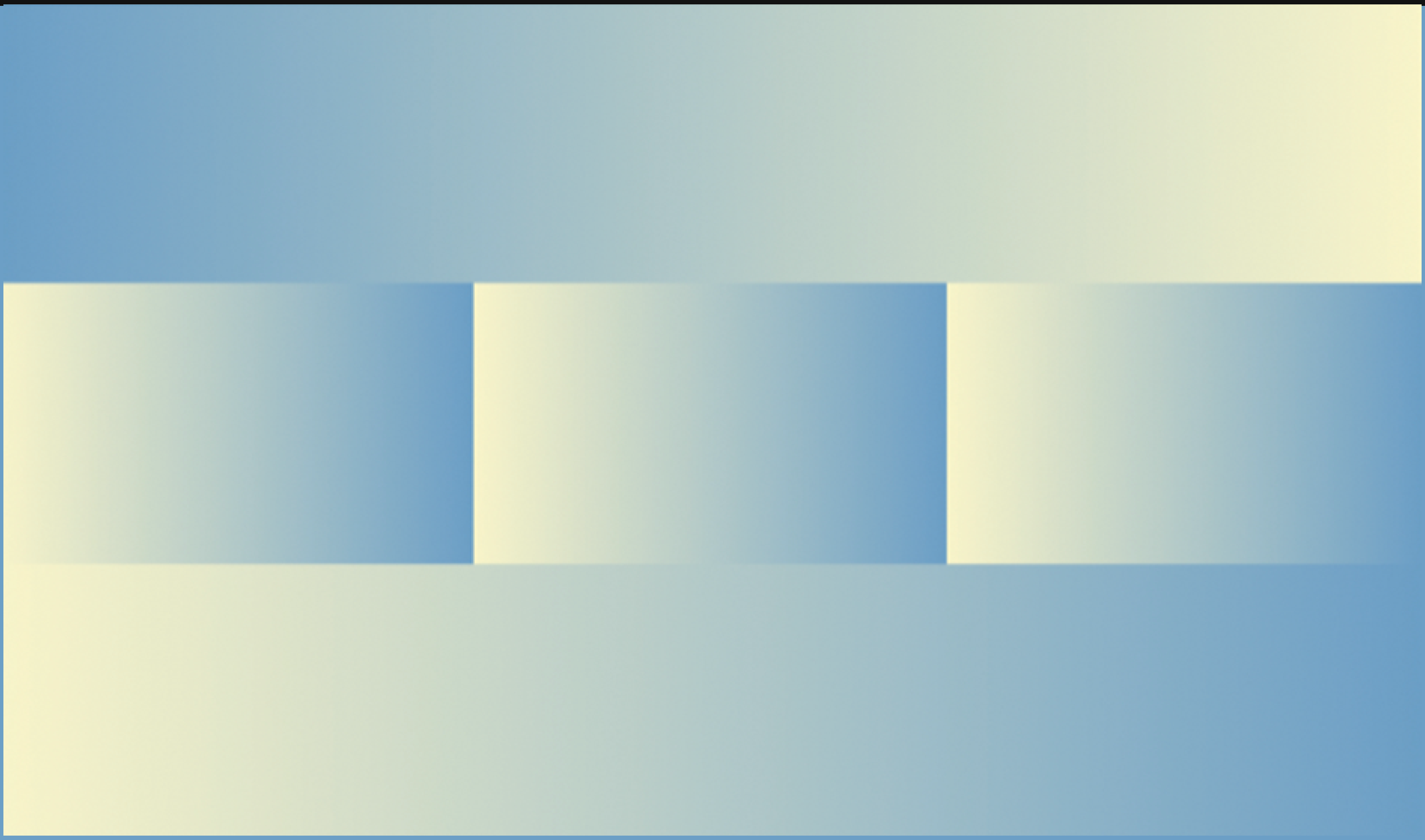


STUDY

Vulnerability Disclosure: Guiding Governments from Norm to Action

How to Implement Norm J of the United Nations Norms of Responsible State Behaviour in Cyberspace

Dr. Sven Herpig

Dec 3rd, 2024

Tech analysis and policy ideas for Europe

interface

Acknowledgments

This analysis was supported by the Transatlantic Cyber Forum working group on “Responsible Vulnerability Disclosure and Mitigation Sharing” through online collaboration and a joint workshop in Berlin. The views and opinions expressed in this paper are those of the author and do not necessarily reflect the official policy or position of the working group members or that of their respective employer(s). In alphabetical order, the author acknowledges the essential contributions of the following individuals:

1. Eugenio Benincasa, Center for Security Studies at ETH Zurich
2. Gregor Bransky, Innovationsverbund Öffentliche Gesundheit
3. Betsy Cooper, Aspen Institute
4. Anastasiya Kazakova, DiploFoundation
5. Carolin Kemper, German Research Institute for Public Administration
6. Adam I. Klein, The University of Texas at Austin
7. Susan Landau, Tufts University
8. Klaus Landefeld, eco - Association of the Internet Industry
9. Thomas Lawson
10. Eugenia Lostri, Lawfare Institute
11. Alexandra Paulus, German Institute for International and Security Affairs
12. Pavlina Pavlova, New America
13. Riana Pfefferkorn, Stanford University
14. Thomas Reinhold, Peace Research Institute Frankfurt
15. Christine Runnegar, Internet Society
16. Thomas Schreck, Munich University of Applied Sciences
17. Aleksandra Sowa, German Informatics Society, PET
18. Rob Spiger, Microsoft Corporation
19. Tara Tarakiyee, Sovereign Tech Fund
20. Tassilo Thieme, Federal Office for Information Security (BSI)
21. Eric MSP Veith, Carl von Ossietzky University Oldenburg
22. Julian-Ferdinand Vögele, Recorded Future
23. Arlena Wellßow, Carl von Ossietzky University Oldenburg
24. Paul Zenker

The author extends special gratitude to Christina Rupp for her support throughout the project, from the initial idea to the fine-tuning of analysis and recommendations. Thanks to Alexandra Paulus for introducing the author to the UN norms of responsible state behavior in cyberspace. The author also thanks Frederic Dutke and Karen Schmiady for their help in implementing the workshop, as well as Luisa Seeling, Alina Siebert, Scribendi Editor EM1310, and ChatGPT for their assistance with editing and layouting this publication.

This project was made possible by the generous support of the *German Federal Foreign Office*. The views expressed in this paper do not necessarily represent the official position of the ministry.

Table of Contents

Executive Summary

As society's expectations of IT systems have increased, the underlying IT infrastructures have grown increasingly complex.[1] That complexity is inevitably accompanied by errors, which can be exploited. The persistent challenge of those errors, or vulnerabilities, in IT infrastructure, which span medical implants to vehicles, poses significant risks due to potential exploitation by criminals, adversarial intelligence agencies, and militaries.

Vulnerability disclosure, "a process through which vendors and vulnerability finders may work cooperatively in finding solutions that reduce the risks associated with a vulnerability,"[2] has emerged as a key process to fix these errors – ideally before they can be exploited. This process may involve multiple parties, including security researchers, coordinators, code owners, and system owners working together. Instances where all relevant stakeholders work together to reduce the risks associated with a vulnerability through disclosure are referred to as Coordinated Vulnerability Disclosure (CVD). The theoretical and practical aspects of Coordinated Vulnerability Disclosure are well established, offering a robust framework for mitigating risks associated with vulnerabilities.

Governments have acknowledged that they themselves play a crucial role in fostering a policy ecosystem conducive to Coordinated Vulnerability Disclosure. In 2015, the United Nations (UN) Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security agreed upon a norm to, inter alia, "encourage responsible reporting of ICT vulnerabilities" as part of their final report. The consensus report was subsequently endorsed by all member states of the United Nations General Assembly.[3]

While this norm, among others, has been agreed on, its implementation needs to be advanced through concrete guidance. Implementation refers to "adjusting or establishing policies, procedures, regulations or capabilities or adopting other measures which support state and national adherence to the projected conditions of the recommendations for norms."[4] This has recently been emphasized again by several governments calling for an improved exchange, in-depth discussions

[1] Herbert Lin (2018): CLTC Seminar "Complexity and Security: Managing the Tradeoffs"

[2] ISO (2024): ISO/IEC TR 5895:2022 – Information technology —– Security techniques —– Vulnerability disclosure

[3] United Nations (2015): Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174)

[4] Mika Kerttunen and Eneken Tikk (2021): PUTTING CYBER NORMS IN PRACTICE: Implementing the UN GGE 2015 recommendations through national strategies and policies

and collaborative initiatives on vulnerability disclosure, and the vulnerability disclosure norm more specifically.[5] **This policy paper therefore seeks to bridge the gap between the abstract formulation of the United Nations norm on vulnerability disclosure and its implementation in practice. It offers concrete, actionable guidance on how states – key stakeholders and enablers of vulnerability disclosure – can achieve compliance.**

> As a **baseline**, governments should
> **I. Designate a Point of Contact and Coordinator;**
> **II. Implement a Government Vulnerability Disclosure Policy;**
> **III. Create Legal Protection and Certainty;**
> **IV. Drive Security Contact and Disclosure Practice Implementation;**
> **V. Offer Guidance and Services.**
>
> As **enhanced** implementation, governments could
> **VI. Implement a Government Disclosure Decision Process;**
> **VII. Foster Government Vulnerability Reward Programs;**
> **VIII. Drive Mitigation Sharing;**
> **IX. Improve Vulnerability Information Sharing;**
> **X. Socialize the Norm Internally;**
> **XI. Not Introduce Vulnerabilities or Prohibit Their Reporting.**
>
> As **advanced** measures, governments could
> **XII. Support Unmaintained Code;**
> **XIII. Internationalize and Specialize Government Coordinators;**
> **XIV. Cooperate and Build Capabilities;**
> **XV. Name and Shame Non-Compliance;**
> **XVI. Curb Vulnerability Trading.**

By implementing and refining the relevant national capabilities, and subsequently engaging in respective international cooperation, governments can significantly bolster national cybersecurity. This proactive approach not only mitigates risks but also fosters trust and cooperation among nations in handling cybersecurity threats.

[5] Ghanaian Representative (2023): (4th meeting) Open-ended working group on Information and Communication Technology (ICT) - Fourth Substantive Session and Malaysian Representative (2023): (2nd meeting) Open-ended working group on Information and Communication Technology (ICT) - Fourth Substantive Session and Swiss Representative (2023): (2nd meeting) Open-ended working group on Information and Communication Technology (ICT) - Fourth Substantive Session

1. Introduction

As society relies increasingly on IT infrastructure, the persistent challenge of vulnerabilities[6] – the "Holy Grail for Hackers"[7] – remains critical,[8] particularly since "state and non-state actors exploit digital vulnerabilities to advance their agendas, disrupting digital peace and undermining trust among nations."[9] With IT integration extending from medical implants to vehicles and the rise of machine learning-enabled systems, these challenges intensify in scope and complexity, as well as risk, engendered by the introduction of cyber physical systems. Threat actors, such as criminals, adversarial intelligence agencies, and militaries are poised to exploit vulnerabilities, underscoring the urgent need for robust cybersecurity policies that enable the mitigation of risk stemming from vulnerabilities. Effective vulnerability disclosure is thus a key aspect of digital security.[10]

One central challenge in vulnerability disclosure is the process of doing so in a coordinated way,[11] which enables **system owners to be aware of the new risk and mitigate it before it can be exploited.** The debate around how to do this correctly and responsibly has been ongoing for decades,[12] with the process ultimately being **dubbed a "wicked problem."**[13] The process is inherently complex, often involving multiple parties with diverse roles (e.g., finders, coordinators, code owners), agendas (e.g., fame, legal requirements), and incentives (e.g., rewards, fines). Success in this area requires substantial trust, clear communication, and robust coordination among stakeholders. Consequently, "the practice of Coordinated

[6] According to the NTIA Awareness and Adoption Group (2016): Vulnerability Disclosure Attitudes and Actions, "vulnerabilities are weaknesses of software, hardware, or online services that can be used to damage the confidentiality, integrity, or availability of those systems or the data they store."

