of a community-driven development and multiple collaborators** OSS is often developed collaboratively by a community of contributors, each with their own priorities and areas of expertise. Coordinating and aligning the efforts of various contributors towards security goals can be challenging. 4. **Time and prioritisation** OSS developers often contribute to projects in their spare time or as part of their other responsibilities. Balancing security efforts with other tasks and commitments can impact the time and priority given to addressing security concerns.

	5. **Dependency chain risks** Open-source projects may rely on other open-source components or libraries. Ensuring the security of the entire dependency chain can be a complex task, especially if some of the components lack proper security scrutiny. 6. **Lack of incentives** In some cases, OSS developers may not receive financial incentives or direct rewards for investing time and effort in security improvements. This can demotivate some of the developers from prioritising security over other aspects of the project.
Good practices	Github code scanning for all public repositories on GitHub.com to analyse the code to find security vulnerabilities and coding errors GitHub Secret Scanning as a tool which assists OSS developers (and contributors) in blocking commits containing secrets in any public repository by enabling push protecting for themselves OECD Recommendations on the Treatment of Digital Security Vulnerabilities as a guidance to promote a culture of cooperation and openness in treating digital security vulnerabilities OpenSSF Guide for Evaluating OSS as a resource to support software developers, before using OSS dependencies or tools, to evaluate them for security and sustainability GitHub Guidance on adding a security policy to a repository as a resource with instructions for reporting security vulnerabilities in an OSS project, so after someone reports such a security vulnerability, OSS maintainers can use GitHub Security Advisories to disclose, fix, and publish information about the vulnerabilities GitHub Guidance on reporting and disclosing vulnerabilities in projects as a resource to assist vulnerability reports and maintainers GitHub Guide to implementing a coordinated vulnerability disclosure process for open source projects Linux Foundation guidance on the vulnerability reporting process for vulnerability reporters Security.txt implemented by Google, Facebook, GitHub, the UK government, and many other organisations worldwide to help organisations define the process for security researchers to disclosure security vulnerabilities securely Glog.ai is an example of a project which implements AI to auto-remediate vulnerabilities in the open source code
Messages	• Security incidents in open-source projects can erode trust in the broader OSS community and impact the reputation of digital products built upon these projects. However, the open-source projects play a crucial role in fostering technological innovation by providing cost-efficiency, interoperability and inclusivity for developers, regardless of their geographic location or organisational affiliation

	• To address the security challenges, open-source communities should prioritise security, implement good practices, provide educational resources, and establish effective processes for vulnerability management and patching. Increased collaboration between open-source projects, industry, and the broader cybersecurity community can also contribute to enhancing the security of OSS • In particular, open source projects need to consider incorporating cybersecurity attestations into standard licences. This would foster the requirement for OSS developers and maintainers to adhere to minimum cybersecurity due diligence for committed code. These attestations could encompass the use of a standardised cybersecurity assurance pipeline, such as SAST and DAST, to assess the suitability of check-in code. Additionally, OSS developers and maintainers might have a minimum obligation in supporting vulnerability remediation • Larger organisations need to support the OSS community to develop more secure software
Open questions	Embracing more security in OSS development while not disincentivising contributors is critical and requires a more creative approach, as the Geneva Dialogue experts noted, such as support from private companies, industry, and the cybersecurity community. Introducing the legislation to regulate the security in OSS is a challenge due to several reasons, and various members of the OSS community, including individual developers and open-source foundations, have already raised concerns about the proposed cybersecurity legislation in Europe – the Cyber Resilience Act (CRA). One of the challenges includes a lack of comprehensive knowledge for OSS developers, whether independent individuals or nonprofit foundations, about all users due to the freely distributed nature of their software. That's why implementing vulnerability remediation and issuing security patches to downstream users may be a challenge, especially for those providing software for free. True, while at the same time, communities such as GitHub make steps to support contributors (see good practices above). A lack of comprehensive knowledge about the users of the software also highlights a challenge to manage and keep track of external libraries and dependencies (what may also be difficult for organisations and their in-house proprietary code). In the meantime, with particular regard to the CRA which may transform the software development industry, open-source foundations offer support to OSS developers by raising their awareness of a possible impact once the law is adopted and currently available ways to influence the policy-making. Artificial intelligence (AI) already assists developers to compose new code. On the one hand, this may allow less skilled individuals to produce their own code, and 'democratise' code-development; this may, however, lead to even more wide-spread vulnerabilities. On the other hand, AI can help identify common vulnerabilities in widespread open source code, and ultimately write a more secure code. There is a need for more efforts to apply AI solutions for the future.

Role: Organisational customers of digital products/ICTs

As a customer and user of digital products, what would you expect from your suppliers? What would motivate you to keep trusting them?



Who	The role refers to any organisation that procures, purchases, manages, and utilises digital products/ICTs for their own use, including to provide services based on such digital products/ICTs to their own customers and end-users. This role includes, but is not limited to, critical infrastructure entities, small and medium organisations, but also other entities from the public and private sectors that provide digital products and services to citizen customers.
Stakeholder group	The private sector Academia Civil society Technical community
What	While such organisations may not be directly involved in developing digital products or be responsible for the security of the products they purchase, they do have responsibility to implement the two cyber norms. In particular, the Geneva Dialogue experts emphasised that while these organisations may not be the creators of digital products, they are still accountable for the security and safety risks associated with the services they provide if these services rely on ICTs from third-party vendors. If a critical vulnerability is discovered in the ICTs used by these organisations, they may be even held liable for negative security and safety consequences that arise as a result.

