2021 13th International Conference on Cyber Conflict
Going Viral
T. Jančárková, L. Lindström, G. Visky, P. Zotz (Eds.)
2021 © NATO CCDCOE Publications, Tallinn

Impact of Good Corporate Practices for Security of Digital Products on Global Cyber Stability

Vladimir Radunović
DiploFoundation
Belgrade, Serbia

Jonas Grätz-Hoffmann
Federal Department of Foreign Affairs
Bern, Switzerland

Marilia Maciel
DiploFoundation
Strasbourg, France

Abstract: The exploitation of vulnerabilities in digital products and services is an essential component of sophisticated cyberattacks. Well-resourced adversaries increasingly exploit vulnerabilities for economic, political, or military gain, causing effects that destabilise cyberspace. Several multilateral and multi-stakeholder fora develop norms and principles to reduce such vulnerabilities. The main challenge lies in implementation. Under the Geneva Dialogue on Responsible Behaviour in Cyberspace[1] (Geneva Dialogue), a dozen leading global companies jointly developed a set of good corporate practices that translate high-level principles into day-to-day operations. This paper argues that these practices make cyberspace less vulnerable, and thus contribute to the implementation of global norms and principles. It further analyses key global norms and principles related to the security of digital products and services and the role of industry. It then presents the most relevant results of the ongoing work of the Geneva Dialogue, particularly good corporate practices related to security by design: threat modelling, supply chain security, development and deployment, and vulnerability processes. It discusses how these measures may reduce vulnerabilities, especially for smaller producers whose importance in the supply chain was elevated by COVID-19. It reflects on the need to turn good practices into baseline requirements to support market newcomers and regulators worldwide.

Keywords: *cybersecurity, cyber norms, vulnerability, good practices, digital products, multi-stakeholder cooperation*

[1] The Geneva Dialogue (https://genevadialogue.ch) is an initiative of the Swiss government and DiploFoundation. Partners of the Geneva Dialogue include Bi.Zone, Cisco, EnSign, FireEye Mandiant, Kaspersky, Huawei, Microsoft, UBS, PNG ICT Cluster, SICPA, Siemens, SwissRe, Tata Consultancy Services, VU, and Wisekey. Good corporate practices regarding the security of digital products and services, discussed in detail in this paper, have been developed through 15 group online meetings and continuous collaboration in the shared document, conducted over 7 months in 2020.

1. INTRODUCTION

Threat actors often exploit vulnerabilities in digital products, making information and communication technology (ICT) companies an initial target of their operations in order to reach their ultimate goals (Hurel and Lobato 2018). The exploitation of vulnerabilities within the supply chain of digital products by Advanced Persistent Threat (APT) actors may impose high economic costs and impact international stability. Two examples stand out. First, the NotPetya ransomware – which exploited vulnerabilities in Windows and spread through the global supply chain via a compromised update of accountancy software in Ukraine – resulted in more than US$10 billion in damages (Greenberg 2018). The US and UK governments publicly attributed the attack to the Russian military (White House 2018; UK NCSC 2018). Second, the SolarWinds hack – where a software update was compromised and was allegedly engineered by a state-sponsored APT actor (CISA 2020) – created a backdoor to about 18,000 entities (SolarWinds 2020), including US public institutions and large corporations.

The exploitation of vulnerabilities is one of the most frequent components of sophisticated cyberattacks (Uren, Hogeveen and Hanson 2018). Product security also plays a fundamental role in the development of offensive cyber capabilities, since a cyberattack is realised when the capabilities of the attackers match the possibility to exploit a vulnerability (Mladenović and Radunović 2018). Leading technical frameworks for describing sophisticated APT attacks also consider the exploitation of vulnerabilities among major components: 'Exploiting a vulnerability to execute code on a victim's system' represents the fourth phase of the Lockheed Martin Cyber Kill Chain™ (Hutchins, Cloppert and Amin 2011), while the MITRE ATT&CK framework of adversarial tactics and techniques reflects on exploiting vulnerabilities at various stages of an attack, starting with developing capabilities by 'building or acquiring solutions such as malware, exploits, and self-signed certificates' (MITRE n.d.).

Unsecured digital products allow attacks that damage global cyber stability. Therefore, states must cooperate with industry to implement international cybersecurity norms and principles (hereinafter referred to as 'norms and principles') – particularly those related to the integrity of the supply chain and the responsible reporting of vulnerabilities.

In this paper we review the related international norms and principles and discuss good corporate practices related to the security of digital products that contribute to the implementation of these norms and principles, and hence to global cyber stability.

2. THE ROLE OF THE BUSINESS SECTOR IN IMPLEMENTING CYBERSECURITY NORMS AND PRINCIPLES

Norms and principles agreed upon at the level of the UN General Assembly (UN GA) have the highest normative authority. This holds true for the report of the 2013–2015 UN Group of Governmental Experts (GGE 2015), which contains 11 voluntary norms for the responsible behaviour of states in cyberspace and has since been endorsed by the UN GA. Since then, there have not been major breakthroughs in the development of norms at the UN level. A further GGE (2016–2017) did not produce a consensus report. The debate continues in the framework of the 2018–2021 GGE (UNODA 2021). The UN Open-Ended Working Group (OEWG), which has been open to all UN member states, did produce a consensus report in March 2021. It contains an important reaffirmation of the need to implement the 11 norms agreed upon in 2015 and directs particular attention to protecting critical health infrastructure, the integrity of the supply chain and responsible reporting of vulnerabilities (UN GA 2021, 5). In 2020, Russia led the process of establishing a new 2021–2025 OEWG, which should, according to its mandate (UN GA 2020), further develop the rules, norms and principles of responsible behaviour.