[7] Dina Temple-Raston (2023): 101. Bug bounties with Chinese characteristics

[8] Acknowledging that "stolen credentials and compromised accounts" are still the number one attack vector for successful breaches, especially when it comes to efficiency. See, for example, Patrick Gray and Adam Boileau (2024): Risky Business #764 – Mossad expands into telecommunications services

[9] German Representative (2024): (3rd meeting) Open-ended working group on Information and Communication Technology (ICT) - Seventh Substantive Session

[10] Hacking Policy Council (2024): Transformative changes needed for vulnerability infrastructure and the National Vulnerability Database and ETSI (2022): Cyber Security; Guide to Coordinated Vulnerability Disclosure

[11] ETSI (2022): Cyber Security; Guide to Coordinated Vulnerability Disclosure

[12] Stephen Shepherd (2003): How do we define Responsible Disclosure? and Ashish Arora, Anand Nandkumar, and Rahul Telang (2006): Does information security attack frequency increase with vulnerability disclosure? An empirical analysis

[13] For example, Allen D. Householder, Garret Wassermann, Art Manion, and Chris King (2017): The CERT® Guide to Coordinated Vulnerability Disclosure

Vulnerability Disclosure (CVD)[14] emerged as a response to the persistent fact of vulnerable software."[15]

Security researchers, Computer Emergency Response Teams (CERTs), code owners (e.g., developers, vendors), and system owners (e.g., operators) have made significant progress in both the theoretical and practical aspects of vulnerability disclosure.[16] While the progress in improving overall disclosure outcomes is a step in the right direction, especially given the rise in reported vulnerabilities,[17] individual disclosures continue to face significant challenges. These challenges are largely attributable to factors that cannot be addressed solely through international standards and process flow diagrams, such as communication breakdowns, legal uncertainty, and lack of trust between involved parties. These issues originate from the complexities associated with the human element and relevant vulnerability policy ecosystems. Refining these policy ecosystems is the responsibility of governments. As the **Organization for Economic Cooperation and Development (OECD)** has observed, "[governments] have a key role to play. They can help change mindsets about vulnerabilities, and encourage vulnerability owners to take responsibility. They can also help change how security researchers are perceived, and raise awareness about their contribution to our collective security and privacy."[18]

Therefore, it is of pivotal importance to remind governments of their commitment stemming from the 2015 report to **"encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to**

[14] This paper will use the term "Coordinated Vulnerability Disclosure (CVD)" instead of the term "responsible vulnerability disclosure" as outlined in Allen D. Householder, Garret Wassermann, Art Manion, and Chris King (2017): The CERT® Guide to Coordinated Vulnerability Disclosure and ERNW (2015): ERNW Newsletter – Reflections on Vulnerability Disclosure and a Case Study and Google (2021): Guide to implementing a coordinated vulnerability disclosure process for open source projects

[15] Allen Householder and Jonathan Spring (2021): A State-Based Model for Multi-Party Coordinated Vulnerability Disclosure (MPCVD)

[16] For example, rain forest puppy (2000), Full Disclosure Policy (RFPolicy) and Chris Wysopal and Steve Christey (2002): Responsible Vulnerability Disclosure Process draft-christey-wysopal-vuln-disclosure-00.txt and Allen D. Householder, Garret Wassermann, Art Manion, and Chris King (2017): The CERT® Guide to Coordinated Vulnerability Disclosure and FIRST (2020): Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure and Google (2021): Guide to implementing a coordinated vulnerability disclosure process for open source projects and ETSI (2022): Cyber Security; Guide to Coordinated Vulnerability Disclosure and Organisation for Economic Co-operation and Development (2023): Good Practice Guidance on the Co-ordination of Digital Security Vulnerabilities and ISO (2024): ISO/IEC 29147:2018 – Information technology — Security techniques — Vulnerability disclosure

[17] statista (2024): Number of common IT security vulnerabilities and exposures (CVEs) worldwide from 2009 to 2024 YTD

[18] Organisation for Economic Co-operation and Development (2021): Encouraging Vulnerability Treatment – Overview for policy makers

such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.”[19] This norm – *norm j*, going forward referred to as the *vulnerability disclosure norm* – forms part of the 11 norms for responsible state behavior in cyberspace adopted by the United Nations Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security (UN GGE).[20] The respective report of the United Nations Group of Governmental Experts – which has included, inter alia, representatives of **Germany, Israel,** the **People’s Republic of China,** the **Russian Federation,** the **United Kingdom,** and the **United States** among its 20 members – was submitted to and later endorsed by all United Nations (UN) member states via the United Nations General Assembly[21]. **United Nations member states** have since continued to confirm the acquis – including the 11 norms for responsible state behavior in cyberspace – for example, in the context of the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025 (UN OEWG).[22] Adherence to the voluntary norms can enable governments to enhance their cyber resilience, bolster international credibility, influence the establishment of global standards, and mitigate the risks of unnecessary tensions and inadvertent conflicts by increasing the predictability of state conduct, and complement or facilitate other cyber diplomacy instruments like public attributions or sanctions.[23]

[19] United Nations (2015): Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174)

[20] United Nations (2015): Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174)

[21] United Nations (2015): Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174)

[22] United Nations (2021): Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135) and United Nations (2021): Open-ended working group on developments in the field of information and telecommunications in the context of international security (A/AC.290/2021/CRP.2) and United Nations (2024): Developments in the field of information and telecommunications in the context of international security (A/79/214)

[23] Bart Hogeveen (2022): The UN norms of responsible state behaviour in cyberspace Guidance on implementation for Member States of ASEAN and Alexandra Paulus (2024): Building Bridges in Cyber Diplomacy. How Brazil Shaped Global Cyber Norms.

Agreeing to abstract norms at the United Nations level is a first step but it is far harder for governments to implement those norms within their jurisdictions through concrete actions. In the case of the vulnerability disclosure norm, it means achieving agreement on the minutia of a vulnerability disclosure. To support governments that aim to implement the coordinated disclosure norm through concrete actions, this paper:

1. distills an actionable reading of the vulnerability disclosure norm from high-level guidance and debates, as well as from practice and practical implications in chapter 2;
2. defines and describes the Coordinated Vulnerability Disclosure process as implementation of the norm in chapter 3;
3. recommends specific actions on how states can create and foster a policy ecosystem that enables the implementation of Coordinated Vulnerability Disclosure in chapter 4;
4. describes through which channels states can share the progress of their implementation efforts in chapter 5.

Based on the recommended actions, a checklist will be introduced in ANNEX A to monitor progress in norm implementation and identify subsequent steps for facilitating ongoing improvement in implementing the norm. ANNEX B traces the United Nations vulnerability disclosure norm implementation perspectives in recent years.

2. Vulnerability Disclosure Norm[24]

United Nations member states have recognized that an important step toward reducing risks stemming from Information and Communication Technologies rests in the responsible reporting of vulnerabilities. Based on these considerations, vulnerability disclosure became one of the 11 agreed norms of responsible state behavior in cyberspace in 2015 (see 2.1 United Nations Norms Guidance). Since then, through debates and contributions, governments and other stakeholders have fostered a more concrete understanding of what implementing that norm could look like in theory (see 2.2 Government and Non-Government Perspectives) and in practice, through actions such as changes to their respective policy ecosystems (see 2.3 Governmental Vulnerability Disclosure Practice and 2.4 Cyber Diplomacy meets Vulnerability Realpolitik). Almost a decade after the vulnerability disclosure norm was agreed on, those debates and actions allow us to have a better understanding of how the norm's abstract wording can be translated into practice (see 2.5 Actionable Reading).

2.1 United Nations Norms Guidance

The United Nations norms of responsible state behavior in cyberspace serve as a mechanism for addressing threats to international peace and security. These norms can be defined as "standards of appropriate behavior with respect to the use of ICT inconsistent with the objectives of maintaining international stability and security."[25] Essentially, these norms encapsulate shared expectations regarding (in)appropriate international state conduct, while remaining voluntary and non-binding. They delineate both desirable activities and positive duties, as well as prohibitions on specific actions.[26]

The underlying norm of responsible state behavior in cyberspace, which asks states to adjust their vulnerability disclosure policies, was articulated by the United Nations Group of Governmental Experts in 2015 as follows:

[24] A special shout-out to my colleague, Christina Rupp, who helped me rewrite and restructure this chapter more than half a dozen times. Your patience is praiseworthy.

[25] Tim Maurer (2019): A Dose of Realism: The Contestation and Policy of Cyber Norms

[26] Alexandra Paulus (2024): Building Bridges in Cyber Diplomacy – How Brazil Shaped Global Cyber Norms

> "(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."[27]

In 2021, a subsequent United Nations Group of Governmental Experts agreed on the following additional high-level guidance for the interpretation of the vulnerability disclosure norm:[28]

> "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 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**[29]**, 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[30] reporting and management of vulnerabilities and the respective roles and

[27] United Nations (2015): Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174)

[28] Highlights by author.

[29] A definition of "impartial legal framework" has been issued neither by the United Nations Groups of Government Experts nor by the Open-Ended Working Group.

[30] A definition of "responsible" in this context has been issued neither by the United Nations Groups of Government Experts nor by the Open-Ended Working Group.

> 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."[31]

In July 2023, United Nations member states requested the Chair of the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025 to compile a norms implementation checklist for consideration by states, including suggestions for several voluntary actions implementing the vulnerability disclosure norm.[32] A year later, in July 2024, United Nations member states decided the checklist "may be viewed as a living document which could continue to be discussed and updated at the forthcoming OEWG sessions."[33] Concrete steps suggested in the checklist include legal protection for security researchers, vulnerability disclosure policies, and a Coordinated Vulnerability Disclosure process. For the latter, guidance on the roles and responsibilities are to be developed and incentivized – including procedural details such as the handling and sharing of sensitive data and technical information. The checklist further lists facilitating international cooperation in several aspects, such as curbing commercial distribution of vulnerabilities and understanding of vulnerability disclosure.

[31] United Nations (2021): Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/153)

[32] United Nations (2023): Developments in the field of information and telecommunications in the context of international security (A/78/265)

[33] United Nations (2024): Developments in the field of information and telecommunications in the context of international security (A/79/214)

2.2 Government and Non-Government Perspectives

Various perspectives have been articulated by governments regarding the interpretation and implementation of the vulnerability disclosure norm, showcasing a diverse array of approaches.[34] Beyond state practices that implicitly touch on how a state implements the vulnerability disclosure norm (see 2.3 Governmental Vulnerability Disclosure Practice) and official statements explicitly linking certain actions to the norm, non-government assessments offer further insights.[35] These external observations provide additional perspectives on state actions – both actual and aspirational – that, according to the respective third party's interpretation, can contribute to implementing the vulnerability disclosure norm.

The following perspectives form a non-exhaustive list of actions that various states and non-government stakeholders directly or indirectly consider part of implementing the vulnerability disclosure norm.[36] The actions are derived from statements and contributions by governments as part of United Nations debates, contributions by states to the United Nations Secretary-General's annual reports on developments in the field of information and telecommunications in the context of international security,[37] governmental activities in the framework of international organizations and third parties such as civil society organizations, industry or academia, addressing or touching upon the vulnerability disclosure norm. The high-level suggestions for implementing the vulnerability disclosure norm can be summarized in thematic clusters as follows (further details can be found in ANNEX B. Perspectives on the United Nations Vulnerability Disclosure Norm).

[34] This has not been done only in the respective fora of the United Nations but also in other multilateral constellations.

[35] Assessment and analysis such as the Anastasiya Kazakova, Vladimir Radunović, Serge Droz (2023): Geneva Manual On Responsible Behaviour in Cyberspace – Implementation of Norms of Responsible Behaviour in Cyberspace by Relevant Non-State Stakeholders are not considered within the third party assessments if they focus on implementation of norms by non-state actors instead of governments.

[36] A more detailed, yet non-exhaustive, tracking of which government or non-government stakeholder has mentioned what implementation action, and where, can be found in B. Perspectives on the United Nations Vulnerability Disclosure Norm.

[37] For instance, for the United Nations (2022): Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies – Report of the Secretary-General (A/77/92), member states were, inter alia, invited "to inform the Secretary-General of their views and assessments on […] (a) efforts taken at the national level to strengthen information security and promote international cooperation in this field [as well as] (b) the content of the concepts mentioned in the report of the Open-ended Working Group and the reports of the Group of Governmental Experts" (similar wording for previous reports). Therefore, these reports also offer states the opportunity to touch upon their norm implementation-related efforts in the context of their contributions.

2.2.1 Coordinated Vulnerability Disclosure

B.1 Coordinated Vulnerability Disclosure is a well-established organizational cybersecurity process to coordinate the disclosure of vulnerabilities in a way that minimizes the risk stemming from those vulnerabilities. A vast number of stakeholders refers to Coordinated Vulnerability Disclosure – sometimes using different wording – as an action to implement the vulnerability disclosure norm. Based on the statements, it can be regarded as a cornerstone of implementing the vulnerability disclosure norm.

Coordinated Vulnerability Disclosure has been mentioned as part of the B. Perspectives on the United Nations Vulnerability Disclosure Norm by **Canada**, **Colombia**, **Czechia**, **France**, **Kuwait**, **Mauritius**, the **Netherlands**, **Pakistan**, **Singapore**, **Switzerland**, and the **United Kingdom,** as well as the **Group of Seven** (G7) and the **Organization for Security and Co-operation in Europe** (OSCE). It has further been mentioned in different contexts by the **Australian Strategic Policy Institute** (ASPI), the authors of a **Global Forum on Cyber Expertise** (GFCE) report, **Global Partners Digital**, the authors of an **ICT4Peace and Leiden University** report, **Kaspersky**, and the **Tech Accord** signatories.

More information on Coordinated Vulnerability Disclosure can be found in 3. Coordinated Vulnerability Disclosure. The corresponding recommended implementation action can be found in II. Government Vulnerability Disclosure Policy and IV. Security Contact and Disclosure Practice.