In various sectors and industries, many organisations are subject to specific regulations and laws that govern their operations concerning cybersecurity and data protection. For instance, critical infrastructure protection laws may apply to organisations that operate vital infrastructures like energy, transportation, or healthcare systems. Additionally, regulations related to personal data protection impose responsibilities on organisations that handle sensitive information.

By complying with the existing sector-specific laws and regulations, organisations can better ensure the security of their operations and the safety of their customers and users, and thus be able to implement the two norms. In particular, the following set of responsibilities, that primarily citizen customers expect from organisational customers, has been outlined in the Geneva Dialogue:

1. Conducting vendor evaluation and selection before making procurement decisions and assessing the security practices of potential vendors
2. Including security requirements in contracts to outline security standards, data protection measures, incident response protocols, and other provisions as identified by applicable rules and laws
3. Conducting regular security audits of digital products and services that have been already procured to identify vulnerabilities and any other potential security risks, requesting the information about the composition of digital products and services (e.g. SBOM documentation)
4. Ensuring compliance with applicable laws and regulations
5. Conducting ongoing vendor management to monitor the security performance of technology providers and establishing regular communication channels with vendors to address security concerns
6. Minimising human-related security risks and investing in user education and awareness to educate their employees and users about the proper use of digital products and services
7. Conducting vulnerability management to ensure that all ICT systems and software are regularly updated with the latest security patches and updates (this represents researchers' expectations from organisational customers, as well)
8. Ensuring the secure integration of ICT systems, with the help of vendors or any other relevant parties
9. Ensuring data security and, in particular, undressing how vendors handle and protect sensitive data, and ensuring compliance with relevant data protection regulations
10. Building incident response plans and collaborating with vendors to establish clear procedures to minimise and mitigate security risks and impact of any potential breaches
11. Ensuring continuous improvement and cyber-resilience planning, including regular reassessment of security needs and staying informed (including C-level management) about emerging security trends

Why	Besides the obvious **cybersecurity and data protection regulatory incentives** for certain industries and sectors to implement the security measures above and thus follow the two norms, the Geneva Dialogue experts have outlined the following: 1. **Security requirements set by stakeholders, partners, investors and donors, and, therefore, reputation and trust from customers, stakeholders, partners, investors or donors**. Misuse of personal data or security breaches revealing poor security practices can hit not only with potential fines and legal consequences, but affect the organisation's reputation. 2. **Intellectual property protection** with the help of stricter cybersecurity measures. 3. **Potential third-party risks.** Since such organisations are not directly involved in software development but do largely rely on ICTs, they operate with inherent risks stemming from third party suppliers. This forces organisers to adopt stricter cybersecurity rules and, as a result, contribute to the implementation of the two norms.
Challenges	Considering that such organisations may cover a wide range of entities – from schools and bakeries, to airports – the Geneva Dialogue experts have outlined a broad list of possible difficulties that may slow down organisations' contribution to the implementation of these two norms: 1. Budget constraints and limited expertise (or lack of such expertise at all) to particularly conduct regular security audits of external solutions, including services from cloud providers 2. The unwillingness of infrastructure owners/operators to change legacy systems and infrastructure which may lack built-in security features or may not be compatible with the latest security updates. In any case, such systems require expertise, which organisations may lack, or require more time for 3. Lack or low awareness of business justification and rationale to implement required security measures (the same difficulty as for the manufacturers and/or suppliers of ICTs). 4. Constantly evolving threat landscape that makes it challenging for organisations to keep up with the latest security measures and practices
Good practices	The NIS2 Directive as an example of the legislation that establishes the cybersecurity risk management measures for entities in scope to protect network and information systems UK NCSC Supply chain security guidance as a resource designed to assist organisations in managing supply chain risks and choosing trusted ICT suppliers ATT&CK Matrix for Enterprise, MITRE ATT&CK® as a knowledge base of adversary tactics and techniques to support organisations in public and private sectors in conducting their threat assessments

	The EU 5G Toolbox which addresses the risks related to non-technical (such as the risk of interference from non-EU state or state-backed actors through the 5G supply chain) and technical factors, and thus is designed to support organisations in public and private sectors Software Bill of Materials (SBOM) and Hardware Bill of Materials (HBOM) as an example of the security document to request from ICT manufacturers/ suppliers and use for evaluating the security and reliability of digital products Singapore Cybersecurity Labelling Scheme (CLS) and the separate scheme for medical devices as an approach to enhance the security of consumer Internet of Things (IoT) devices and support consumers in making security-informed purchases Singapore Common Criteria Scheme is established to support the info-communications industry with means to evaluate and certify their IT products against the CC standard in Singapore
Messages	• Customers, especially large organisations, should demand SBOM/ HBOM documentation from ICT manufacturers in order to ensure their security practices and, at the same time, incentivise the adoption of automated processes. Organisations in the public sector also need to step in and require SBOM/HBOM documentation for their security assessments (and, for instance, incorporate these requirements in their procurement policies) • For customers with limited resources, but yet a necessity to ensure the cybersecurity of their own processes and operations, ICT manufacturers and supplies should provide, where possible, results of third-party security assessments (e.g. security certifications based on known industry standards) to regularly prove the security of their solutions and help customers make informed decisions

Role: Cybersecurity researchers

Do researchers – when discovering the vulnerability – always have to coordinate actions with vendors? Authorities? To whom would the reporting of vulnerabilities be considered as 'responsible' following the norm 13j?