In this context, better implementation of existing norms and principles is essential to enhancing cyber stability. Implementation takes different approaches at different levels. Some government-led and non-government initiatives aim to clarify, fill the gaps, or strengthen compliance with the norms developed by the GGE.

In parallel, non-government-led initiatives focusing on norms and principles have also flourished in recent years. This is an important development because the UN processes remain intergovernmental and the norms developed therein are targeted at states, even if they indirectly impact other actors. Non-government initiatives, however, expand the group of actors that hold *agency* (Passoth 2012) in promoting cyber stability and assigning active responsibilities to companies, the technical community and individuals. These normative efforts aim not only to pull non-government actors to comply with norms announced by the GGE, but also to fill gaps in these norms.

Table I shows the norms developed by the 2013–2015 GGE focusing on the security of digital products and services that have been echoed by some multi-stakeholder initiatives, including: a) the Global Commission on the Stability of Cyberspace (GCSC); b) the Paris Call for Trust and Security in Cyberspace (Paris Call); and c) the Charter of Trust.

TABLE I: A COMPARISON BETWEEN NORMS FOCUSED ON THE SECURITY OF DIGITAL PRODUCTS AND SERVICES BY THE UN GGE AND MULTI-STAKEHOLDER INITIATIVES, ADAPTED FROM GROTTOLA (2020)

UN GGE (GGE 2015)	**UN OEWG** (UN GA 2021)	**GCSC** (GCSC 2019)	**Paris Call** (Paris Call 2018)	**Charter of Trust** (Charter of Trust 2018)
Protection of the integrity of the supply chain (para 13 (i))	States 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'.	**Avoidance of tampering:** State and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with (Norm 3). **ICT devices and botnets:** State and non-state actors should not commandeer the general public's ICT resources for use as botnets or for similar purposes (Norm 4).	**Lifecycle security:** Strengthen the security of digital processes, products and services throughout their lifecycle and supply chain (Principle 6).	**Responsibility throughout the supply chain:** Ensure confidentiality, authenticity, integrity and availability by setting baseline standards (Principle 2). **Security by default:** Adopt the highest appropriate level of security and data protection and ensure that it is preconfigured into the design of products, processes, technologies, etc. (Principle 3).
Sharing vulnerability knowledge (para 13 (j))	States should 'encourage the responsible reporting of vulnerabilities'.	**Vulnerability equity process:** States should create transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities, with the default presumption in favour of disclosure (Norm 5). **Reduce and mitigate significant vulnerabilities:** Developers and producers of products and services on which cyber stability depends should (1) prioritise security and stability, (2) take reasonable steps to ensure their products and services are free from significant vulnerabilities, and (3) take measures to mitigate vulnerabilities that are later discovered in a timely manner and to be transparent about the process (Norm 6).		

At the same time, norms must be rooted in practice and acted upon (Finnemore and Hollis 2016). The implementation of norms depends on shared ownership with engagement from both the private sector and civil society (Klimburg and Almeida 2019).

Industry plays a particular role, as the main driver and pace-setter of innovation (Kaufmann 2016), in creating digital products and owning most infrastructure. Since cyberattacks are typically executed remotely from different locations, global reach is one distinct advantage of industry over states when it comes to norm implementation. Hence, if global ICT and related industries implement similar good practices (e.g. vulnerability disclosure), norm implementation will also be advanced globally, rather than only nationally or regionally. Even though states are ultimately responsible for global cyber stability, other actors can make destabilising actions more costly by implementing existing norms and principles. This holds especially true for the private sector.

Industry generally shares an interest in having a more stable global cyberspace and protecting their business model. Early arguments have pointed to the growing economic costs of cyberattacks that would drive companies towards responsible behaviour (Anderson 2001). Voluntary corporate social responsibility, based on ‘a range of corporate motives, including integrated internal motives and external pressures’, is particularly important in areas in which designing holistic legal instruments is difficult (Airike, Rotter and Mark-Herbert 2016, 9).

The literature has already identified a few roles for industry in the implementation of norms, such as assisting with attribution (Fairbank 2019, 394). A mapping by the Geneva Dialogue (Rizmal and Radunović 2019) outlines several roles the corporate sector assumes and advocates for: a) information sharing on best practice and vulnerabilities, b) developing corporate norms through standardisation (focused on security by design), c) ensuring end-user security by prioritising privacy, integrity and reliability in design, and d) ensuring transparency regarding products and breaches. In addition, companies contribute to the protection of critical infrastructure and thoroughly test products (Eggenschwiler 2018).

Yet there is also growing recognition that voluntary corporate social responsibility may not be enough, and that industry must do more to enhance the security of their own products in contribution to the implementation of norms (Maxwell and Barnsby 2019). Matwyshyn (2010) warned producers were not sufficiently transparent regarding the security of their products and suggested a three-layered commitment: 1) control the security of their code, 2) warn when vulnerabilities emerge and exploitations occur, and 3) provide fixes and patches. Hathaway and Savage (2012) went further to suggest company liability, with regulations requiring a specific vulnerability disclosure process as well as an early warning requirement, among others. Because many institutions need longer than 30 days (considered the gold standard) to apply patches – if they are able to at all – they should take greater social and legal responsibility to prevent the emergence of vulnerabilities in the first place (Hathaway 2019).