2.2.2 Equities Process

B.2 Equities Process describes a pre-disclosure policy framework in which various agencies weigh up arguments for and against a delayed vulnerability disclosure. Arguments for delayed disclosure include, for example, that the vulnerable software is coded and maintained by cyber criminals and used only in malicious ransomware operations.[38] Most governments certainly would not want to help cyber criminals improve their tools. While there certainly is healthy skepticism from certain governments and non-government stakeholders toward equities processes, a number of actors regard running an equities process as a core component for implementing the vulnerability disclosure norm.

[38] For a list of equities and a blueprint for a corresponding policy process, see Sven Herpig (2018): Governmental Vulnerability Assessment and Management – Weighing Temporary Retention versus Immediate Disclosure of 0-Day Vulnerabilities

Equities processes have been explicitly mentioned as part of the B. Perspectives on the United Nations Vulnerability Disclosure Norm by **Canada**, **India**, and the **United Kingdom**. **Egypt** and **Pakistan** have expressed criticism toward "stockpiling vulnerabilities", a description used by the opponents of such processes. **Global Partners Digital** and the authors of an **ICT4Peace and Leiden University** report have asked for a robust legal framework and transparency should governments implement such processes.

More information on equities processes, as well as the corresponding recommended implementation action, can be found in VI. Government Disclosure Decision Process.

2.2.3 Guidance

B.3 Guidance consists of various actions that states can take to help other states and non-government stakeholders to implement actions in the area of vulnerability disclosure. This includes, but is not limited to, sharing best practices, templates, and policies, creating online courses and awareness campaigns, or endorsing specific standards.

Guidance has been mentioned as part of the B. Perspectives on the United Nations Vulnerability Disclosure Norm by **Cuba**, **Fiji**, the **Netherlands,** and **Switzerland**. Non-government stakeholders that have mentioned actions related to vulnerability disclosure norm guidance are the **Australian Strategic Policy Institute**, the authors of a **ICT4Peace and Leiden University** report, and the authors of a **Global Forum on Cyber Expertise** report.

More information on guidance, as well as the corresponding recommended implementation action, can be found in V. Guidance and Services.

2.2.4 Information Exchange

B.4 Information Exchange refers to the sharing of technical information on vulnerabilities bilaterally, multilaterally, or regionally. This can take place in an ad hoc manner, through advisories or through vulnerability databases. Information sharing is widely recognized as a key element of the vulnerability disclosure norm and is highlighted by government perspectives and non-government stakeholders.

Information exchange has been mentioned as part of the B. Perspectives on the United Nations Vulnerability Disclosure Norm by **Argentina**, **Brazil**, **Canada**, **Colombia**, **Egypt**, **France**, **Honduras**, **India**, **Kazakhstan**, **Pakistan**, the **Republic of Korea**, and **Türkyie**. **Albania**, **India**, **Kenya**, **Mauritius**, and the **Philippines** have highlighted the possible role of a United Nations-wide database or threat repository containing information on vulnerabilities. As for non-government stakeholders, information exchange has been mentioned by the authors of a **ICT4Peace and Leiden University** report, as well as in a **Global Forum on Cyber Expertise** report. While several stakeholders support the idea of a United Nations-wide database or threat repository, only **Hitachi America** has specifically mentioned that it should facilitate vulnerability information exchange.

More information on information exchange, as well as the corresponding recommended implementation action, can be found in IX. Vulnerability Information Sharing.

2.2.5 Legal Protection

B.5 Legal Protection for those finding and reporting vulnerabilities is considered essential by those affected. It allows security researchers and others to contact the responsible code owner or a third party coordinator, such as a National Computer Security Incident Response Team without facing (the threat of) legal repercussions for simply finding and reporting a vulnerability.

Legal protection has been mentioned as part of the B. Perspectives on the United Nations Vulnerability Disclosure Norm by **Access Now**, the **Association for Progressive Communications**, the **Australian Strategic Policy Institute**, the **Forum of Incident Response and Security Teams** (**FIRST**), **Global Partners Digital,** the authors of a **ICT4Peace** and **Leiden University** report, **Kaspersky**, and **Tech Accord**. While there is a vast range of non-government stakeholders pointing toward legal protection as a key enabling element for implementing the vulnerability disclosure norm, there is a lack of government perspectives on the matter.

More information on legal protection, as well as the corresponding recommended implementation action, can be found in III. Legal Protection and Certainty.

2.2.6 Mitigation Sharing

B.6 Mitigation Sharing for vulnerabilities forms an explicit component of the vulnerability disclosure norm. Therefore, it is not surprising that it is mentioned by both government and non-government stakeholders. However, the perspectives do not address whether such mitigations or remedies should be limited to actual patches or if they should contain temporary fixes before patches also become available.

Mitigation sharing has been mentioned as part of the B. Perspectives on the United Nations Vulnerability Disclosure Norm by **India**, **Mexico**, and **Pakistan**. Furthermore, **Canada** and **France** have shared some of their concrete actions in this area. Similarly, the **Australian Strategic Policy Institute** has shared its observations of concrete steps taken in the Southeast Asia region.

More information on mitigation sharing, as well as the corresponding recommended implementation action, can be found in VIII. Mitigation Sharing.

2.2.7 Harmful Hidden Functions and Proliferation Risks

B7. Harmful Hidden Functions and Proliferation Risks refer to governments abstaining from intentionally integrating, assisting in the integration, or mandating the integration of vulnerabilities in code of information and communication technologies. While this aspect seems to be rather part of a software design or supply chain discussion, it is indirectly tied to vulnerability disclosure. As a second tier effect, governments may require code owners not to reveal information about such functions or even try to (legally) shut down reporters of such vulnerabilities – making it an issue for vulnerability disclosure norm implementation.

Harmful hidden functions and proliferation risks have been mentioned as part of the B. Perspectives on the United Nations Vulnerability Disclosure Norm by the **Bolivarian Republic of Venezuela**, **Cuba**, **Colombia**, the **Democratic People's Republic of Korea**, **France,** the **Islamic Republic of Iran**, **Pakistan**, the **Republic of Belarus**, the **Republic of Nicaragua,** the **Russian Federation**, the **Syrian Arab Republic**, and the **United Kingdom.** The **Global Commission on the Stability of Cyberspace,** as well as **Global Partners Digital** together with the **Association for Progressive Communications,** have mentioned harmful hidden functions. **Egypt** and the **Netherlands** have highlighted the role of proliferation but not remarked on harmful hidden functions. While this issue is not closely related to vulnerability disclosure, it has been pushed by an aligned group of states, as well as individual states and non-government stakeholders, to varying extents. **France** and the **United Kingdom** are two states that seem to have positioned themselves in such a way that they regard the topic as relevant but more as an area of responsibility of the private sector.

More information on harmful hidden functions and proliferation risks, as well as the corresponding recommended implementation action, can be found in XI. No Government-Introduced Vulnerabilities.

2.2.8 Point of Contact

B.8 Point of Contact is a government authority in charge of vulnerability disclosure, such as a National Computer Security Incident Response Team or Computer Emergency Response Team (CERT). Operational tasks can range from coordinating vulnerability disclosure for government agencies to serving as coordinators between security researchers that find vulnerabilities and the stakeholders that are responsible for the vulnerable code.

A point of contact has been mentioned as part of the B. Perspectives on the United Nations Vulnerability Disclosure Norm by **Canada, Türkiye,** and the **Group of Seven,** as well as by the non-government stakeholders **Global Commission on the Stability of Cyberspace**, and the authors of a **ICT4Peace and Leiden University** report. While the government voices remained vaguer as to the actual setup of such a point of contact, the non-government suggestions were more concrete on which government agency should be the point of contact and what it should do.

More information on a point of contact, as well as the corresponding recommended implementation action, can be found in I. Point of Contact and Coordinator.

2.2.9 Reward Programs

B.9 Reward Programs provide positive incentives, in the form of rewards (both monetary and non-financial), to reporters of vulnerabilities that follow the scope and framework of the program. These programs come in slightly different forms, such as hack-the-government programs, bug bounty programs, or government vulnerability reward programs. While bug bounty programs and hack-the-government programs concretely ask for security researchers to find vulnerabilities in certain areas, such as government websites or specific software, government vulnerability reward programs appear more reactively. If someone happens to find a vulnerability in the code that is in the scope of the program, they know that there is a reward waiting if they report it through this program.

Reward programs have been mentioned as part of the B. Perspectives on the United Nations Vulnerability Disclosure Norm by the **Republic of Korea** as well as a range of non-government stakeholders including the **Australian Strategic Policy Institute**, a **Global Forum on Cyber Expertise** report, **Global Partners Digital**, and **Kaspersky**. While reward programs are in line with implementing the vulnerability disclosure norm, as indicated by many non-government stakeholders, they do not appear to be a priority for governments.

More information on reward programs, as well as the corresponding recommended implementation action, can be found in VII. Government Vulnerability Reward Programs.

2.3 Governmental Vulnerability Disclosure in Practice

States influence notions of responsible behavior not only through diplomatic channels and discussions within the United Nations, but also through their conduct. Thus, state practice – actions taken by states both domestically and globally – plays a critical role in shaping how states interpret these norms and influencing which specific behavioral expectations they are being attached to. Based on the assumption that governmental vulnerability disclosure practices at least implicitly reflect ideas about how the state in question considers that vulnerabilities should or should not be disclosed, observing the actions of states permits inferring what activities these countries consider as appropriate or inappropriate on a daily basis.[39]

Against this backdrop, it is worth noting that states have driven numerous changes within their vulnerability policy ecosystems prior to and particularly after the adoption of the vulnerability disclosure norm in 2015. Those changes are not always linked to the norm but they "serve as foundations for implementing the recommendations."[40] Such steps indicate that these policy changes can contribute to the implementation of the vulnerability disclosure norm, even if the connection is not explicitly acknowledged. Additionally, it is highly probable that countries that are actively engaged in implementing the vulnerability disclosure norm base their policies and actions upon the norms without even knowing it. This is because, from what is publicly known, countries rarely map their policies and actions against the norms or consider the norms when developing domestic policies and are even less likely to share their related progress publicly (see 5. Sharing Implementation Efforts).

Particularly since many governments likely lack a comprehensive overview over their own specific norm implementation actions, it is not clear how closely the following actions are tied to governments' intentions of implementing the

[39] Alexandra Paulus (2022): Why Germany should practice the Cyber Norms it preaches: "The case of a Vulnerabilities Equities Process" and Christina Rupp and Alexandra Paulus (2023): Official Public Political Attribution of Cyber Operations – State of Play and Policy Options

[40] Mika Kerttunen and Eneken Tikk (2021): PUTTING CYBER NORMS IN PRACTICE: Implementing the UN GGE 2015 recommendations through national strategies and policies

vulnerability disclosure norm. Despite these caveats, they offer a first overview of the vulnerability disclosure policy ecosystem and related government interventions pursued within the past years and, accordingly, provide insights into what specific practices they consider as contributions to how vulnerabilities should be disclosed.

Some selected examples that help illustrate the development in this policy subfield are:

In the realm of civilian cybersecurity policies, there is considerable variation in the timing and implementation across nations. For instance, since 2012 the **South Korean** cybersecurity agency has incentivized finding and reporting vulnerabilities through rewards by running bug bounty programs. The **Netherlands** launched a civilian Coordinated Vulnerability Disclosure policy in 2013, **Japan** in 2019, the **United States** and **Israel** established similar policies in 2021, and **Germany** followed suit in 2023.[41]

Meanwhile, the **United States** initiated its military Vulnerability Disclosure Program (VDP) in 2016, whereas the **United Kingdom** established its Vulnerability Reporting Service (VRS) in 2018, and **Singapore** its Vulnerability Rewards Program (VRP) in 2018 as well, followed by the **German** armed forces implementing their Vulnerability Disclosure Program in 2020.[42]

Despite these initiatives, both **Germany** and the **United States** have long struggled to make significant progress in providing comprehensive legal protection for good faith security researchers.[43] [44] In the midst of its war against Ukraine, the

[41] Republic of Korea (2020): Implementation of the 2015 UNGGE Norms and Marietje Schaake, Lorenzo Pupillo, Afonso Ferreira, and Gianluca Varisco (2018): Software Vulnerability Disclosure in Europe — Technology, Policies and Legal Challenges and National Cyber Security Centre (2018): Coordinated Vulnerability Disclosure: the Guideline and JPCERT/CC (2019): JPCERT/CC Vulnerability Coordination and Disclosure Policy and Cybersecurity & Infrastructure Security Agency (2021): Vulnerability Disclosure Policy (VDP) Platform and Israel National Cyber Directorate (2021): Vulnerabilities Disclosure Program - CVE ® and Bundesamt für Sicherheit in der Informationstechnik (2023): BSI CVD guideline for security researchers