Can (and should?) cybersecurity researchers independently mitigate the exploitation of the vulnerability without notifying the manufacturer? Or national authorities?

Who	The role of a cybersecurity researcher refers to a professional who specialises in exploring and analysing various aspects of cybersecurity to identify vulnerabilities, threats, and potential risks in digital systems, software, and networks.
Stakeholder group	Technical community The private sector (in those cases where researchers represent a company) Academia
What	The Geneva Dialogue experts agreed that the **primary role of a researcher is to find and disclose vulnerabilities, but is not expected to find a comprehensive solution to the entire security problem**. Researchers are expected to follow certain **ethical and security guidelines** and, in particular, **always report discovered vulnerabilities to code owners** and choose secure communication channels for doing so. Where needed, researchers should **consider engaging appropriate authorities such as CERTs/CSIRTs** to ensure the coordination in vulnerability disclosure.

Researchers also play an important role in **providing threat intelligence and assistance in investigation of supply chain threats**. However, their reporting and research can be influenced by business incentives, profit-driven motives, as well as geopolitics, and thus lack independence and impartiality.

The discussion with the Geneva Dialogue experts allowed to specifically outline the actions which cybersecurity researchers should avoid in order to contribute to the implementation of the two UN GGE norms:

1. **Publicly disclosing vulnerabilities without first notifying the affected vendors or relevant authorities.** Responsible vulnerability disclosure would involve giving vendors a reasonable amount of time to address and patch the vulnerability before making them publicly known.

   What is an appropriate threshold for a vendor to respond, where a vulnerability has been discovered by a researcher? To this question, a group of experts agreed that first it's important to define the criticality of the discovered vulnerability (e.g. whether the vulnerability affects the national critical infrastructure). If it does, further considerations come into play, such as whether it is cross-jurisdictional or localised, and if the researcher is in the same place as the vulnerability or not. The research community sticks to a 90-day maximum threshold to wait for a vendor to release a fix to the vulnerability reported if the vendor doesn't have an established timeline in their security policy.

2. **Exploiting or misusing discovered vulnerabilities.** Researchers should refrain from exploiting or misusing the vulnerabilities they discover for personal gain, malicious intent, or any other unauthorised purpose. A group of experts stated that **exploiting vulnerabilities for commercial gain should be prohibited**.

3. **Engaging in unauthorised access.** Researchers must not engage in unauthorised access or unauthorised activities while investigating vulnerabilities.

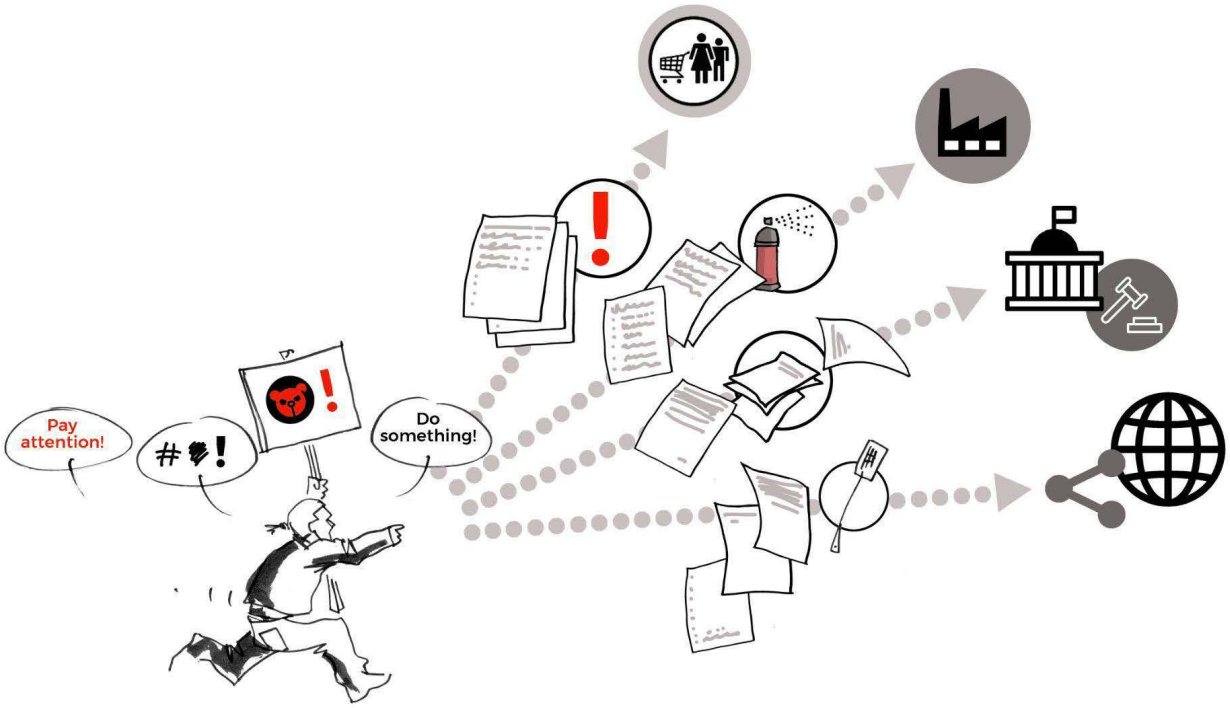
4. **Demanding payment or engaging in extortion tactics in exchange for information about vulnerabilities.** The Geneva Dialogue experts agreed that such actions are unethical and can be illegal, depending on the jurisdiction.