Increasing expectations, coupled with cases of APT operations that exploited vulnerabilities in widespread commercial products and with various normative initiatives and global principles, have put pressure on companies to invest more in securing their digital products. Yet, it has also become clear that the cost related to patching discovered vulnerabilities (and to reputation) surpasses the cost of embedding security throughout the development lifecycle (Dougherty et al. 2018). At the same time, the community has started mapping and discussing weaknesses in the design or implementation of security architecture (particularly in software) of various producers (Santos, Tarrit and Mirakhorli 2017). All this has incentivised companies to turn (some of) their efforts to reducing vulnerabilities during the pre-market phase, instead of (only) reacting to them once the product is on the market.

3. GOOD CORPORATE PRACTICES FOR SECURITY OF DIGITAL PRODUCTS AND SERVICES

This section of the paper serves to highlight current industry approaches to enhance the security of digital products. It draws on the findings from the Geneva Dialogue (Radunović and Grätz 2020).

3.1. Security by Design and Related Concepts

The concept of *security by design* has emerged in relation to software, hardware, services, and system integration. Geneva Dialogue partners defined it as ‘designing with security in mind: addressing risks from an early stage and throughout the product development lifecycle. It may be understood as designing with security controls from the beginning’ (Radunović and Grätz 2020, 5). Importantly, companies understand this as a comprehensive process that considers engineering, security, business, and human resources aspects, and involves engineers, security professionals, and C-level management.

Further, industry partners outline the *security development lifecycle* (SDL) as the most common practical model of implementing security by design. It requires producers to model security risks, driving timely decisions about reducing risk throughout the development lifecycle. SDL is particularly applied in software development but is increasingly being adapted to cloud services and internet of things (IoT) devices.

Finally, the concept of the *trustworthiness* of products relates to 'the rigorous application of design principles and concepts within a disciplined and structured set of processes that provides the necessary evidence and transparency to support risk-informed decision making and trades' (Ross, McEvilley and Carrier Oren 2016). It can be understood more broadly as a fresh perspective on SDL, which also considers non-technical issues such as internal processes and reputation (Buchheit et al. 2020), thereby relating to the trustworthiness of producers and their internal processes, rather than just products.

3.2. Good Corporate Practices

After in-depth discussions on good practices, industry partners of the Geneva Dialogue distinguished several main elements of security by design: threat modelling, supply chain and third-party security, secure development deployment, and vulnerability processes and support. In addition, they recognised the need to adjust the corporate mindset and internal processes to the security by design approach as a cross-cutting element. These elements apply across industries: software, hardware and devices, online services, and integrated systems.

3.2.1. Threat Modelling

Threat modelling is 'an engineering technique to identify possible threats, attacks, vulnerable areas, and countermeasures that could affect the product or the related environment' (Radunović and Grätz 2020, 8), which should be conducted throughout the product lifecycle and involve different departments of the company – from developers and cybersecurity specialists to senior management. Threat models depend on specific customers and the way products are implemented and used; therefore, direct cooperation with customers is recommended when possible.

Steps for performing threat modelling include: (a) identifying assets, (b) defining security requirements, (c) creating a diagram of the system, (d) identifying and analysing threats, (e) performing risk management and prioritisation, (f) mitigating threats and identifying fixes, and (g) validating mitigation (Cisco n.d.; Microsoft n.d.). In industry environments, Geneva Dialogue partners noted it is necessary to look into the system as a whole rather than focusing only on its components.

3.2.2. Supply Chain and Third-party Security

Producers commonly integrate third-party components (TPC) – both proprietary and open source – into their digital products. It is crucial that companies 'offer updates, upgrades, and patches throughout a reasonable lifecycle for their products, systems, and services via a secure update mechanism' to ensure a secure supply chain (Charter of Trust 2020a, 2). Geneva Dialogue partner practices underline the importance of a risk-based approach for digital supply chains based on three components: 1) baseline requirements, which should also include transparency of TPC and may be an integral part of contracts, 2) supplier criticality, including defining different requirements and compliance modalities (from self-declaration and self-assessment to external audits) for various types of TPC suppliers depending on their level of criticality, and 3) verification, including establishing an internal supply chain risk management team.

Companies should create and maintain an inventory of TPC by developing a product bill of materials (BoM), creating tools for scanning and decomposition to inspect source code and images, or issuing unique IDs for hardware components. Companies should also devise a plan for when new vulnerabilities are discovered and notify suppliers about discovered TPC vulnerabilities. It is particularly important to monitor TPC that have reached their end-of-life (EoL), and thus are left without support. Suppliers, on their side, should monitor disposing of their product by EoL. Finally, producer transparency regarding the development process is crucial, and may be enhanced through transparency centres, even though the effects may be limited in cases where customers have limited knowledge of the product in question or limited resources to thoroughly check security.

3.2.3. Secure Development and Deployment

Security needs to be embedded in product development, building and testing, releasing and deployment, and validation and compliance. Security rules and checks in automated continuous integration and continuous delivery software pipelines include responsible coding, scanning source codes for vulnerabilities, dynamic analysis of code, checking dependencies for vulnerabilities, and unit tests with security checks. Particular attention must be paid to the build environment to prevent unauthorised changes, as was the case with the compromise of the SolarWinds build (CrowdStrike Intelligence Team 2021). Companies should use vetted common modules and libraries that focus on secure communications, coding and information storage.