[42] Ionut Arghire (2024): Pentagon Received Over 50,000 Vulnerability Reports Since 2016 and National Cyber Security Centre (2023): Thanking the vulnerability research community with NCSC Challenge Coins and Natasha Ganesan (2021): Hackers to get monetary rewards as part of GovTech's new vulnerability discovery programme and Bundeswehr (2020): Vulnerability Disclosure Policy der Bundeswehr

[43] The Good Faith Cybersecurity Researchers Coalition (2024): An Analysis of US Hacking Law, with Riana Pfefferkorn and Sven Herpig (2024): Schwachstellen gemeinsam richtig offenlegen and Tagesspiegel Background Cybersecurity (2024): Reform des Hackerparagraphen: Zeitplan weiter unklar

[44] At the time of writing, a political initiative to improve legal protection for good faith security researchers in Germany remains in flux, and changes may take place before this publication is released, see for example Andre Meister (2024): Wir veröffentlichen den Gesetzentwurf zum Computerstrafrecht und Johannes Rundfeldt (2024): Nachbesserungsbedarf beim Reformvorschlag zum Hackerparagraph

Russian Federation has been finalizing a bill “to legalize white hat hacking.”[45] It remains to be seen whether this legal framework, and its enforcement once adopted, will offer the legal certainty and protection desired by good faith security researchers, especially since the Russian Federation succeeded in pushing for a low level of legal safeguards for security researchers on the international level through the **United Nations** consensus agreement on a draft convention at the Ad Hoc Committee on Cybercrime (AHC)[46].[47]

The **United States** has been a pioneer in implementing Government Disclosure Decision Processes (GDDP)[48] through its 2010 Vulnerabilities Equities Policy and Process (VEP).[49] However, only a few governments, including the **Netherlands**, the **United Kingdom**, and **Australia**, have adopted similar measures – and shared these publicly.[50] **Germany** has been attempting to establish a Government Disclosure Decision Process since at least 2018 but has not yet succeeded.[51]

The **European Union** made notable advancements in enhancing its vulnerability policy ecosystem with the entry into force of the Directive on measures for a high common level of cybersecurity across the Union (NIS-2 Directive) in 2023. This Directive mandates, inter alia, that European Union member state governments adopt a vulnerability management policy as part of their national cybersecurity strategy and designate a national CSIRT as Coordinated Vulnerability Disclosure

[45] Justin Sherman (2024): Russia’s white hat hacker bill exposes cyber struggles and strengths

[46] United Nations (2024): Draft United Nations convention against cybercrime – Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes (A/AC.291/L.15)

[47] Tobias B. Bacherle (2024): Russia and China Cheer UN Cybercrime Convention and Karen Gullo (2024): Draft UN Cybercrime Treaty Could Make Security Research a Crime, Leading 124 Experts to Call on UN Delegates to Fix Flawed Provisions that Weaken Everyone’s Security and Katitza Rodriguez (2024): The UN Cybercrime Draft Convention Remains Too Flawed to Adopt

[48] Sven Herpig and Ari Schwartz (2019): The Future of Vulnerabilities Equities Processes Around the World

[49] The White House (2017): Vulnerabilities Equities Policy and Process for the United States Government

[50] Marietje Schaake, Lorenzo Pupillo, Afonso Ferreira, and Gianluca Varisco (2018): Software Vulnerability Disclosure in Europe — Technology, Policies and Legal Challenges and Nathaniel Fick, Jami Miscik, Adam Segal, and Gordon M. Goldstein (2022): Confronting Reality in Cyberspace — Foreign Policy for a Fragmented Internet and Government Communications Headquarters (2024): The Equities Process and Australian Signals Directorate (2024): Responsible Release Principles for Cyber Security Vulnerabilities and Communications Security Establishment (2024): CSE’s Equities Management Framework. The actual number of governments implementing a Government Disclosure Decision Process-like process is likely higher. Due to national security concerns, public information on this policy field is scarce.

[51] Marietje Schaake, Lorenzo Pupillo, Afonso Ferreira, and Gianluca Varisco (2018): Software Vulnerability Disclosure in Europe — Technology, Policies and Legal Challenges and Sven Herpig (2024): Vulnerability Equities Process

coordinator, and requires the European Cybersecurity Agency (ENISA) to develop a "European vulnerability database."[52] Additionally, ENISA became a Common Vulnerabilities and Exposures (CVE) Numbering Authority (CNA), offering this service to EU Computer Security Incident Response Teams (CSIRTs).[53] With the vulnerability handling requirements for manufacturers outlined in the Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act),[54] the **European Union** took even further its focus on minimizing vulnerabilities in products and the risks stemming from them. The requirements include, among others, having a policy on Coordinated Vulnerability Disclosure, sharing information about potential vulnerabilities, and having mechanisms in place to securely distribute mitigations and patches.

In contrast, the **People's Republic of China's** 2021 Regulation on the Management of Network Product Security Vulnerabilities is an extremely worrisome policy development.[55] Rather than enabling the sharing of information about the vulnerability with code owners or coordinators, thus enabling an improvement in cybersecurity through Coordinated Vulnerability Disclosure, this regulation requires researchers to report vulnerabilities to the Chinese authorities within 48 hours.[56] Moreover, China has set up a membership-based system in which companies and researchers can disclose directly to a vulnerability database, the China National Vulnerability Database of Information Security (CNNVD).[57] This steady stream of reports allows Chinese government agencies to selectively decide which vulnerabilities to disclose publicly and which to potentially leverage in future cyber operations. China appears to have created the opposite of an ecosystem encouraging proper Coordinated Vulnerability Disclosure – an ecosystem where researchers and vulnerabilities are regarded as strategic assets for offensive operations.

[52] Christina Rupp (2024): Navigating the EU Cybersecurity Policy Ecosystem — A Comprehensive Overview of Legislation, Policies and Actors

[53] European Union Agency for Cybersecurity (2024): Another step forward towards responsible vulnerability disclosure in Europe

[54] The European Parliament (2024): REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

[55] Dina Temple-Raston (2023): 101. Bug bounties with Chinese characteristics and Eugenio Benincasa (2024): From Vegas to Chengdu: Hacking Contests, Bug Bounties, and China's Offensive Cyber Ecosystem and Catalin Cimpanu (2021): Chinese government lays out new vulnerability disclosure rules

[56] Dakota Cary and Kristin Del Rosso (2023): Sleight of hand: How China weaponizes software vulnerabilities

[57] Dakota Cary and Kristin Del Rosso (2023): Sleight of hand: How China weaponizes software vulnerabilities and Eugenio Benincasa (2024): From World Champions to State Assets: The Outsized Impact of a Few Chinese Hackers

The recent **United Nations** consensus agreement on a draft convention at the Ad Hoc Committee on Cybercrime (AHC)[58] also marks a step in the wrong direction by cementing legal uncertainty for security researchers. Among other issues, the scope of the convention is too broad and does not protect good faith security researchers.[59] It leaves it up to the implementing governments to decide whether criminal intent matters for persecution or not – maintaining an internationally heterogeneous system of legal uncertainty for security researchers.

2.4 Cyber Diplomacy Meets Vulnerability Realpolitik

Given their abstract nature, bringing normative ideas that were agreed on at the United Nations in New York together with day-to-day operations taking place in countries such as China, France, Germany, Iran, Israel, Russia, South Africa, the United Kingdom, and the United States, is no easy feat. And it becomes a Herculean task when it concerns vulnerabilities in code.

On the one side – and this is what states discuss at the United Nations – is the risk that vulnerabilities may pose to cybersecurity. Addressing this risk would require collaboration between various stakeholders – governmental and non-governmental alike – to improve global cybersecurity and the stability of cyberspace, for example, through better vulnerability disclosure.

However, the other side of the coin is the reality that states can leverage vulnerabilities as strategic assets to further core sovereign interests (see, e.g., 2.3 Government Vulnerability Disclosure Practice).

High-level discussions about vulnerabilities are focused mainly on the threat they pose. Meanwhile, governments' perceived need to exploit vulnerabilities for national security purposes tends to remain in the shadows. Hence, the public narrative created by states features vulnerabilities almost exclusively as a risk. While this is true, states rarely get to the hard points of the discussion.

[58] United Nations (2024): Draft United Nations convention against cybercrime – Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes (A/AC.291/L.15)

[59] United Nations Human Rights Office of the High Commissioner (2024): Human rights and the draft Cybercrime Convention and Karen Gullo (2024): Protect Good Faith Security Research Globally in Proposed UN Cybercrime Treaty and Tobias B. Bacherle (2024): The UN Cybercrime convention is a victory for digital authoritarianism

Policies such as the **Chinese** Regulation on the Management of Network Product Security, along with the increasing deployment of cyber campaigns in geopolitical conflicts[60] and systemic rivalries,[61] highlight the **growing utilization of vulnerabilities and security researchers as strategic assets,** as they are typically not disclosed to maximize their potential for exploitation.

Therefore, when observing the B. Perspectives on the United Nations Vulnerability Disclosure Norm, public statements should not be taken at face value. Additionally, the mere expression of related activities and ambitions does not allow for the distilling or even measuring of how effectively or successfully these are implemented in practice. Thus, tracing a public debate at the United Nations level produces a one-sided overview of what states would like to feature publicly. Subsequently, "publicly accessible information very likely only reflects a small portion of actual state practices and states probably choose to publicize only parts or aspects in their particular interest."[62]

It becomes even more complicated when governments opine on measures in which they have no experience.[63] While there is value for all states to be part of such debates – for example, to better understand the real-world impact of their policies – experience comes from operationally handling vulnerabilities, defensively and offensively. If countries suggest measures in which they have little or no practical experience, it may be a good idea that serves as inspiration but could also just be empty virtue-signaling. Moreover, while what countries suggest could be a good idea that they just have not yet got around to implementing themselves, it may also be pure diplomatic posturing. That could, for example, include proposals for limiting offensive cyber capabilities coming from countries that do not themselves have such capabilities or regulations in place.

It does, for example, make a huge difference whether, hypothetically speaking, the **United States** suggests curbing vulnerability trading for military use, while employing such capabilities themselves, or if **Costa Rica** – a country without a

[60] For example, JD Work (2021): Balancing on the rail – considering responsibility and restraint in the July 2021 Iran railways incident

[61] For example, Cybersecurity and Infrastructure Security Agency (2024): U.S. and International Partners Publish Cybersecurity Advisory on People's Republic of China State-Sponsored Hacking of U.S. Critical Infrastructure

[62] Christina Rupp and Alexandra Paulus (2023): Official Public Political Attribution of Cyber Operations – State of Play and Policy Options

[63] While far from perfect in terms of significance, indices such as the International Telecommunication Union (2024): Global Cybersecurity Index, e-Governance Academy Foundation (2023): national cyber security index – Archived data from 01.09.2023, or the Julia Voo, Irfan Hemani, and Daniel Cassidy (2022): National Cyber Power Index 2022 may offer an indication of a country's general expertise and maturity in the domain.

military force – recommends the same. In this scenario, if proposed by Costa Rica, the United States would face the uncomfortable choice of either restricting the use of vulnerability trading for military purposes – even though Costa Rica would not be engaging in it – or admitting that it is unwilling to impose such restrictions.

Lastly, government representatives may suggest measures in which they have expertise, and pretend to be undertaking, but do not actually intend to comply with whatever commitments they have made. The goal is to put other countries, especially adversaries, at a strategic or even operational disadvantage while appearing to be the voice of reason. One example is that **Russia** advocates strongly against "integrating undeclared capabilities in ICTs" in the B. Perspectives on the United Nations Vulnerability Disclosure Norm, while the Russia-linked threat actor APT44[64] has been responsible for inserting malicious code into an update of an accounting software (*M.E.Doc*)[65] and the Russia-linked threat actor APT29[66] has been responsible for inserting malicious code into infrastructure monitoring and management software (*SolarWinds Orion*).[67]

Considering all these challenges, points made during the United Nations norms debate (see 2.2 Government and Non-Government Perspectives), as well as actions taken by governments independently from whether they are explicitly linked to the vulnerability disclosure norm or not (see 2.3 Governmental Vulnerability Disclosure Practice), can both serve as inspiration of what governments can do to implement the vulnerability disclosure norm. Ultimately and realistically, however, any government will need to vet this inspiration against its applicability, limitations, risks, and usefulness in bolstering national security. It is ideal if activities can achieve this and support the implementation of the vulnerability disclosure norm at the same time. This forms the basis for the 4. Implementation Actions recommended in this paper.

[64] Fraunhofer FKIE (2024): malpedia – Sandworm

[65] Jack Rhysider and Andy Greenberg (2019): Ep 54: NotPetya

[66] Fraunhofer FKIE (2024): malpedia – UNC2452

[67] FireEye (2022): Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor

2.5 Actionable Reading

As 1. Introduction, 2.1 United Nations Norms Guidance, 2.2 Government and Non-Government Perspectives, and 2.3 Government Vulnerability Disclosure Practice show, the current interpretation of the vulnerability disclosure norm is a puzzle made up of high-level guidance, explicit state practice and government perspectives, implicit state practice – what states already do in the area of vulnerability disclosure without specifically tying it to the norm – and third-party interpretation. Informed by these practices, this section offers an actionable reading of the vulnerability disclosure norm. This understanding will guide the concrete recommendations for operationalization by governments.