5. **Publicly shaming vendors for their response to vulnerability disclosures or ignoring vendor disclosure policies.** Researchers should focus on constructive engagement and collaboration to resolve the security issues. The Geneva Dialogue experts discussed possible actions for the researchers in situations where a code owner (i.e. manufacturer) does not respond, or responds too slowly. Some experts shared that researchers could find themselves in a difficult situation: either to wait for a response and further action from a manufacturer, or to act further without it, if risks are too high for the users. Maintaining good working relationships with vendors is important, however, as the experts agreed, the **ultimate goal is to have the vulnerabilities fixed and enhance the security posture for all users**. Therefore, researchers are expected to respect the vendor's policies where possible, and should consider the context and specifics of the vulnerability (as well as any other factors) in order to minimise the risks.

	6. **Engaging in dual-use research and disrupting or damaging systems which would result in negative impacts on the availability or functionality of the target systems**. In this context, the Geneva Dialogue experts particularly discussed the complex question of legitimacy in vulnerability research, especially if critical systems or legacy platforms are involved. With respect to such life-critical systems, the experts highlighted that testing or finding vulnerabilities should be approached with extreme caution due to the high risks involved. 7. **Ignoring legal and regulatory considerations and, in particular, neglecting end-user safety and privacy.** At the same time, it should be noted that legal requirements can be somewhat vague for researchers, or too complex to grasp, depending on a jurisdiction.
Why	There are several incentives driving researchers to implement responsible vulnerability disclosure and, specifically, to implement, at least, the norm 13j: 1. Clear reporting channels, clear processes and terms for coordination with vendors in vulnerability disclosure 2. Initiatives and programmes offering legal protections and encouraging ethical vulnerability research and disclosure (e.g. safe harbours) 3. Access to pre-release software or early access to security updates for vulnerability testing 4. Publicity, recognition, and acknowledgement, including with monetary regards (e.g. bug bounty programs) 5. Decriminalisation of ethical vulnerability research, and disclosure and exemption from prosecution for those who ensure proper authorisation and compliance with responsible disclosure guidelines 6. Institutional support where governments, through laws and programs, require other organisations to promote and support responsible vulnerability disclosure (e.g. as an element in national cybersecurity strategy, or any other relevant national laws and rules) 7. Research grants and funding by governments to support cybersecurity research initiatives 8. Public–private collaboration between governments, including law enforcement agencies, private companies, and researchers
Challenges	Researchers may face several demotivating factors and obstacles that prevent them from conducting responsible vulnerability disclosure: 1. Legal barriers and a complex regulatory environment which can create uncertainties and deter researchers from engaging responsible with other parties 2. Fear of criminalisation as well as difficulty distinguishing harmless actions 3from malicious intent 3. Lack of clarity in vendors' policies and terms, including in legal protections

	4. Limited knowledge about vulnerability impact. Researchers may not always know if a vulnerability is present across multiple products or affects open-source libraries, making it challenging to assess the potential impact and determine the appropriate level of care for reporting 5. Lack of a supportive legal and institutional environment to nurture the conditions for the welcomed and in-demand vulnerability research across different organisations 6. Complexity of supply chain disclosures: coordinating efforts and sharing vulnerabilities across supply chains can be challenging due to legal and logistical complexities. Such complexity may discourage researchers from engaging in cross-jurisdictional vulnerability disclosure
Good practices	OECD Recommendations on the Treatment of Digital Security Vulnerabilities as a guidance which promotes safe harbours for vulnerability researchers to protect them against legal proceedings from vulnerability owners Security.txt as good practice and project implemented by Google, Facebook, GitHub, the UK government, and many other organisations worldwide to help organisations define the process for security researchers to disclosure security vulnerabilities securely GitHub Guidance for Security Researchers to Coordinate Vulnerability Disclosures with Open Source Software Projects as a resource to support security researchers engage with OSS project maintainers to participate in the coordinated vulnerability response process OWASP Vulnerability Disclosure Cheat Sheet: Reporting Vulnerabilities as a guidance to support both security researchers and organisations with the vulnerability disclosure FIRST Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure as a resource to assist researchers in improving multi-party vulnerability coordination and minimising the security risks in vulnerability disclosure
Messages	The Geneva Dialogue experts highlighted that the limitations of data and research provided by private actors should be acknowledged, as their interests may introduce biases or lack impartiality. To counter this, independent institutions or bodies, such as those from academia or civil society, can step in to mitigate these risks. By providing impartial monitoring and research, these independent organisations can contribute to creating a framework for reducing vulnerabilities and promoting stronger security in ICTs. To address these demotivating factors and encourage responsible vulnerability disclosure, there is a need for legal reforms that decriminalise vulnerability reporting and provide clear protections for researchers. Establishing supportive legal frameworks that focus on encouraging responsible reporting without malicious intent can foster a more welcoming environment for researchers to come forward with their findings. Additionally, enhancing collaboration between researchers, vendors, and authorities can help address the challenges associated with cross-jurisdictional vulnerability disclosure and supply chain security.