When it comes to software, testing for vulnerabilities and validation involves static and dynamic testing, vulnerability assessment, fuzzing, penetration testing, protocol robustness testing and web application scanning. While third parties may be involved in conducting specific tests (e.g. bug-bounty programmes), a third-party audit of product and update development processes is equally important. In the case of integrated systems, testing is required for the overall configuration in addition to each of the components.

3.2.4. Vulnerability Processes and Support

Companies also set up processes to react to discovered and reported vulnerabilities by developing and distributing fixes and supporting customers. This goes hand in hand with regulatory efforts in establishing responsible vulnerability disclosure policies, as called for by global norms. Geneva Dialogue industry partners have suggested the following elements of the process with explanations below:

- Vulnerability management: Producer 'practices and security controls to ensure products are running with the latest security updates (...) including monitoring and mitigating the effects of vulnerabilities in TPC used' (Radunović and Grätz 2020, 15). A dedicated internal product security team – often dubbed Product Security Incident Response Team (PSIRT) – should be established with a clear protocol for security servicing and plans for reacting to vulnerabilities, serving as a contact point, working in close cooperation with development, security and other teams, and issuing public security advisories.
- Vulnerability handling: Analysis of a vulnerability that is discovered or reported to the vendor, and the required remediation (i.e. developing a fix or update).
- Vulnerability disclosure: 'Overarching term for the process of sharing vulnerability information between relevant stakeholders' (Radunović and Grätz 2020, 16), related to the element below.
- Vulnerability reporting: Third-party reporting to a producer about the vulnerabilities discovered in a producer's product.
- Coordinated vulnerability disclosure: 'Coordinated information sharing and mitigation efforts about reported vulnerabilities, with producers, researchers, and other interested stakeholders' (Radunović and Grätz 2020, 17). The term *responsible vulnerability disclosure* is sometimes used instead to emphasise ethical aspects, implying a proactive investment by either party in ensuring the end goal of minimum user risk.

Importantly, this understanding of vulnerability reporting, management, and coordinated disclosure is in line with the definitions by one of the lead authorities, the Carnegie Mellon University CERT (Householder et al. 2017), while the latter is in line with the ISO/IEC 29147:2014 standard (ISO 2014).

There is a particular challenge related to the deployment of updates, since some customers may miss information about vulnerabilities and fixes and others may lack the capacity to apply them, while certain critical and complex sectors may risk their regular operations if they deploy the patch. While more research on assessing the effectiveness of patching processes is needed, it is essential that companies put more focus on preventing vulnerabilities in the first place.

3.2.5. Adjusting the Mindset and Internal Processes

Secure design demands companies to establish the right mindset throughout an organisation; understanding security is everyone's task (Charter of Trust 2018, Principle 1). This requires 'ensuring that the organisation's people, processes, and technology are prepared to perform secure software development at the organisation level' (Dodson, Souppaya and Scarfone 2020, 4). Organisational setup should bring security and developer teams closer and enable different departments – including C-level management – to be involved throughout the product design lifecycle.

Continuous training throughout a company is essential, especially among engineers that implement security features during the design phase in cooperation with security teams. It should involve multiple teams and be practical and interactive (including games and realistic simulations). In addition, training for customers and third parties should also be provided where possible 'to help government organisations, academia, and other companies to develop skills and knowledge for product security evaluation' and 'allow them to benefit from the transparency on the product security and vulnerability related policies' (Radunović and Grätz 2020, 21).

4. ADVANCING THE IMPLEMENTATION OF GOOD CORPORATE PRACTICES TO ENHANCE CYBER STABILITY

If implemented consistently, good practices among large companies – particularly those whose products are widely used across various sectors and infrastructure – will have a wider positive impact. This has been underlined by recent major attacks enabled by design flaws, as described above. Hence, implementing the above-mentioned good practices will have a positive impact on cyber stability. This underscores the urgency to ensure that most, if not all, producers introduce security by design practices.

High complexity, market failures, unclear responsibilities, and lack of national and global cooperation are inhibiting greater security of digital products (OECD 2021). In the following section, we will discuss how increasing interdependence, regulatory action and globally agreed baseline requirements can address some of these issues, thereby contributing to the broader and more rigorous adoption of security by design practices.

4.1 Increasing Interdependence

The increasing interdependence of digital products and services (a supply chain issue) and the increasing level of criticality of ordinary services due to COVID-19 (pandemic-driven digitalisation) have enhanced vulnerabilities. The emerging IoT environment adds to this by integrating physical systems with the digital world (Carruthers 2016), allowing cyberattacks to generate even more far-reaching physical impacts.

4.1.1. Supply Chain

Digital products and services increasingly rely on TPC. This trend may be more intuitive for products such as hardware, where different manufacturers specialise to produce different components, as well as with integrated systems. It is also a trend in software development: open-source software (OSS) and off-the-shelf components have a clear advantage over in-house software (Badampudi, Wohlin and Petersen 2016). Geneva Dialogue partners warn about a risk with OSS as TPC, and examples like the Ripple20 and Amnesia:33 reports about vulnerabilities impacting the medical, transportation, energy, and retail industries are illustrative (Kol and Oberman 2020; dos Santos et al. 2020). It is therefore important that various producers, including open-source communities, embrace the elements of security by design discussed above to reduce the risks from TPC. This would contribute to a more secure supply chain – a goal set by the 2015 GGE Report (art. 13(i)), the Paris Call (Principle 6), and the Charter of Trust (Principle 2), among others.