Going back to the norm j, it reads as follows: “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.” Crucial here are the following aspects: *encourage responsible reporting of vulnerabilities* and *share associated information on available remedies*. The rest of the norm does not contain actionable components. While there is no agreed definition for *responsible reporting* in the cybersecurity communities, *coordinated disclosure* reflects the meaning of the term and is a well-established practice that excludes “inherent value judgment.”[68] Therefore, interpreting *responsible reporting* as *coordinated disclosure* makes the norm actionable while keeping its intention intact. Additionally, *associated information on available remedies* is known in cybersecurity communities as *patches* and *mitigations*. *Sharing associated information on available remedies*, *patches* and *mitigations* is part of *Coordinated Vulnerability Disclosure*[69].

On that basis, a shortened, actionable version of the vulnerability disclosure norm in line with its objectives is:

[68] For example, rain forest puppy (2000), Full Disclosure Policy (RFPolicy) and Chris Wysopal and Steve Christey (2002): Responsible Vulnerability Disclosure Process draft-christey-wysopal-vuln-disclosure-00.txt and Allen D. Householder, Garret Wassermann, Art Manion, and Chris King (2017): The CERT® Guide to Coordinated Vulnerability Disclosure and FIRST (2020): Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure and Google (2021): Guide to implementing a coordinated vulnerability disclosure process for open source projects and ETSI (2022): Cyber Security; Guide to Coordinated Vulnerability Disclosure and Organisation for Economic Co-operation and Development (2023): Good Practice Guidance on the Co-ordination of Digital Security Vulnerabilities and ISO (2024): ISO/IEC 29147:2018 – Information technology — Security techniques — Vulnerability disclosure

[69] For example, Allen D. Householder, Garret Wassermann, Art Manion, and Chris King (2017): The CERT® Guide to Coordinated Vulnerability Disclosure

> "States should encourage Coordinated Vulnerability Disclosure through creating and fostering an enabling policy ecosystem."

This actionable reading builds upon three considerations that are pivotal for shaping policies governing the reporting and management of cybersecurity vulnerabilities.

- The first consideration involves the concept of *reporting*, better understood as *Coordinated Vulnerability Disclosure*. The original wording of the norm implies that states should focus on encouraging *reporting* discovered vulnerabilities rather than encouraging their finding. Thus, policies that incentivize the *finding* of new vulnerabilities, such as supporting bug bounty programs, may technically not fall within the scope of the norm. This involves two key areas for potential policy development: legal protection for security researchers and vulnerability reward programs. However, as can also be seen in the 2.2 Government and Non-Government Perspectives, there is an overlap between the vulnerability disclosure norm and these areas. Consequently, policies in this domain require a nuanced approach. For instance, legal protection for security researchers should cover the *finding* of vulnerabilities, provided they act in good faith. The latter includes actions that aim to reduce the risk stemming from the vulnerability found (e.g., contacting the code owner for Coordinated Vulnerability Disclosure) or at least not exacerbating it (e.g., by not selling it to a third party). To facilitate this, the government should provide a mechanism for processing vulnerabilities when no other viable means of initiating a *Coordinated Vulnerability Disclosure* exist.
- The second consideration pertains to *encouraging* both positive and negative incentives. *Encouraging*, in this context, involves creating incentives to promote desired behaviors and disincentives to deter undesirable actions from state and non-state actors. Positive incentives include legal protections for security researchers or Government Disclosure Decision Processes, encouraging the respective actors to process their vulnerabilities through a *Coordinated Vulnerability Disclosure* process. Negative incentives may involve lack of legal protection as well as sanctioning own government entities that fail to process vulnerabilities promptly through a *Coordinated Vulnerability Disclosure* process.
- The third consideration is that while *Coordinated Vulnerability Disclosure* is an established and well-defined organizational process – that many regard as the ideal way to reduce risks when disclosing vulnerabilities – there are many key enabling measures that are only loosely affiliated with or that touch lightly upon the process. Therefore, the actionable reading is not limited

strictly to *Coordinated Vulnerability Disclosure* as a process defined by the corresponding international standards, but extends to *an enabling policy ecosystem* for this process. The recommended measures in 4. Implementation Actions reflect this consideration.

3. Coordinated Vulnerability Disclosure

As discussed in 2. Vulnerability Disclosure Norm, Coordinated Vulnerability Disclosure is the key vehicle for governments to implement the vulnerability disclosure norm. This chapter briefly recapitulates both the theory and practice of Coordinated Vulnerability Disclosure, covering its definition, the structure of the process, the roles and phases involved, and the challenges related to its effective implementation. The primary aim of this section is to summarize the existing rich body of literature, rather than to introduce new contributions. The final part of the chapter highlights the various roles governments may assume during the Coordinated Vulnerability Disclosure process.

3.1 Process

The actionable reading of the vulnerability disclosure norm focuses on the implementation of a well-known, standardized cybersecurity process:[70] Coordinated Vulnerability Disclosure. While the terms "vulnerability disclosure" and "Coordinated Vulnerability Disclosure" have both already been introduced briefly in this paper, it is important to review their comprehensive definitions as basis for further analyses and recommendations.

Vulnerability disclosure is defined by International Standards as:

> "A process through which vendors and vulnerability finders may work cooperatively in finding solutions that reduce the risks associated with a vulnerability. It encompasses actions such as reporting, coordinating, and publishing information about a vulnerability and its resolution. The goals of vulnerability disclosure include the following: a) ensuring that identified vulnerabilities are addressed; b) minimizing the risk from vulnerabilities;

[70] For example, rain forest puppy (2000), Full Disclosure Policy (RFPolicy) and Chris Wysopal and Steve Christey (2002): Responsible Vulnerability Disclosure Process draft-christey-wysopal-vuln-disclosure-00.txt and Allen D. Householder, Garret Wassermann, Art Manion, and Chris King (2017): The CERT® Guide to Coordinated Vulnerability Disclosure and FIRST (2020): Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure and Google (2021): Guide to implementing a coordinated vulnerability disclosure process for open source projects and ETSI (2022): Cyber Security; Guide to Coordinated Vulnerability Disclosure and Organisation for Economic Co-operation and Development (2023): Good Practice Guidance on the Co-ordination of Digital Security Vulnerabilities and ISO (2024): ISO/IEC TR 5895:2022 – Information technology — Security techniques — Vulnerability disclosure

> c) providing users with sufficient information to evaluate risks from vulnerabilities to their systems."[71]

Based on this, Coordinated Vulnerability Disclosure is defined as:

> "The process of gathering information from vulnerability finders, coordinating the sharing of that information between relevant stakeholders, and disclosing the existence of software vulnerabilities and their mitigations to various stakeholders, including the public. CVD is an important aspect of any successful [Vulnerability Response] process. CVD inputs are vulnerability reports arising from vulnerability discovery practices. CVD outputs for product vulnerabilities (software or hardware) usually include patches as well as vulnerability report documents or vulnerability database records, typically with some formal identifier (e.g., CVE [...], VU# [...], and BID [...]). Many operational vulnerabilities such as router misconfigurations, website vulnerabilities, or cloud service problems can be fixed in situ by the operator, but often do not result in a public disclosure."[72]

A view from the open source communities defines Coordinated Vulnerability Disclosure as:

> "The process of sharing vulnerability details with the person or group who has the ability to respond and fix, and/or remediate the vulnerability. This is typically the open project maintainer, but could include project developers, collaborators, administrators, or other invested parties. The CVD process involves privately disclosing the vulnerability details, creating and testing a fix for the vulnerability, and then disclosing the fix and details with all downstream consumers simultaneously. This coordination ensures that all required parties are prepared with fixes, communications, updates at the same time. The benefits of disclosing a vulnerability through this method is that there is a fix available to all consumers at the same time, and no one group is put more at risk than others. Maintaining an information embargo during the mitigation and patching phase is key to protecting the users here.[73]

[71] ISO (2024): ISO/IEC TR 5895:2022 – Information technology — Security techniques — Vulnerability disclosure

[72] Allen D. Householder, Garret Wassermann, Art Manion, and Chris King (2017): The CERT® Guide to Coordinated Vulnerability Disclosure

[73] Open Source Security Foundation (2023): Guidance for Security Researchers to Coordinate Vulnerability Disclosures with Open Source Software Projects

In simple words, Coordinated Vulnerability Disclosure is about how to disclose found vulnerabilities in a way that ensures the highest possible level of cybersecurity for all affected parties. Since this is a process that usually involves various actors with different interests – creating a demand for the right incentives – the ideal approach is to proceed together, and in a coordinated manner, whenever possible."[74]

3.2 Roles

While the roles and most of their terms are universally recognized in cybersecurity communities, this paper borrows the two less-recognized terms *code owners* and *system owners* from the Organisation for Economic Co-operation and Development.[75] For other roles, the paper relies on well-established role descriptions, for example, from the Carnegie Mellon University.[76] Roles that are involved in Coordinated Vulnerability Disclosure are therefore:

- find vulnerabilities ("*finder*");
- report vulnerabilities ("*reporter*");
- maintain code that has vulnerabilities ("*code owner*");
  - maintain vulnerable code that is used by other code owners ("*upstream code owner*");
  - maintain code that depends on vulnerable code of another owner ("*downstream code owner*");
- run code that has vulnerabilities ("*system owner*");
  - run systems that depend on their own code ("*code-and-system owner*");[77]
- coordinate communication and actions between stakeholders ("*coordinator*").

In each Coordinated Vulnerability Disclosure there may be a multitude of actors assuming one or more of those roles. For example a finder may also become a reporter.

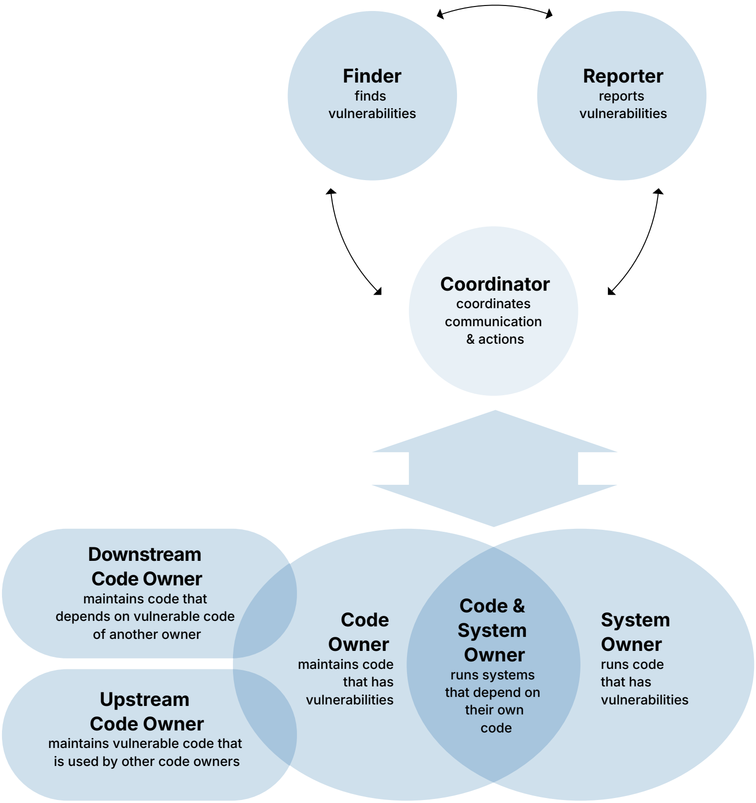
[74] Sven Herpig (2024): Schwachstellen gemeinsam richtig offenlegen

[75] Organisation for Economic Co-operation and Development (2021): Encouraging Vulnerability Treatment – Overview for policy makers

[76] Allen D. Householder, Garret Wassermann, Art Manion, and Chris King (2017): The CERT® Guide to Coordinated Vulnerability Disclosure

[77] This refers to cloud-based solutions where the code owner can directly patch or mitigate due to running the same systems that are being used by the clients.

1 **Roles that are involved in Coordinated Vulnerability Disclosure**


Finder
finds vulnerabilities
Reporter
reports vulnerabilities
Coordinator
coordinates communication & actions
Downstream Code Owner
maintains code that depends on vulnerable code of another owner
Upstream Code Owner
maintains vulnerable code that is used by other code owners
Code Owner
maintains code that has vulnerabilities
Code & System Owner
runs systems that depend on their own code
System Owner
runs code that has vulnerabilities

In each Coordinated Vulnerability Disclosure there may be a multitude of actors assuming one or more of those roles.