Role: Civil society engaged in advocacy, research, and training



Who	The role refers to a non-governmental organisation (NGO) or academia or policy institution, or to individuals who serve as intermediaries between users of digital products and decision-makers (including from both the private and public sector) to shape policies as well as influence public opinion on issues relevant to their mission. Such organisations can also engage in capacity building to help educate decision-makers, as well as users, about issues related to the security of digital products, safety for users, and other topics related to the implementation of the two UN GGE norms.
Stakeholder group	Civil society Academia

What	The Geneva Dialogue experts have particularly noted that civil society needs to be more involved in policy development to help manufacturers and policymakers inter alia ensure that the rights of users are respected, to better consider the role of consumers and users in the security process, and also help define criteria for a trustworthy technology. The Geneva Dialogue experts highlighted the role of civil society and academia in advancing the implementation of the two UN GGE norms. In particular:
	1. **Driving policy and institutional changes**, e.g. by requiring greater transparency in vulnerability handling from companies and governments, or by driving cybersecurity labels for digital products. The Geneva Dialogue experts have particularly noted that civil society needs to be more involved in policy development to help manufacturers and other stakeholders better consider the role of organisational and citizen customers and users in the security process, and also help define criteria for a trustworthy technology. Civil society and academia can also help address trust issues related to ICT supply chain security (and implementation of the norm 13i) by providing a corresponding framework and tools to governments and ICT manufacturers/suppliers. 2. **Training and capacity building for bridging the gap** between policymakers and technical experts to help decision-makers (e.g. between the government and the private sector) to speak the same language and specifically translate technical terms into national policies aligned with the UN cyber-stability framework. Academia can also support governments in building harmonised interpretation of the norms and framework across different jurisdictions. 3. **Creating pressure** on decision-makers to prohibit the commercial exploitation of vulnerabilities. 4. **Facilitating international collaboration** and information sharing between researchers, industries, and governments to minimise the risks stemming from the exploitation of ICT vulnerabilities. 5. **Measuring impact and effectiveness** of initiatives, policies, and laws related to enhancing the security of digital products by conducting research to help refine and improve implementation strategies. 6. **Representing organisational and citizen customers and users** to incentivise companies to improve the security in their products and processes. 7. **Teaming up with the private sector** to help educate users about their possible role in ensuring the security of digital products.
Why	Both academia and civil society organisations can be motivated to call for the implementation of the two UN GGE norms due to the following reasons: 1. Protecting users from security and safety risks, as well as users' data protection rights through stronger security in digital products 2. Advancing research and knowledge for academia 3. Addressing cybersecurity challenges with a global impact

Challenges	Several key challenges can prevent both civil society and academia from calling for stronger security in digital products, reducing ICT vulnerabilities, and thus implementing the two UN GGE norms: **1. Lack of technical expertise and limited access to industry data and insights** Even though both academia and civil society can greatly help in capacity building to bridge the gap between different stakeholders, they themselves may lack necessary knowledge and expertise about nuances in vulnerability disclosure and security ICT supply chains. Furthermore, both civil society organisations and academia may face challenges in accessing proprietary information and industry insights. As a result, without access to comprehensive data related to digital product security and supply chain risks, they may find it difficult to make informed and evidence-based calls to represent users' interests. **2. Influence of corporate interests** Interested stakeholders and their lobbying efforts in shaping policy and regulations can impact the ability of civil society organisations and academia to advocate for stronger security in digital products.
Good practices	Swiss Digital Initiative as an example of the effort to bring ethical principles and values into technologies and urge organisations to ensure trustworthy digital services for end-users Global Encryption Coalition as an example of an international effort initiated by the Center for Democracy and Technology, Global Partners Digital, Mozilla Corporation, Internet Society, and the Internet Freedom Foundation to promote and defend encryption in ICTs Cyber Incident Tracer by CyberPeace Institute as the platform to bridge the information gap about cyberattacks on the healthcare sector and their impact on people Geneva Declaration on Targeted Surveillance and Human Rights initiated by AccessNow, the Government of Catalonia, the private sector, and civil society organisations to implement an immediate moratorium on the export, sale, transfer, servicing, and use of targeted digital surveillance technologies until rigorous human rights safeguards are put in place
Messages	Civil society and academia often lack comprehensive industry data and insights (as mentioned above), including visibility into the supply chains of private companies and organisations from the public sector. Access to such information is usually restricted, but may be critical for building expertise across civil society and academia organisations so they can conduct high-quality research and analysis. At the same time, despite the lack of technical expertise, it is the civil society and academia who can help raise uneasy questions (e.g. human rights impacts from the exploitation of ICT vulnerabilities by both private and state actors) or build much-needed trust among different stakeholders for ICT supply chain security and responsible reporting of ICT vulnerabilities (thus implementation of both norms) by promoting an international dialogue and collaborative approach.

It is important to note that the Geneva Dialogue experts have recognised that each of the listed stakeholders has many sub-groups that might have additional specific roles and responsibilities. For instance, manufacturers include producers of software and hardware, as well as service operators of the cloud or telecommunication infrastructure, while civil society includes advocacy groups, grassroot organisations, think-tank and educational institutions. In addition, there may be a need to elaborate on roles of responsibilities of additional stakeholder groups, such as the standardisation community. Such discussion may be part of the future work of the Geneva Dialogue, towards the next edition of the Geneva Manual.