At the same time, national security considerations play an important role in supply chain security. The development of state-sponsored attacks that exploit vulnerabilities has contributed to increased digital security risk (OECD 2021, 25). There is a risk of states influencing suppliers to embed hidden functions or weaknesses into digital products, thus making the supply chain vulnerable. A report by the UK government warns of the significant access that some states have to supply chains, which may lead to espionage and disruptive or destructive operations (UK 2019, 23). The EU invites supply chain risk assessments to also take into account non-technical factors by assessing suppliers based on inter alia the likelihood of interference from a non-EU country, the degree of control over its own supply chain, and the prioritisation of security practices (NIS Cooperation Group 2019, 22).

The increasing attention towards supply chain risks may incentivise industry to manage those risks more proactively, with broader implications for the adoption of good practices by small and medium-sized enterprises and start-ups.

4.1.2. Pandemic-driven Digitalisation

The pandemic has accelerated the overall digitalisation of society to unforeseen levels. According to McKinsey & Company (2020), companies have accelerated the digitalisation of their customer and supply chain by three to four years, while the share of digital or digitally-enabled products in their portfolios have been accelerated by seven years. Almost overnight, some ordinary services have become essential in society's 'new normal'. E-commerce, for instance, has allowed continued business cooperation (OECD 2020).

Most of these services were never conceived with security as a priority: Producers, often smaller enterprises and even start-ups, have used limited resources to focus on functionality and affordability as drivers in market competition. Their underdeveloped internal organisational culture and structure – with issues like financial and human resources – limit efforts related to security (Lavallée and Robillard 2015). There is, therefore, a need to ensure producers that may become more critical in certain circumstances embrace security by design.

It is important to underline that producers are not only IT companies. Various sectors, such as finance, health, automobiles and energy, are becoming digitalised and initiating their own digital services. Public institutions and local municipalities are also developing their own e-services – many of which have proven essential in times of crisis like that of COVID-19.

4.2. Regulations and Standards

Greater application of standards and regulatory action are also ways of enhancing the implementation of best practices. Standards related to software and device security confirm the relevance of the practices discussed in this section – yet they often do not match entirely. The Secure Software Development Framework by the US National Institute of Standards and Technology (NIST) (Dodson, Souppaya and Scarfone 2020) incorporates these practices under the framing of well-secured software and responses to vulnerabilities, which are elaborated in greater detail and with emphasis on organisational processes. In the manufacturing of hardware, software and firmware for products used in industrial systems, the discussed practices match the SDL requirements of the IEC 62443-4 standard (IEC 2019): secure implementation and coding, verification and validation, patch management and product EoL. To minimise the risk from the misuse of IoT devices, such as in botnets, the ETSI 303 645 standard (ETSI 2020) matches the discussed practices by defining baseline requirements for IoT devices: managing reports of vulnerabilities, software validation and maintenance, and security by default elements. However, it fails to directly reference threat modelling and TPC review.

Emerging regulatory frameworks also reflect on the discussed practices directly. The IoT Cybersecurity Labelling Scheme of Singapore (CSA 2020) incorporates the baseline requirements (in Tier 1) of the ETSI 303 645 standard and strengthens them with requirements (in Tier 2) for threat modelling based on the Infocom Media Development Authority of Singapore IoT Cyber Security Guide (IMDA 2020, 7) and (in Tier 3 and 4) for software testing on common errors and known TPC vulnerabilities, lists of all software components, and penetration testing (CSA 2020, 11). According to the Cybersecurity Act (EU 2019, Art. 54–55), the EU cybersecurity certification scheme shall include vulnerability disclosure policies, contact points, and a public list of advisories. A broad range of requirements within the EU candidate certification scheme for cloud services focuses on the security of organisation and processes but will also include supply chain security, secure development environments, identification of vulnerabilities, directory and risk assessment of suppliers, controlling and monitoring third parties, and incident management (ENISA 2020, 132–144). In terms of critical sectors, the lead principles and practices for medical device cybersecurity by the International Medical Device Regulators Forum (IMDRF 2020) clearly match the main discussed practices, including threat modelling, security testing, software BoM, vulnerability disclosure, scoring, patching and support (even for legacy medical devices); the principles also add security requirements, architecture design and information sharing.

4.3. From Good Practices to Common Baseline Security Requirements

Good practices form a useful guide on how to approach security by design. Many producers, however – particularly those with limited resources and awareness – may lack incentives to invest in security by design or find it difficult to implement good practices and existing standards. To make a broader range of industries aware of and ready to embrace security by design, good practices should be used to shape the regulatory environment and assist producers in embracing the basics first.

Developing a global framework with baseline security requirements that are 'common for all digital suppliers and define the fundamentals that a supplier must address in order to ensure the cybersecurity foundations for their product/service' (Charter of Trust 2020a, 2) would be important in supporting the implementation of related norms and principles. Such baselines would also assist regulators in developing an environment based on corporate practice that is harmonised across jurisdictions.

Common baseline requirements need to account for several elements:

- Good corporate practices and requirements (e.g. by Charter of Trust (2020b));
- Regulatory instruments and requirements (e.g. labelling and certification schemes);
- Guidelines and principles of multilateral and multi-stakeholder organisations and fora (e.g. the work of the OECD and the Paris Call);
- International standards related to the security of digital products and services (e.g. International Organization for Standardization);
- Global agreements, norms and principles (e.g. GGE).