Government Roles: An Organization for Economic Co-operation and Development study states that "governments cumulate almost all possible roles in the vulnerability treatment landscape"[78] where Householder et al. assess that "governments are multifaceted stakeholders in regards to cybersecurity vulnerabilities and their disclosure. While they have always had a role as owners and operators of vulnerable networks and systems, issues surrounding vulnerability discovery, coordination, disclosure, and mitigation have become increasingly important to governments worldwide."[79] So there is actually no role in which the government could not find itself. Through "leading by example Governments can play a key role in encouraging the adoption of CVD and promoting a cultural shift with respect to vulnerability treatment."[80] In every capacity, government entities must set an example for

[78] Organisation for Economic Co-operation and Development (2021): Encouraging Vulnerability Treatment – Overview for policy makers

[79] Allen D. Householder, Garret Wassermann, Art Manion, and Chris King (2017): The CERT® Guide to Coordinated Vulnerability Disclosure

[80] Organisation for Economic Co-operation and Development (2021): Encouraging Vulnerability Treatment – Overview for policy makers

non-government entities[81] by adhering to internationally accepted standards and practices on Coordinated Vulnerability Disclosure.[82]

At this point, the government's role as possible coordinator should be specifically highlighted. Governments, often through their National Computer Security Incident Response Team, can act as coordinators in multiple dimensions. This includes horizontal coordination across national government entities, vertical coordination with local governments, and coordination with international organizations such as the European Union, the Association of Southeast Asian Nations (ASEAN), the African Union (AU) the Organization of American States (OAS), the North Atlantic Treaty Organization (NATO), the Organization for Security and Co-operation in Europe, and other international partners. Governments may also act as reporters for non-government stakeholders or as coordinators between multiple government and non-government entities. By assuming this central coordinating role, government agencies may be well positioned to offer complementary services, publish best practices, raise awareness for Coordinated Vulnerability Disclosure, and recommend policy changes.

3.3 Phases

A typical Coordinated Vulnerability Disclosure runs through various phases that may involve one or more of the abovementioned roles. There will always be vulnerability edge cases, which may lead to delays or even a complete halt at different phases during the Coordinated Vulnerability Disclosure process. For example, a vulnerability may exist in code that is abandoned[83] or no longer supported by the code owner as it has reached its end of life (EOL)[84] or runs

[81] NIS Cooperation Group (2023): Guidelines on Implementing National Coordinated Vulnerability Disclosure Policies and Global Forum on Cyber Expertise (2017): GFCE Global Good Practices – Coordinated Vulnerability Disclosure (CVD)

[82] For example, rain forest puppy (2000), Full Disclosure Policy (RFPolicy) and Chris Wysopal and Steve Christey (2002): Responsible Vulnerability Disclosure Process draft-christey-wysopal-vuln-disclosure-00.txt and Allen D. Householder, Garret Wassermann, Art Manion, and Chris King (2017): The CERT® Guide to Coordinated Vulnerability Disclosure and FIRST (2020): Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure and Google (2021): Guide to implementing a coordinated vulnerability disclosure process for open source projects and ETSI (2022): Cyber Security; Guide to Coordinated Vulnerability Disclosure and Organisation for Economic Co-operation and Development (2023): Good Practice Guidance on the Co-ordination of Digital Security Vulnerabilities and ISO (2024): ISO/IEC TR 5895:2022 – Information technology — Security techniques — Vulnerability disclosure and Kim Schaffer, Peter Mell, Hung Trinh, and Isabel Van Wyk (2023): NIST SP 800-216 – Recommendations for Federal Vulnerability Disclosure Guidelines

[83] Sven Herpig (2023): Fostering Open Source Software Security – Blueprint for a Government Cybersecurity Open Source Program Office

[84] Sven Herpig (2024): Was kommt nach dem Ende des Lebenszyklus?

on a device that is not easily patched. The latter may include situations where physical access is necessary for patching but the device is in a remote location – for example, wind turbines or satellites.[85] The following description is a summary of various in-depth discussions about the different phases.[86]

Discovery of the vulnerability: During the discovery, a *finder* identifies a vulnerability. Several *finders* may stumble upon the same vulnerability at the same time, making it a parallel discovery. The vulnerability can either be a misconfiguration by the *system owner*, a vulnerability known to *code owners* and possibly even the *system owner* but unpatched – for example, because the patch has not been applied – or a vulnerability unknown to *code owners* and *system owners*. *Finders* may already run more vulnerability analyses during this stage, trying to replicate it and assess its severity.

Disclosure of the vulnerability: After the discovery, *finders* decide whether to disclose the vulnerability in a coordinated manner or not. If *finders* decide to disclose them through Coordinated Vulnerability Disclosure, they can either turn into *reporters* themselves or hand over vulnerability information to a *reporter* who will start the Coordinated Vulnerability Disclosure process. During the disclosure, *reporters* contact *code owners* or *system owners* either directly or through a *coordinator* and submit the information they have on the vulnerability. For this phase, it is important that *reporters* can easily find and access contact details[87] as well as the vulnerability disclosure policy[88] of the *code owner* or *system owner* so they know who to contact and what to expect, for example, in terms of legal protection or rewards.

Verification and assessment of the vulnerability: During the verification and assessment, *code owners* and *system owners* verify the existence of the vulnerability and assess severity, impacted products, dependencies and other aspects of the vulnerability. In this phase, *code owners* may need to contact

[85] See, for example, Viasat (2022): KA-SAT Network cyber attack overview

[86] Tassilo Thieme (2021): Heureka! Von der Schwachstellenfindung bis zur Veröffentlichung: Entwicklung eines Coordinated Vulnerability Disclosure Prozesses für kleine und mittelständische IT-Unternehmen and Allen Householder and Jonathan Spring (2021): A State-Based Model for Multi-Party Coordinated Vulnerability Disclosure (MPCVD) and FIRST (2020): Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure for roles during various stages and visualized timelines.

[87] For example, by code owners and system owners implementing RCF 9116, see Edwin Foudil and Yakov Shafranovich (2022): A File Format to Aid in Security Vulnerability Disclosure or through querying dedicated databases such as Forum of Incident Response and Security Teams (2024): Incident Response Database

[88] ISO (2024): ISO/IEC 29147:2018 – Information technology — Security techniques — Vulnerability disclosure

downstream code owners for information about their code and *upstream code owners* to give advance notice about the vulnerability. If needed, *code owners* and *system owners* will communicate with the *reporter* – through the *coordinator,* if one was leveraged – to gather additional information about the vulnerability. Ideally, *code owners* and *system owners* will update the *reporter* on the progress.

Preparation of patches and/or mitigations: During this phase, *code owners* prepare a patch and/or mitigation. They may work together with the *reporter* and/or *coordinator* as well as *upstream code owners* and *downstream code owners* to make sure that the patch or mitigation is effective.

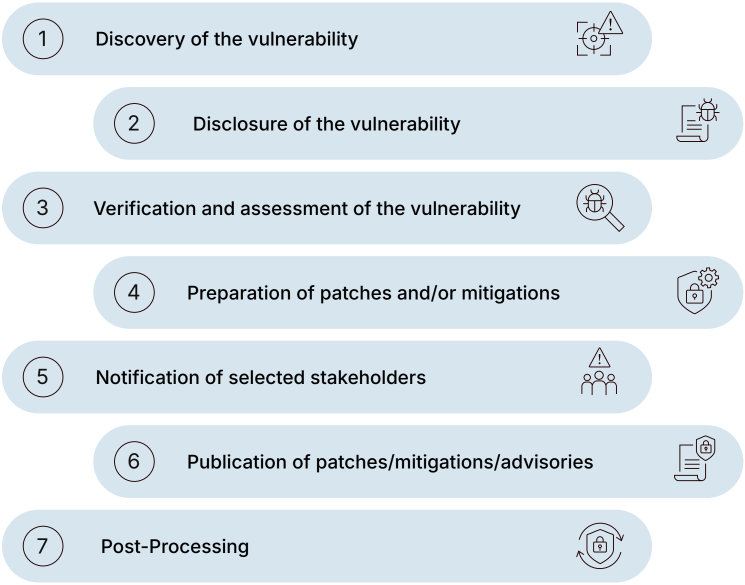
Notification of selected stakeholders: If not already done during the previous phases, *code owners* notify affected *upstream code owners* and *downstream code owners* about the vulnerability and patch and/or mitigation. Additionally, *code owners* may inform security vendors to update their detection rules to notify them about exploitation attempts.[89] *Code owners* may also inform other selected stakeholders, such as National Computer Security Incident Response Teams, ahead of patch and/or mitigation publication.

Publication of patches and/or mitigations and/or advisories: *Code owners* publish the patch and/or mitigation in close coordination with potential patches and/or mitigations from *upstream code owners* and *downstream code owners* as well as publication work of the *finder,* for example, blog articles or presentations at cybersecurity conferences. *Code owners* and other stakeholders may also publish advisories and communicate information about the patch and/or mitigation through various channels and with the support of other stakeholders, such as the *coordinator* or National Computer Security Incident Response Teams. *Code-and-system owners* apply patches to their systems, issue advisories and inform their customers. *System owners* apply patches and/or mitigations.

Post-Processing: All involved stakeholders monitor the effectiveness of the patch and/or mitigation. *Code owners, upstream code owners, downstream code owners,* and *code-and-system owners* adjust mitigations and/or patches if they are not effective or prepare an additional patch and/or mitigation. Various stakeholders such as *code owners* or National Computer Security Incident Response Teams may monitor the mitigation and/or patch update and potentially issue additional warnings and/or advisories to improve mitigation/patch implementation rate by *system owners*.

[89] Eric Pauley, Paul Barford, and Patrick McDaniel (2023): The CVE Wayback Machine: Measuring Coordinated Disclosure from Exploits against Two Years of Zero-Days

2 Phases of Coordinated Vulnerability Disclosure



1 Discovery of the vulnerability

2 Disclosure of the vulnerability

3 Verification and assessment of the vulnerability

4 Preparation of patches and/or mitigations

5 Notification of selected stakeholders

6 Publication of patches/mitigations/advisories

7 Post-Processing

ⓘ Each phase is crucial to ensure vulnerabilities are addressed in a responsible and coordinated manner.

Additional operational parameters of Coordinated Vulnerability Disclosure include, for example, whether anonymous reporting is allowed, whether encrypted reporting is feasible, and the length of the waiting period for reporters before escalating the disclosure to a limited or full disclosure.[90,91] While these specifications may seem minor, ensuring their accuracy is crucial, as the process can fail at any point due to incorrect or incorrectly perceived parameters. Generally, these parameters are largely standardized in both theory and practice, with only slight deviations.

[90] According to Jukka Ruohonen and Luca Allodi (2018): A Bug Bounty Perspective on the Disclosure of Web Vulnerabilities full disclosure “refers to a vulnerability disclosure practice via which full technical details are released to the public, possibly regardless whether a vendor was even contacted about the vulnerabilities prior to the release. There were—and still are—good reasons for hackers to prefer this type of vulnerability disclosure. Among these is the reluctance of many vendors to acknowledge and fix the vulnerabilities reported.”

[91] For example, Stephen Shepherd (2003): How do we define Responsible Disclosure? and ETSI (2022): Cyber Security; Guide to Coordinated Vulnerability Disclosure and Allen D. Householder, Garret Wassermann, Art Manion, and Chris King (2017): The CERT® Guide to Coordinated Vulnerability Disclosure and Jukka Ruohonen and Luca Allodi (2018): A Bug Bounty Perspective on the Disclosure of Web Vulnerabilities

3.4 Challenges

Coordinated Vulnerability Disclosure practice has progressed from "utter chaos"[92] and a "loosely organized effort"[93] to "doing a lot better than it did 20 years ago"[94] with some ups and downs in between.[95] Thanks to efforts by various stakeholders, there is a vast body of accessible literature on how to get Coordinated Vulnerability Disclosure right, depending on your role. Perception seems also to have changed to a degree where Coordinated Vulnerability Disclosure is now most often seen as the gold standard of disclosing a vulnerability, as compared to, for example, full disclosure[96]. While, as mentioned in 2.2 Development of State Practice, government intervention is still catching up and sometimes unfortunately moving in the wrong direction, most key stakeholders should be aware of Coordinated Vulnerability Disclosure and have access to information about how to do their part. However, Coordinated Vulnerability Disclosure still remains challenging in practice[97] today, not improving cybersecurity as much as it could. Coupled with continual digitization and thereby an increase of reported vulnerabilities,[98] this becomes a serious challenge for national and international security. Several challenges have been identified for Coordinated Vulnerability Disclosure in practice.

Legal Uncertainty: Vulnerability reporters can rarely be sure how the code owners and system owners will respond. Legal action has occasionally been threatened against the reporters, strongly disincentivizing vulnerability reporting.[99] A threat of legal action coupled with legal uncertainty creates a chilling effect that is strongly disincentivizing, regardless of whether reporters have in the past been convicted or not. Therefore, the corresponding legal framework[100] needs clarity and should err on the side of the researchers.

[92] Stephen Shepherd (2003): How do we define Responsible Disclosure?

[93] Stephen Shepherd (2003): How do we define Responsible Disclosure?

[94] Kaspersky (2020): Can we avoid an arms race in cyberspace?