Separately, the Geneva Dialogue experts have discussed expectations from **states and regional organisations** and highlighted their role in coordinating efforts with other states to ensure the ICT supply chain security (given ICT supply chains are global and cross-border) as well as in addressing security issues in digital products with efficient legal framework and policies:

- Codifying the norms and promoting responsible behaviour norms should be translated into **clear regulatory expectations**, though this can be very challenging given the complex nature of ICT supply chains. The clear interoperable security criteria for testing and security assessments are needed to address both technical and political concerns these days

- However, even if such regulatory frameworks emerge, the challenge is to ensure the **adoption of cybersecurity recommendations** across organisations, especially across small and medium companies. While guidelines may be published to mitigate supply chain vulnerabilities and reduce risks, it remains unclear how to ensure that organisations actually follow these recommendations

- In the context of OSS, government bodies could step in **coordinating efforts between manufacturers, open-source community, and other relevant parties**, sharing information, and leveraging international collaborations to address cybersecurity threats and support their respective countries in times of crisis

- The national governments' ability to **communicate and collaborate with other states** is considered crucial in effectively addressing cybersecurity challenges, as well

- States are also expected to **encourage responsible reporting of ICT vulnerabilities, recognise their exploitation as a threat**, **increase transparency** about stockpiling of ICT vulnerabilities (such as through vulnerability equities processes, VEP), and **limit commercial exploitation of ICT vulnerabilities.**

5 Messages and next steps: Areas requiring further discussion and action

The Geneva Manual builds on the principle of 'shared responsibility' and, as the Geneva Dialogue, highlights the importance of multistakeholder participation in the implementation of agreed cyber norms and, thus, in ensuring security and stability in cyberspace. Success in reducing risks in cyberspace relies on an effective multistakeholder participation. However, it also comes with several challenges: power imbalances (e.g. between larger private companies and individual independent OSS developers), communication barriers (e.g. difference in technical expertise between cybersecurity researchers and academia), resource disparities, lack of trust, changing dynamics (i.e. changes in leadership and organisational structures) and others.

The inaugural edition of the Geneva Manual reveals numerous areas where relevant non-state stakeholders have different views, but also where they come to agreement with each other and with the norms as a 'product' of inter-state diplomatic agreements and views. These areas include:

- *#Norms and #roles* Stakeholders agree with the norms in general and that everyone has a role to play, though the private sector, and especially those who develop digital products, have a bigger role to play

- *#Civilsociety* Relevant non-state stakeholders from civil society and academia do have a role to play to implement the two norms on ICT supply chain security and responsible reporting of ICT vulnerabilities. In particular, they are critical in posing challenging questions (e.g., addressing human rights implications resulting from the exploitation of ICT vulnerabilities by private and state actors) and fostering trust among different stakeholders to promote an international dialogue and collaborative approach

- *#Norms* Translating the two norms into more practical actions, including policies and regulations are of the essence. A neutral and geopolitics-free governance framework is required to globally approach the security of ICT supply chains, responsible reporting of ICT vulnerabilities, and security of digital products. While this may be an ambitious goal, the Geneva Dialogue experts emphasised the significance of international dialogue across different jurisdictions involving industry, the private sector, independent developers, SMEs, cybersecurity researchers, and technical community members who contribute to responsible vulnerability disclosure

- *#Governments* Stakeholders do also expect governments to take a lead and set an example by implementing the norms. This would, in particular, include steps to responsible report vulnerabilities and enhance transparency in government disclosure decision processes

- *#Regulations* Emerging cybersecurity regulations should avoid requirements to mandate reporting of unpatched vulnerabilities to anyone else but to code owner in order to minimise the risks of accessing this information by malicious actors

- *#OSS* Implementing both norms is impossible without actively involving, and paying attention to, the OSS community. The community-driven open source development is the achievement in the software development industry which enables technological innovation and growth. And while the security of open-source projects is a challenge, there are ways – more creative than regulations – to support OSS contributors to adhere

to a more secure code and practices to mitigate vulnerabilities and respond to incidents related to OSS projects

- *#Norms* Increasing geopolitical polarisation and technological competition between jurisdictions end up with conflicting laws and therefore poses a challenge for relevant non-state stakeholders to implement the norm, specifically norm 13i, and address risks associated with ICT supply chain security

- *#Vulnerabilityreporting* There is a need for legal reforms that decriminalise vulnerability reporting and provide clear protections for researchers. Establishing supportive legal frameworks to implement the norm, specifically norm 13j, and which focus on encouraging responsible reporting without malicious intent can foster a more welcoming environment for researchers to come forward with their findings

At the same time there are open questions which require future discussion with relevant non-state stakeholders and further iterations of work to expand the views captured in the Geneva Manual. These questions include:

- Is it possible to develop common global rules for ICT supply chain security today? Is there an appropriate international platform for facilitating these discussions?

- How can the implementation of both norms be measured?

- How can we avoid the emergence of regulations mandating the reporting of unpatched ICT vulnerabilities to governments and the risks associated with such reporting?

- How should states protect ethical researchers and incentivise them to responsibly report vulnerabilities to relevant code owners and manufacturers?

- Do citizen customers of digital products have a role and responsibility to play in implementing both norms?

- How can customers and manufacturers of digital products be incentivised to choose cybersecurity along with convenience and innovation?

- How can we enhance private and state actors' accountability in exploiting ICT vulnerabilities?

- How can civil society and academia help address risks for human rights stemming from the exploitation of ICT vulnerabilities?

- What can industry and governments do to support the OSS community in producing a more secure code while avoiding demotivating OSS development and innovation?

These and other more specific questions will guide the Geneva Dialogue in further work to address the implementation gap in discussion with the relevant non-state stakeholders.