The Geneva Dialogue output document suggests that 'as the first step, a small set of very limited and universally applicable prescriptive requirements are defined'

(Radunović and Grätz 2020, 22). Particular models and challenges in developing and implementing baseline requirements should be further studied.

5. CONCLUSION

Sophisticated threat actors challenge the stability of cyberspace by exploiting vulnerabilities in digital products and services. At the level of the UN, states have endorsed norms agreed upon by the GGE in 2015. Some of these norms address the security of digital products and services. Several multi-stakeholder initiatives, such as the GCSC and the Paris Call, have also advanced principles and proposed norms on this issue. The review of norms and principles related to reducing vulnerabilities provided in this paper emphasises the important role producers have in their implementation. The industry may increasingly take on this role due to increasing public expectations about their accountability, as well as growing market incentives.

This paper presents the common understanding achieved by some leading global companies developed within the framework of the Geneva Dialogue on key concepts related to the security of products and services, such as security by design, security development lifecycle and trustworthiness. Further elaboration on good corporate practices, collected and systematised through this dialogue, distinguishes the main components of security by design: threat modelling, supply chain and third-party security, secure development and deployment, vulnerability processes and support, and changes in the corporate mindset and internal processes. A clear match with the requirements set in the related standards and regulatory frameworks confirms their applicability.

Such good practices directly contribute to the implementation of the discussed norms, and thus to global cyber stability – though further study on quantifying this effect is necessary. This paper warns, however, of the urgency to ensure all other producers embrace security by design, particularly those whose services may become more critical to society in times of crisis like that of COVID-19, as well as those whose products play an important role within global supply chains. It suggests the development of common baseline requirements to support the uniform implementation of good practices, assist a broader range of producers (especially those with limited resources), and support practice-driven and globally harmonised regulatory environments. Developing common baseline requirements should consider existing good corporate practices, regulatory instruments, global guidelines, norms and principles, and international standards. Further study of particular models and the challenges of developing and implementing such baseline requirements is suggested.

REFERENCES

Airike, Peppi-Emilia, Julia P. Rotter, and Cecilia Mark-Herbert. 2016. ‘Corporate Motives for Multi-Stakeholder Collaboration – Corporate Social Responsibility in the Electronics Supply Chains’. *Journal of Cleaner Production* 131 (September): 639–48. https://doi.org/10.1016/j.jclepro.2016.04.121.

Anderson, Ross. 2001. ‘Why Information Security Is Hard – an Economic Perspective’. In *Seventeenth Annual Computer Security Applications Conference*, 358–65. Washington, DC: IEEE Computer Society. https://doi.org/10.1109/ACSAC.2001.991552.

Badampudi, Deepika, Claes Wohlin, and Kai Petersen. 2016. ‘Software Component Decision-Making: In-House, OSS, COTS or Outsourcing – A Systematic Literature Review’. *Journal of Systems and Software* 121 (November): 105–124. https://doi.org/10.1016/j.jss.2016.07.027.

Buchheit, Marcellus, Mark Hermeling, Frederick Hirsch, Bob Martin, and Simon Rix. 2020. ‘Software Trustworthiness Best Practices’. An Industrial Internet Consortium White Paper. Industrial Internet Consortium. https://www.iiconsortium.org/pdf/Software_Trustworthiness_Best_Practices_Whitepaper_2020_03_23.pdf.

Charter of Trust. 2018. ‘Charter of Trust: Our 10 Principles’. Charter of Trust. 2018. https://www.charteroftrust.com/about/.

Charter of Trust. 2020a. ‘Common Risk-Based Approach for the Digital Supply Chain’. CoT Principle 2-Report 1. Charter of Trust. https://www.charteroftrust.com/wp-content/uploads/2020/02/20-02-11-CoT-P2-phase-1-report.pdf.

Charter of Trust. 2020b. ‘Achieving Security by Default for Products, Functionalities, and Technologies - Baseline Requirements’. CoT Principle 3-Phase 1. https://www.charteroftrust.com/wp-content/uploads/2020/05/200212-P3-Phase-1-Baseline-Requirements_FINAL.pdf.

Cisco. n.d. ‘What Is Threat Modeling?’ Accessed 6 January 2021. https://www.cisco.com/c/en/us/products/security/what-is-threat-modeling.html.

CrowdStrike Intelligence Team. 2021. ‘SUNSPOT Malware: A Technical Analysis’. *CrowdStrike Blog*, 11 January 2021. https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/.

Cyber Security Agency of Singapore [CSA]. 2020. ‘Cybersecurity Labelling Scheme’. https://www.csa.gov.sg/-/media/csa/documents/cls/cls-pub-2--scheme-specifications-v1.pdf.

Cybersecurity & Infrastructure Security Agency [CISA]. 2020. ‘Alert (AA20-352A): Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations’. 17 December 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-352a.

Dodson, Donna, Murugiah Souppaya, and Karen Scarfone. 2020. ‘Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)’. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04232020.

Dougherty, Chad R., Kirk Sayre, Robert Seacord, David Svoboda, and Kazuya Togashi. 2018. ‘Secure Design Patterns’. Software Engineering Institute, Carnegie-Mellon University Pittsburgh. https://doi.org/10.1184/R1/6583640.V1.

Eggenschwiler, Jaqueline. 2018. ‘Geneva Dialogue on Responsible Behaviour in Cyberspace: Private Sector (Framework Document)’. Geneva Dialogue on Responsible Behaviour in Cyberspace. Zurich, Switzerland: ETH Zurich. https://genevadialogue.ch/wp-content/uploads/Geneva-Dialogue-Role-of-the-Private-Sector.pdf.