[95] ERNW INSINUATOR (2015): Reflections on Vulnerability Disclosure

[96] Aleksandra Sowa (2024): Security by Obscurity: Die nächste Generation

[97] Sven Herpig (2024): Schwachstellen gemeinsam richtig offenlegen

[98] statista (2024): Number of common IT security vulnerabilities and exposures (CVEs) worldwide from 2009 to 2024 YTD

[99] For example. ENISA and RAND Europe (2015): Good Practice Guide on Vulnerability Disclosure – From challenges to recommendations and NTIA Awareness and Adoption Group (2016): Vulnerability Disclosure Attitudes and Actions and Simon Hurtz (2021): CDU blamiert sich mit Anzeige gegen IT-Expertin and Good Faith Cybersecurity Researchers Coalition (2024): Riana Pfefferkorn - US Anti-Hacking Laws: It's Not Just Criminal Penalties and Sunoo Park and Kendra Albert (2020): A Researcher's Guide to Some Legal Risks of Security Research and Global Forum on Cyber Expertise (2017): GFCE Global Good Practices – Coordinated Vulnerability Disclosure (CVD)

[100] For a list of legal frameworks, see Good Faith Cybersecurity Researchers Coalition (2024): Laws and Rules

Absence of Rewards: Finders and reporters often are not offered any kind of reward for their work, thereby creating no positive incentives to report a vulnerability. Finders and reporters spend time identifying and disclosing vulnerabilities to code owners and system owners. Since this communication can be time consuming, this effort should lead to such basic rewards as recognition and/or monetary remuneration.[101]

Lack of Guidance: It can often take reporters too much effort to find out how to report a vulnerability and to whom. As a consequence, they may decide it is not worth the effort as code owners and system owners – and, to a certain degree coordinators – should facilitate initial contact as much as possible.[102]

Trust Deficit: Reporters who want to ensure that the vulnerability will be processed to increase IT security do not trust governmental stakeholders in any role. A 2015 study showed that "interviewees expressed concerns about the potential implications of sharing vulnerability information with an organisation which is 'part of the government' and may not be 'independent'".[103] They suspect that the vulnerability may be exploited in intrusive governmental cyber operations instead of being immediately processed through a Coordinated Vulnerability Disclosure.[104]

Immature Vulnerability Disclosure: Code owners are not prepared for vulnerability intake and handling for various reasons.[105] The reporter may get the vulnerability information to the code owner but the code owner may not know what to do with that information or may simply lack the technical capacity and organizational management to act on it. Complexity is added when coordination is needed across the supply chain with multiple parties such as upstream and downstream code owners. The challenge becomes more severe with an increasing number of non-traditional stakeholders becoming code owners,[106] such as those

[101] Organisation for Economic Co-operation and Development (2021): Encouraging Vulnerability Treatment – Overview for policy makers

[102] For example, ENISA and RAND Europe (2015): Good Practice Guide on Vulnerability Disclosure – From challenges to recommendations

[103] ENISA and RAND Europe (2015): Good Practice Guide on Vulnerability Disclosure – From challenges to recommendations

[104] For example, ENISA and RAND Europe (2015): Good Practice Guide on Vulnerability Disclosure – From challenges to recommendations and Organisation for Economic Co-operation and Development (2021): Encouraging Vulnerability Treatment – Overview for policy makers

[105] For example, ENISA and RAND Europe (2015): Good Practice Guide on Vulnerability Disclosure – From challenges to recommendations and Global Forum on Cyber Expertise (2017): GFCE Global Good Practices – Coordinated Vulnerability Disclosure (CVD)

[106] ERNW (2015): ERNW Newsletter – Reflections on Vulnerability Disclosure and a Case Study

responsible for cars, medical devices, or a range of household devices that were not previously digitized and networked.

Communication Breakdowns: Even after successful initial contact, follow-up communication may be hampered for various reasons. Reporters may not be given a secure or anonymous channel to report details on the vulnerability, may not be kept in the loop of the disclosure process, may be threatened with legal action or just be ignored by the code owners or systems owners.[107] However, code owners and system owners may have no way of inquiring about further details, the report may lack a first assessment and be unable to be verified, or the reporter may threaten premature publication or ignore them completely.[108]

Multi-Party Coordination Complications: As software supply chains are growing increasingly complex, it is worthwhile pointing to a subcategory of Coordinated Vulnerability Disclosure: Multi-Party Coordinated Vulnerability Disclosure (MPCVD).[109] Multi-Party Coordinated Vulnerability Disclosure is "a more complex form of CVD, involving the necessity to coordinate numerous stakeholders in the process of recognizing and fixing vulnerable products. [...] The need for MPCVD arises from the complexities of the software supply chain."[110] For example, "a remediation development and testing for a vulnerability in a hardware component can depend on an operating system running on the hardware, and require different actions from different operating system providers. Due to these considerations, multiple vendors need to participate in remediation efforts involving certain vulnerabilities."[111] Such scenarios are prone to ending in premature public disclosure by one or more parties. For example, if the reporter does not get any feedback on the current stage of the disclosure process, they may decide to publish a warning or article. Or it may be the case that several code owners are ready to roll out patches while others are not yet ready at that stage.[112]

[107] For a recent example, see Simone Margaritelli (2024): Attacking UNIX Systems via CUPS, Part I

[108] For example, ENISA and RAND Europe (2015): Good Practice Guide on Vulnerability Disclosure – From challenges to recommendations and Organisation for Economic Co-operation and Development (2021): Encouraging Vulnerability Treatment – Overview for policy makers and NTIA Awareness and Adoption Group (2016): Vulnerability Disclosure Attitudes and Actions and Global Forum on Cyber Expertise (2017): GFCE Global Good Practices – Coordinated Vulnerability Disclosure (CVD)

[109] See, for example, Forum of Incident Response and Security Teams (2020): Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure and Allen Householder and Jonathan Spring (2021): A State-Based Model for Multi-Party Coordinated Vulnerability Disclosure (MPCVD)

[110] Allen Householder and Jonathan Spring (2021): A State-Based Model for Multi-Party Coordinated Vulnerability Disclosure (MPCVD)

[111] ISO (2022): Cybersecurity — Multi-party coordinated vulnerability disclosure and handling

[112] For example, Allen Householder and Jonathan Spring (2021): A State-Based Model for Multi-Party Coordinated Vulnerability Disclosure (MPCVD)

Patch Deployment and Distribution Shortcomings: For various reasons, such as a lack of understanding of the vulnerability, lack of technical capacity, or management support, the code owner fails to provide working patches and/or mitigations at all or within a reasonable/agreed-on timeframe. Moreover, code owners may be able to provide working patches and/or mitigations but, due to the complexity of the supply chain, resource restrictions, or other reasons, are unable to identify and proactively push patches and/or mitigations to the system owners.[113]

Patch Implementation Delays: The Coordinated Vulnerability Disclosure process ideally ends with all vulnerable systems being patched. System owners, however, may fail to implement existing patches or mitigations in a timely manner for several reasons. These reasons include a lack of awareness regarding what systems are in use and not having patches and mitigations available, lack of staff resources to maintain the systems, uncertainty about whether patches and mitigations may break vital dependencies – particularly in IT infrastructures with legacy systems and custom-made applications – or, in the case of end users, simply ignoring the "patch-now" button.[114]

Cybersecurity at large would benefit from these challenges being mitigated, as a study shows that "minor improvements to the CVD process could yield outsize protection in practice."[115] The state can play a role in addressing these challenges by broadly creating positive and negative incentives – steering the interests of the involved stakeholders toward successful Coordinated Vulnerability Disclosure.

[113] For example, Organisation for Economic Co-operation and Development (2021): Encouraging Vulnerability Treatment – Overview for policy makers

[114] For example, ENISA and RAND Europe (2015): Good Practice Guide on Vulnerability Disclosure – From challenges to recommendations and Jukka Ruohonen and Luca Allodi (2018): A Bug Bounty Perspective on the Disclosure of Web Vulnerabilities and Global Forum on Cyber Expertise (2017): GFCE Global Good Practices – Coordinated Vulnerability Disclosure (CVD)

[115] Eric Pauley, Paul Barford, and Patrick McDaniel (2023): The CVE Wayback Machine: Measuring Coordinated Disclosure from Exploits against Two Years of Zero-Days

4. Implementation Actions

Governments are frequently perceived as merely "designers of [the] legal framework interacting with vulnerability disclosure."[116] In this role, governments make and shape "public policies [which] can encourage stakeholders to treat vulnerabilities more efficiently."[117] How governments should shape public policy in the area of vulnerability disclosure – on the national level and through international cooperation – is shown in this chapter.

The following section outlines 16 specific actions that governments can take to implement the vulnerability disclosure norm by creating and fostering a policy ecosystem that enables Coordinated Vulnerability Disclosure implementation. These actions draw on the vulnerability disclosure norm guidance (see 2.1 United Nations Norms Guidance), norm debates (see 2.2 Governmental and Non-Governmental Perspectives), policy practice (see 2.3 Governmental Vulnerability Disclosure Practice), and norm operationalization (see 2.5 Actionable Reading), with a focus on foundational tasks for establishing and managing 3. Coordinated Vulnerability Disclosure processes, while addressing the existing 3.4 Challenges.

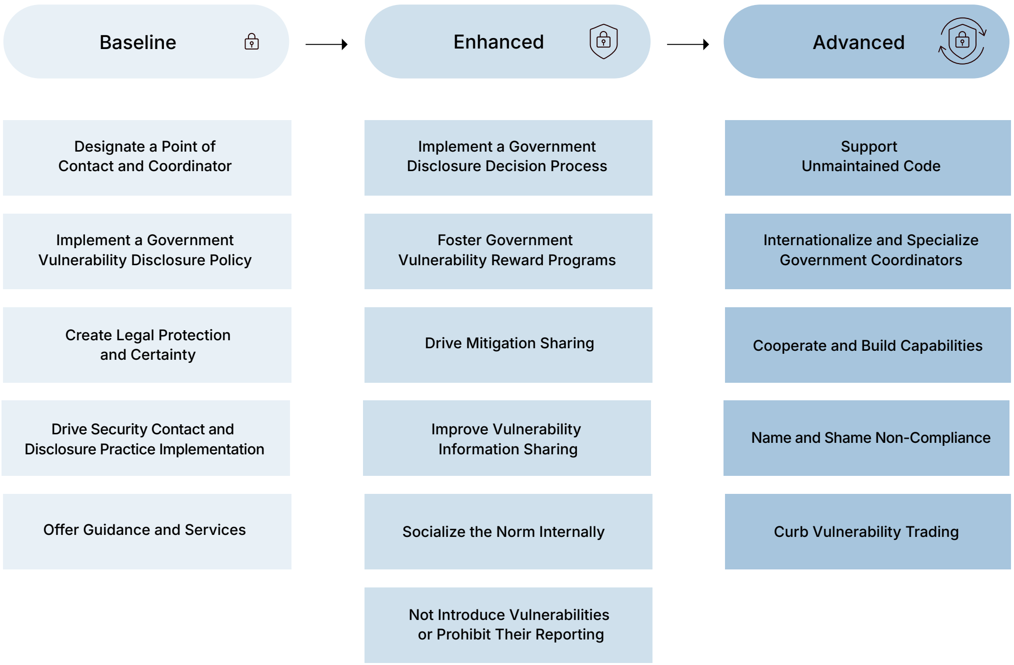
Each proposed measure is detailed and summarized, indicating its relevant phases and roles within the Coordinated Vulnerability Disclosure process. The instruments are categorized into "baseline," "enhanced," and "advanced" to distinguish foundational tasks from more advanced ones in terms of required resources and capabilities. Within each category measures are sorted, starting with the core instruments and moving toward enabling elements. For further prioritization, the terms "should" and "could" are used deliberately in the summaries.

An overview can be found in the A. Checklist.

[116] ENISA (2016): Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations

[117] Organisation for Economic Co-operation and Development (2021): Encouraging Vulnerability Treatment – Overview for policy makers

3 **Vulnerability Disclosure Norm Implementation Actions Checklist**



Baseline

- Designate a Point of Contact and Coordinator
- Implement a Government Vulnerability Disclosure Policy
- Create Legal Protection and Certainty
- Drive Security Contact and Disclosure Practice Implementation
- Offer Guidance and Services

Enhanced

- Implement a Government Disclosure Decision Process
- Foster Government Vulnerability Reward Programs
- Drive Mitigation Sharing
- Improve Vulnerability Information Sharing
- Socialize the Norm Internally
- Not Introduce Vulnerabilities or Prohibit Their Reporting

Advanced

- Support Unmaintained Code
- Internationalize and Specialize Government Coordinators
- Cooperate and Build Capabilities
- Name and Shame Non-Compliance
- Curb Vulnerability Trading

4.1 Baseline Implementation

I. Point of Contact and Coordinator

Role/s: **Coordinator**
Phase/s: **Discovery; Disclosure; Verification; Preparation; Notification: Publication; Post-Processing**

Action: **Governments should establish a well-resourced point of contact to manage all phases of Coordinated Vulnerability Disclosure and act as a coordinator between government and non-government entities.**

Governments should designate a single point of contact for managing Coordinated Vulnerability Disclosure throughout all stages, from identifying vulnerabilities to publishing advisories and tracking patch deployment.[118] A cybersecurity agency or the National Computer Security Incident Response Team would be ideal choices for this role. If neither exists, the government should first establish

[118] For example, Allen D. Householder, Garret Wassermann, Art Manion, and Chris King (2017): The CERT® Guide to Coordinated Vulnerability Disclosure and NIS Cooperation Group (2023): Guidelines on Implementing National Coordinated Vulnerability Disclosure Policies

a National Computer Security Incident Response Team, which typically oversees vulnerability responses for critical infrastructure.[119]

This designated government point of contact for Coordinated Vulnerability Disclosure - going forward referred to as government coordinator - will serve as the coordinator for vulnerability disclosures, both within the government and among other stakeholders. The government coordinator's goal is to take actions that favor successful outcomes and minimize less desirable outcomes, regardless of the stage of involvement.[120] Government coordination can enhance the responsiveness of code owners[121] and may accelerate patch releases compared to non-governmental coordinated disclosure[122].