6 Recommended resources

ATT&CK Matrix for Enterprise, MITRE ATT&CK®, by MITRE

Brief on UN OEWG and UN GGE processes at DigWatch

Cyber Incident Tracer, by CyberPeace Institute

Cybersecurity 10 Principles, by the Charter of Trust

EU 5G Security Toolbox, by the European Union

Geneva Declaration on Targeted Surveillance and Human Rights, initiated by AccessNow, the Government of Catalonia, the private sector, and civil society organisations

Geneva Dialogue webinars on vulnerabilities in digital products: webinar on risks and impacts of vulnerabilities, and webinar on who can do what about it (2023)

Geneva Dialogue output report on 'Security of digital products and services: Reducing vulnerabilities and secure design: Good practices' (2021)

Geneva Dialogue comparative analysis on 'Governance Approaches to the Security of Digital Products' (2021)

Geneva Dialogue event reports on 'Security of digital products and the regulatory environment' and 'Security of digital products and international standards' (2021)

Geneva Dialogue output report on 'Security of digital products and services: Reducing vulnerabilities and secure design: Good practices' (2020)

GCA Cybersecurity Toolkit For Small Business, by Global Cyber Alliance

Global Encryption Coalition, by the Center for Democracy and Technology, Global Partners Digital, Mozilla Corporation, Internet Society, and the Internet Freedom Foundation

Glog.ai: a project to implement AI to auto-remediate vulnerabilities in OSS

Guide for Evaluating OSS, by OpenSFF

Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure (2020), by FIRST

Hardware Bill of Materials (HBOM), by CycloneDX

International 'Secure by Design' guidance from 18 countries (national authorities), by the US Cybersecurity and Infrastructure Security Agency (CISA)

ISO vulnerability disclosure and handling standards: ISO/IEC 29147 and ISO/IEC 30111

Norms of the Global Commission on the Stability of Cyberspace

NIS2 Directive: Directive on measures for a high common level of cybersecurity across the European Union

OECD Recommendations on Digital Security Risk Management and High-level principles to enhance the Digital Security of Products

OECD Recommendations on the Treatment of Digital Security Vulnerabilities (2022)

OSCE Confidence-Building Measures to reduce the risks of conflict stemming from the use of information and communication technologies (2016)

OSS Code Scanning, by GitHub

OSS Guidance on adding a security policy to a repository, by GitHub

OSS Guidance on the vulnerability reporting process, by Linux Foundation

OSS Guide to Implementing Implementing a Coordinated Vulnerability Disclosure, by GitHub

OSS Secret Scanning, by GitHub

OSS Vulnerability Guide, by GitHub

Paris Call for Trust and Security in Cyberspace: 9 Principles

Paris Call for Trust and Security in Cyberspace: Report on Securing ICT Supply Chains (2021)

Secret Scanning for OSS, by GitHub

Security.txt: a proposed standard to allow websites to define security policies, by Google, Facebook, GitHub, the UK government, and other international partners

Singapore Common Criteria Scheme, by the Singapore Cyber Security Agency (CSA)

Singapore Cybersecurity Labelling Scheme (CLS), by the Singapore Cyber Security Agency (CSA)

Singapore Cybersecurity Labelling Scheme (CLS) for Medical Devices, by the Singapore Cyber Security Agency (CSA)

Software Bill of Materials (SBOM), by the US Cybersecurity and Infrastructure Security Agency (CISA)

SP 800-218 Secure Software Development Framework (SSDF), by the US National Institute of Standards and Technology

Supply chain security guidance, by the UK National Cyber Security Centre

Swiss Digital Initiative: an example of the effort to bring ethical principles and values into technologies

Vulnerability Disclosure Cheat Sheet: Reporting Vulnerabilities, by OWASP

Vulnerability Exploitability eXchange (VEX) - an overview, by the US National Telecommunications and Information Administration (NTIA)

7 Annex

UN GGE 2013 (A/68/98), UN GGE 2015 (A/70/174) and UN GGE 2021 (A/76/135) reports provide the following two norms related to supply chain security and responsible reporting of ICT vulnerabilities:

Norm 13 (i) "States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions."

56. This norm recognizes the need to promote end user confidence and trust in an ICT environment that is open, secure, stable, accessible and peaceful. Ensuring the integrity of the ICT supply chain and the security of ICT products, and preventing the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions are increasingly critical in that regard, as well as to international security, and digital and broader economic development.

57. Global ICT supply chains are extensive, increasingly complex and interdependent, and involve many different parties. Reasonable steps to promote openness and ensure the integrity, stability and security of the supply chain can include:

(a) Putting in place at the national level comprehensive, transparent, objective and impartial frameworks and mechanisms for supply chain risk management, consistent with a State's international obligations. Such frameworks may include risk assessments that take into account a variety of factors, including the benefits and risks of new technologies.

(b) Establishing policies and programmes to objectively promote the adoption of good practices by suppliers and vendors of ICT equipment and systems in order to build international confidence in the integrity and security of ICT products and services, enhance quality and promote choice.

(c) Increased attention in national policy and in dialogue with States and relevant actors at the United Nations and other fora on how to ensure all States can compete and innovate on an equal footing, so as to enable the full realization of ICTs to increase global social and economic development and contribute to the maintenance of international peace and security, while also safeguarding national security and the public interest.

(d) Cooperative measures such as exchanges of good practices at the bilateral, regional and multilateral levels on supply chain risk management; developing and implementing globally interoperable common rules and standards for supply chain security; and other approaches aimed at decreasing supply chain vulnerabilities.

58. To prevent the development and proliferation of malicious ICT tools and techniques and the use of harmful hidden functions, including backdoors, States can consider putting in place at the national level:

(a) Measures to enhance the integrity of the supply chain, including by requiring ICT vendors to incorporate safety and security in the design, development and throughout the lifecycle of ICT products. To this end, States may also consider establishing independent and impartial certification processes.

(b) Legislative and other safeguards that enhance the protection of data and privacy.