European Telecommunications Standards Institute [ETSI]. 2020. ‘ETSI Releases World-Leading Consumer IoT Security Standard’. 2020. https://www.etsi.org/newsroom/press-releases/1789-2020-06-etsi-releases-world-leading-consumer-iot-security-standard.

European Union [EU]. 2019. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). *Official Journal* L151 (7 June 2019): 15–69. https://eur-lex.europa.eu/eli/reg/2019/881/oj.

European Union Agency for Cybersecurity [ENISA]. 2020. 'EUCS – Cloud Services Scheme'. Report/Study. 20 December 2020. https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme.

Fairbank, Nancy. 2019. 'The state of Microsoft?: the role of corporations in international norm creation'. *Journal of Cyber Policy* 4, no. 3: 380–403.

Finnemore, Martha, and Duncan B. Hollis. 2016. 'Constructing Norms for Global Cybersecurity'. *American Journal of International Law* 110, no. 3: 425–479.

Global Commission on the Stability of Cyberspace [GCSC]. 2019. 'Advancing Cyberstability: Final Report'. Global Commission on the Stability of Cyberspace (GCSC). https://cyberstability.org/wp-content/uploads/2020/02/GCSC-Advancing-Cyberstability.pdf.

Greenberg, Andy. 2018. 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History'. *Wired* (22 August 2018). https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Grottola, Stefania Pia. 2020. 'Proliferation of Cyber Norms: the Limitations of Traditional Diplomacy in Discussing Cyberconflict'. Conference paper for the 15th Annual GigaNet Symposium, 2 November 2020.

Group of Governmental Experts [GGE]. 2015. 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security'. 22 July 2015. https://undocs.org/A/70/174.

Hathaway, Melissa E., and John E. Savage. 2012. 'Stewardship of Cyberspace: Duties for Internet Service Providers'. Canada Centre for Global Security Studies, Munk School of Global Affairs, University of Toronto. https://www.belfercenter.org/sites/default/files/files/publication/cyberdialogue2012_hathaway-savage.pdf.

Hathaway, Melissa. 2019. 'Patching Our Digital Future Is Unsustainable and Dangerous'. *CIGI Papers*, 219. https://www.cigionline.org/sites/default/files/documents/Paper%20no.219web.pdf.

Householder, Allen D., Garret Wassermann, Art Manion, and Chris King. 2017. 'The CERT Guide to Coordinated Vulnerability Disclosure'. CMU/SEI-2017-SR-022. Software Engineering Institute, Carnegie Mellon University. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330.

Hurel, Louise Marie, and Luisa Cruz Lobato. 2018. 'Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs'. *Journal of Cyber Policy* 3, no. 1: 61–76. https://doi.org/10.1080/23738871.2018.1467942.

Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. 2011. 'Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains'. *Leading Issues in Information Warfare & Security Research* 1 (2011): 80, edited by Julie Ryan, 80–106. Reading: Academic Publishing International Limited.

Infocom Media Development Authority of Singapore [IMDA]. 2020. 'Internet of Things (IoT)Cyber Security Guide'. https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/ICT-Standards/Telecommunication-Standards/Reference-Spec/IMDA-IoT-Cyber-Security-Guide.pdf?la=en.

International Electrotechnical Commission [IEC]. 2019. 'IEC 62443-4-2:2019'. 2019. https://webstore.iec.ch/publication/34421.

International Medical Device Regulators Forum [IMDRF]. 2020. 'Principles and Practices for Medical Device Cybersecurity'. IMDRF/CYBER WG/N60FINAL:2020. http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf.

International Organization for Standardization [ISO]. 2014. ‘ISO/IEC 29147:2014’. ISO. 2014. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/04/51/45170.html.

Iswaran, S. 2020. ‘Opening Speech by Mr S Iswaran, Minister for Communications and Information, Minister-in-Charge of Cybersecurity, at the ASEAN Ministerial Conference on Cybersecurity 2020’. 7 October 2020. https://www.csa.gov.sg/news/speeches/asean-ministerial-conference-on-cybersecurity-2020.

Kaufmann, Christine. 2016. ‘Multistakeholder Participation in Cyberspace’. *Swiss Review of International and European Law* 26, no. 2: 217–234.

Klimburg, Alexander, and Virgilio A. F. Almeida. 2019. ‘Cyber Peace and Cyber Stability: Taking the Norm Road to Stability’. *IEEE Internet Computing* 23, no. 4: 61–66. https://doi.org/10.1109/MIC.2019.2926847.

Kol, Moshe, and Shlomi Oberman. 2020. ‘Ripple20: CVE-2020-11896 RCECVE-2020-11898 Info Leak’. Technical Whitepaper. Ripple20. JSOF. https://www.jsof-tech.com/wp-content/uploads/2020/06/JSOF_Ripple20_Technical_Whitepaper_June20.pdf.

Lavallée, Mathieu, and Pierre N. Robillard. 2015. ‘Why Good Developers Write Bad Code: An Observational Case Study of the Impacts of Organizational Factors on Software Quality’. In *2015 IEEE/ACM 37th IEEE International Conference on Software Engineering* 1, 677–87. https://doi.org/10.1109/ICSE.2015.83.

Matwyshyn, Andrea M. 2010. ‘Hidden Engines of Destruction: The Reasonable Expectation of Code Safety and the Duty to Warn in Digital Products’. *Florida Law Review* 62, no. 1: 109–58.

Maxwell, Paul, and Robert Barnsby. 2019. ‘Insecure at any bit rate: why Ralph Nader is the true OG of the software design industry’. *Journal of Cyber Policy* 4, no. 3: 346–361.

McKinsey & Company. 2020. ‘How COVID-19 Has Pushed Companies over the Technology Tipping Point—and Transformed Business Forever’. McKinsey & Company. https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever.

Microsoft. n.d. ‘Microsoft Security Development Lifecycle Threat Modelling’. Accessed 6 January 2021. https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling.

MITRE. n.d. ‘MITRE ATT&CK’. Accessed 6 January 2021. https://attack.mitre.org/matrices/enterprise/.

Mladenović, Dragan, and Vladimir Radunović. 2018. ‘Defining Offensive Cyber Capabilities’. *Briefing and Memos from the Research Advisory Group, The Hague Centre for Strategic Studies*, GCSC Issue Brief 2 (Memo 4): 91–134. https://cyberstability.org/wp-content/uploads/2018/06/GCSC-Research-Advisory-Group-Issue-Brief-2-Bratislava.pdf.

NIS Cooperation Group. 2019. ‘EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks’. ENISA. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132.

Organisation for Economic Co-operation and Development [OECD]. 2020. ‘E-Commerce in the Time of COVID-19’. OECD. https://read.oecd-ilibrary.org/view/?ref=137_137212-t0fjgnerdb&title=E-commerce-in-the-time-of-COVID-19.

Organisation for Economic Co-operation and Development [OECD]. 2021. ‘Understanding the digital security of products: An in-depth analysis’. OECD Digital Economy Papers, No. 305, OECD Publishing, Paris, https://doi.org/10.1787/abea0b69-en.

Paris Call for Trust and Security in Cyberspace [Paris Call]. 2018. ‘Paris Call: The 9 Principles’. 11 December 2018. https://pariscall.international/en/principles.

Passoth, Jan-Hendrik, Birgit Peuker, and Michael Schillmeier. 2012. ‘Introduction’. In *Agency without Actors?* New Approaches to Collective Action, edited by Jan-Hendrik Passoth, Birgit Peuker, and Michael Schillmeier, 1–11. London: Routledge.

Radunović, Vladimir, and Jonas Grätz. 2020. 'Security of Digital Products and Services: Reducing Vulnerabilities and Secure Design (Industry Good Practices)'. Geneva Dialogue on Responsible Behaviour in Cyberspace. Geneva, Switzerland: DiploFoundation. https://genevadialogue.ch/goodpractices/.

Rizmal, Irina, and Vladimir Radunović. 2019. 'Baseline Study'. Geneva Dialogue for Responsible Behaviour in Cyberspace. Geneva, Switzerland. https://genevadialogue.ch/wp-content/uploads/Geneva-Dialogue-Baseline-Study.pdf.

Ross, Ron, Michael McEvilley, and Janet Carrier Oren. 2016. 'Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems'. NIST SP 800-160. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160.

Santos, Daniel dos, Stanislav Dashevskyi, Jos Wetzels, and Amine Amri. 2020. 'Amnesia:33'. Forescout. https://www.forescout.com/company/resources/amnesia33-how-tcp-ip-stacks-breed-critical-vulnerabilities-in-iot-ot-and-it-devices/.

Santos, Joanna C. S., Katy Tarrit, and Mehdi Mirakhorli. 2017. 'A Catalog of Security Architecture Weaknesses'. In *2017 IEEE International Conference on Software Architecture Workshops (ICSAW)*, 220–223. Gothenburg, Sweden: IEEE. https://doi.org/10.1109/ICSAW.2017.25.

SolarWinds. 2020. Current Report, United States Securities and Exchange Commission. 14 December 2020. https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm.

United Kingdom Government [UK]. 2019. 'UK Telecoms Supply Chain Review Report'. UK Government, Department for Digital, Culture, Media & Sport. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf.

United Kingdom National Cyber Security Centre [UK NCSC]. 2018. 'Russian Military "Almost Certainly" Responsible for Destructive 2017 Cyber Attack'. 14 February 2018. https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack.

United Nations General Assembly [UN GA]. 2020. 'Developments in the field of information and telecommunications in the context of international security'. Accessed 23 March 2021. https://undocs.org/en/A/RES/75/240.

United Nations General Assembly [UN GA]. 2021. 'Open-ended working group on developments
in the field of information and telecommunications in the context of international security
Final Substantive Report'. Accessed 23 March 2021. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

United Nations Office for Disarmament Affairs [UNODA]. 2021. 'Group of Governmental Experts'. Accessed 8 March 2021. https://www.un.org/disarmament/group-of-governmental-experts/.

Uren, Thomas, Bart Hogeveen, and Fergus Hanson. 2018. 'Defining Offensive Cyber Capabilities'. *Briefing and Memos from the Research Advisory Group, The Hague Centre for Strategic Studies* GCSC Issue Brief 2 (Memo 3): 73–90. https://cyberstability.org/wp-content/uploads/2018/06/GCSC-Research-Advisory-Group-Issue-Brief-2-Bratislava.pdf.

White House. 2018. 'Statement from the White House Press Secretary'. U.S. Embassy & Consulates in Russia. 16 February 2018. https://ru.usembassy.gov/statement-white-house-press-secretary-021518/.