(c) Measures that prohibit the introduction of harmful hidden functions and the exploitation of vulnerabilities in ICT products that may compromise the confidentiality, integrity and availability of systems and networks, including in critical infrastructure.

59. In addition to the steps and measures outlined above, States should continue to encourage the private sector and civil society to play an appropriate role to improve the security of and in the use of ICTs, including supply chain security for ICT products, and thus contribute to meeting the objectives of this norm.

Norm 13 (j) "States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure."

60. This norm reminds States of the importance of ensuring that ICT vulnerabilities are addressed quickly in order to reduce the possibility of exploitation by malicious actors. Timely discovery and responsible disclosure and reporting of ICT vulnerabilities can prevent harmful or threatening practices, increase trust and confidence, and reduce related threats to international security and stability.

61. Vulnerability disclosure policies and programmes, as well as related international cooperation, aim to provide a reliable and consistent process to routinize such disclosures. A coordinated vulnerability disclosure process can minimize the harm to society posed by vulnerable products and systematize the reporting of ICT A/76/135 16/26 21-04030 vulnerabilities and requests for assistance between countries and emergency response teams. Such processes should be consistent with domestic legislation.

62. At the national, regional and international level, States could consider putting in place impartial legal frameworks, policies and programmes to guide decision - making on the handling of ICT vulnerabilities and curb their commercial distribution as a means to protect against any misuse that may pose a risk to international peace and security or human rights and fundamental freedoms. States could also consider putting in place legal protections for researchers and penetration testers.

63. In addition, and in consultation with relevant industry and other ICT security actors, States can develop guidance and incentives, consistent with relevant international technical standards, on the responsible reporting and management of vulnerabilities and the respective roles and responsibilities of different stakeholders in reporting processes; the types of technical information to be disclosed or publicly shared, including the sharing of technical information on ICT incidents that are severe; and how to handle sensitive data and ensure the security and confidentiality of information.

64. The recommendations on confidence-building and international cooperation, assistance and capacity-building of previous GGEs can be particularly helpful for developing a shared understanding of the mechanisms and processes that States can put in place for responsible vulnerability disclosure. States can consider using existing multilateral, regional and sub-regional bodies and other relevant channels and platforms involving different stakeholders to this end.

Further elaboration of these norms can be found in the UN GGE 2021 report (A/76/135).

Subsequently, the final report of the UN OEWG (A/AC.290/2021/CRP.2) in 2019 also provide that, "*States, reaffirming General Assembly resolution 70/237 and acknowledging General Assembly resolution 73/27, should: take reasonable steps to ensure the integrity of the supply chain, including through the development of objective cooperative measures, so that end users can have confidence in the security of ICT products; seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions; and encourage the responsible reporting of vulnerabilities*" (para 28).

8 Contributors

The Geneva Manual on Responsible Behaviour in Cyberspace: Implementation of Norms by Relevant Non-State Stakeholders

December 2023

Published by DiploFoundation

Authors: Anastasiya Kazakova (DiploFoundation), Vladimir Radunović (DiploFoundation), Serge Droz (Swiss Federal Department of Foreign Affairs)

Illustrations: Vladimir Veljasevic (DiploFoundation)

Layout and design: Viktor Mijatović (DiploFoundation), Aleksandar Nedeljkov (DiploFoundation)

Contributors to the Geneva Dialogue in 2023 include both organisations and experts participating in their personal capacity:

- Private sector companies and organisations: ABB, Alibaba, Bi.Zone (Sber Group), Cisco, CL2R Advisory, Cognizant, Ensign InfoSecurity, Ericsson, FireEye, Huawei, InfoGuard, Kaspersky, Mandiant, Microsoft, PNG Digital ICT Cluster, Proton, QI-ANXIN, Roche, SICPA, Siemens, Swiss Re, Swiss Risk Association, Tata Consultancy Services, Tech Mahindra, UBS, Wisekey, and Vu Security
- Academia and policy experts: Winnona DeSombre (Atlantic Council), Bart Hogeveen (Australian Strategic Policy Institute), Imad Aad and Melanie Kolbe-Guyot (Center for Digital Trust (C4DT) - EPFL), Lennart Maschmeyer (Center for Security Studies (CSS) at ETH Zurich), Jan Martin Lemnitzer (Copenhagen Business School), Katherine Getao (Cyber Hygiene, Cyber Diplomacy, and ICT Strategy and Governance Consultant, former CEO of ICT Authority in Kenya and the Kenyan representative to the UN GGE), Mischa Hansel (Berlin University of Economics and Law, HWR Berlin), Jen Ellis (NextJen Security), Benjamin Ang (S. Rajaratnam School of International Studies, RSIS), Alexandra Paulus (Stiftung Neue Verantwortung, SNV), Nicolas Zahn (Swiss Digital Initiative), Jeroen van der Ham (University of Twente and FIRST), Chao Wang (Wuhan University)
- Technical community experts: Pablo Hinojosa (APNIC), Madison Q. Oliver (GitHub Security Labs), Klée Aiken (FIRST), Koichiro Komiyama (JPCERT/CC), Steven Sim Kok Leong (OT-ISAC Executive Committee, Singapore), Maninder Singh Narang, Takayuki Uchiyama
- Civil society organisations and experts: Consumers International, CyberPeace Institute, CIPESA, DataSphere Initiative, Christopher James Sampson (Future Earth Systems), Global Forum on Cyber Expertise, Global Partners Digital, ICT4Peace, Swiss Digital Initiative

genevadialogue@diplomacy.edu

https://genevadialogue.ch/