In its role as the *government-wide coordinator*, the point of contact will handle three key functions:

1. **Services and Support to Other Government Entities:** This includes assisting with the development of vulnerability disclosure policies, assessing the risks associated with vulnerabilities in their systems, and providing communication guidelines.
2. **Vulnerability Intake for All Government Entities:** If a vulnerability is discovered in government systems or code, it should be reported to the government coordinator, who will manage communication between the reporter and the affected government code or system owners.
3. **Vulnerability Reporting for Government Entities:** Upon being notified by a government entity of a vulnerability found within government code or systems, the government coordinator will reach out to the code or system owner and initiate the disclosure process, rather than the finding agency doing so, thereby leveraging the expertise and resources of the coordinator.

[119] Allen D. Householder, Garret Wassermann, Art Manion, and Chris King (2017): The CERT® Guide to Coordinated Vulnerability Disclosure

[120] Allen Householder and Jonathan Spring (2021): A State-Based Model for Multi-Party Coordinated Vulnerability Disclosure (MPCVD)

[121] ERNW (2015): ERNW Newsletter – Reflections on Vulnerability Disclosure and a Case Study

[122] Pu Li and H. Raghav Rao (2007): An examination of private intermediaries' roles in software vulnerabilities disclosure

A *government-wide coordinator* should always be the preferred option for government entities with few or no resources when it comes to handling vulnerabilities.[123] Ideally, government entities with a vast number of diverse applications and special use cases – for example, the military – should strive to handle their own vulnerability intake and manage the ensuing Coordinated Vulnerability Disclosure.

In its role as a *multi-stakeholder coordinator*, the point of contact will act as an intermediary among various government and non-government entities to ensure effective Coordinated Vulnerability Disclosures. This involves:

> 1. **Mediation Between Parties:** The coordinator will address issues such as improper communication channels between involved parties, difficulty in reproducing vulnerabilities, delays in responses, and patch development, ensuring that the disclosure process proceeds smoothly.
> 2. **Facilitating Multi-Party Disclosures:** For vulnerabilities involving multiple parties, including upstream and downstream code owners, the government coordinator will use its expertise and resources to identify affected code owners and system owners, improve communication, and reduce friction.
> 3. **Point of Contact for Vulnerabilities of National Security Relevance:** If a vulnerability could impact critical activities, safety, national security, or could cause significant harm to a country's economy or population, reporters, system owners, and code owners may involve the government coordinator to ensure appropriate handling.[124]

As trust is crucial for effective coordination, the government coordinator must have technical expertise and must be integrated into the relevant communities.[125] Proper staffing is essential to avoid becoming "a bottleneck during especially active coordination situations."[126] A lack of resources will compel a government coordinator to be selective in its involvement with vulnerability disclosures, a process known as "triage." For instance, the CERT Coordination Center (CERT/

[123] Kim Schaffer, Peter Mell, Hung Trinh, and Isabel Van Wyk (2023): NIST SP 800-216 – Recommendations for Federal Vulnerability Disclosure Guidelines

[124] Organisation for Economic Co-operation and Development (2021): Encouraging Vulnerability Treatment – Overview for policy makers

[125] Organisation for Economic Co-operation and Development (2021): Encouraging Vulnerability Treatment – Overview for policy makers

[126] Allen D. Householder, Garret Wassermann, Art Manion, and Chris King (2017): The CERT® Guide to Coordinated Vulnerability Disclosure

CC) clearly addresses this issue by stating that it "does not accept or respond to every report. We prioritize reports that affect multiple vendors or that impact safety, critical or internet infrastructure, or national security. We also prioritize reports that affect sectors that are new to vulnerability disclosure. We may be able to provide assistance for reports when the coordination process breaks down".[127]

Moreover, the CERT Coordination Center advises that vulnerability disclosure capabilities should be managed by a well-resourced team, rather than a small or single-person team, to prevent burnout.[128]

To maintain trust and manage expectations, the government coordinator should publish a policy outlining its role and functions, providing all necessary details for stakeholders to engage effectively in Coordinated Vulnerability Disclosure.[129]

States could decide to share the contact data of their Coordinated Vulnerability Disclosure National Points of Contacts and Coordinators internationally, either publicly or with other states via private channels. In the context of the latter, states could consider building upon or leveraging existing non-Coordinated-Vulnerability-Disclosure-specific initiatives, for example, the Global Intergovernmental Points of Contact Directory on the Use of Information and Communications Technologies in the Context of International Security, through which states can nominate both technical and diplomatic national points of contact.[130]

II. Government Vulnerability Disclosure Policy

Role/s: **Finder; Reporter; Code Owner; System Owner; Coordinator**
Phase/s for: **Disclosure; Verification; Preparation; Notification; Publication; Post-Processing**

Action: **Governments should adopt a comprehensive vulnerability disclosure policy to manage expectations of involved stakeholders.**

[127] Carnegie Mellon University (2024): Report a Vulnerability

[128] Allen D. Householder, Garret Wassermann, Art Manion, and Chris King (2017): The CERT® Guide to Coordinated Vulnerability Disclosure

[129] Chris Wysopal and Steve Christey (2002): Responsible Vulnerability Disclosure Process draft-christey-wysopal-vuln-disclosure-00.txt

[130] United Nations Office for Disarmament Affairs (2024): Global Intergovernmental Points of Contact Directory on the Use of Information and Communications Technologies in the Context of International Security and Samuele Dominioni (2023): Operationalizing a Directory of Points of Contact for Cyber Confidence-Building Measures. It is worth noting that Points of Contact Directories also exist at the regional level in the framework of confidence-building measures adopted within regional organizations such as the OSCE, ASEAN, or the OAS.

As a basis and framework to implement Coordinated Vulnerability Disclosure, governments need a vulnerability disclosure policy.[131] To maintain trust and manage expectations, government and non-government stakeholders should be informed about what to expect from the government coordinator before making contact. This includes details about the role and services of the government coordinator, as well as the legal framework and concrete response timelines.

The policy should include:

1. **Scope:** The policy should define the scope of applicability, ensuring stakeholders can assess whether they can approach the government coordinator with a particular request. For example, the policy should clarify whether the coordinator can be approached only by government entities (*government-wide coordinator*) or also by other stakeholders (*multi-stakeholder coordinator*).
2. **Contact:** The policy must specify whom to contact and how to do so. Ideally, government coordinators can be approached through secure communication channels that allow pseudonymous or anonymous contact. These channels should support two-way communication, enabling anonymous reporters to track the progress of their disclosures.
3. **Details:** An actionable vulnerability report requires sufficient details for the receiving entity to understand the issues. Thus, the report should include such information as the name of the code product with its version number, proof of concept (PoC) code, or instructions demonstrating how the vulnerability can be exploited, an assessment of the vulnerability's severity – for example, using the Common Vulnerability Scoring System (CVSS)[132] – and information about applicable threat models.
4. **Exclusion:** The policy should outline the conditions that lead to the exclusion of legal safe harbor protections for vulnerability reporters, such as whether the reporter has exploited the vulnerability to manipulate data.
5. **Expectations:** Reporters need to know what they can expect in return for disclosing a vulnerability to the government coordinator. This includes legal protections, confidentiality regarding both the vulnerability and the reporter, regular feedback about the process, assurance of non-use in intrusive cyber operations by government entities, legal safe harbor, public acknowledgment, and coordination of any potential public disclosure activities.

[131] For example, NIS Cooperation Group (2023): Guidelines on Implementing National Coordinated Vulnerability Disclosure Policies and Global Forum on Cyber Expertise (2017): GFCE Global Good Practices – Coordinated Vulnerability Disclosure (CVD)

[132] Dave Dugal and Dale Rich (2023): Announcing CVSS v4.0

6. **Process:** The policy should describe the entire process, emphasizing that it must be "well organised, predictable, and reliable [...], in particular with respect to the security, clarity and regularity of its communications with stakeholders."[133] Aspects such as response times should be described in as much detail as possible.

Every Coordinated Vulnerability Disclosure process initiated under this policy with government involvement should be concluded. To this end, government coordinators must have an internal policy for handling vulnerabilities in end of life code and managing a high quantity of low-severity vulnerabilities. All parties involved should be informed about the outcome and the basis for the decision. Transparent statistics about the number and details of Coordinated Vulnerability Disclosures involving the government should be regularly provided as part of good policymaking. Lastly, the entire process should be as lightweight and adaptable as possible so as not to overburden the stakeholders involved with bureaucracy and thereby deter them from using the process.

III. Legal Protection and Certainty

Role/s: **Finder; Reporter**
Phase/s: **Discovery, Disclosure**

Action: **Governments should prioritize comprehensive legal reform and protections for researchers to eliminate the legal uncertainties and repercussions that deter reporting and potentially lead to malicious use of unreported vulnerabilities.**

Governments benefit greatly when researchers and others identify vulnerabilities in code and systems and disclose their findings through Coordinated Vulnerability Disclosure. Unfortunately, reporting these vulnerabilities exposes researchers to legal action from code owners and system owners and entails criminal prosecution in many jurisdictions.[134] This legal uncertainty and the potential repercussions create a dilemma; researchers may choose not to report vulnerabilities, make full disclosure directly to the media, or, worse, sell their findings. In the latter scenario,

[133] Organisation for Economic Co-operation and Development (2021): Encouraging Vulnerability Treatment – Overview for policy makers

[134] For example, Karen Gullo (2024): Protect Good Faith Security Research Globally in Proposed UN Cybercrime Treaty and Center for Democracy and Technology (2017): "The Cyber" – Hard Questions In The World Of Computer Security Research and Mika Kerttunen and Eneken Tikk (2021): PUTTING CYBER NORMS IN PRACTICE: Implementing the UN GGE 2015 recommendations through national strategies and policies and Marietje Schaake, Lorenzo Pupillo, Afonso Ferreira, and Gianluca Varisco (2018): Software Vulnerability Disclosure in Europe — Technology, Policies and Legal Challenges and NIS Cooperation Group (2023): Guidelines on Implementing National Coordinated Vulnerability Disclosure Policies

the information could end up in the hands of criminals or mercenaries who could use it for malicious cyber activities, thereby undermining cybersecurity efforts.

To address this issue, governments need to prioritize legal protection and certainty for those who discover and report vulnerabilities, even before considering rewards for their unpaid work. Some proposed solutions include anonymous reporting mechanisms and the involvement of coordinators from either government or civil society.[135] While these measures may help individually, they are merely temporary fixes that do not address the root of the problem. Comprehensive legal reform is necessary to eliminate the significant negative incentive against investigating and reporting vulnerabilities through coordinated disclosure.[136]

Legal protection and certainty must extend into non-disclosure agreements (NDAs) signed by vulnerability reporters.[137] Sometimes companies or vulnerability reward programs require the signing of non-disclosure agreements or other documents that prohibit researchers from disclosing their findings under any circumstances to any third party without the explicit consent of the code owner or system owner with whom they signed the agreement. While the intention to protect their confidential information, security, and public image is understandable, these measures can also hinder proper vulnerability disclosure. Particularly in cases where the security of the affected product is in the public interest because it is widely used, part of critical infrastructure, and/or a critical vulnerability, it is important that the vulnerability gets remediated properly and promptly. If that is not the case, the vulnerability reporter should be legally allowed to escalate the disclosure to a government coordinator, without repercussions from the non-disclosure agreement or similar documents.

Furthermore, governments must ensure that international treaties – such as the United Nations convention against cybercrime – do not undermine their national efforts.[138] Governments need researchers to report vulnerabilities to code owners and system owners within their jurisdiction, regardless of where the researchers are located.

[135] For example, Chaos Computer Club (2024): Disclosure

[136] For details, see, for example, NIS Cooperation Group (2023): Guidelines on Implementing National Coordinated Vulnerability Disclosure Policies

[137] For example, HackerOne (2024): Clear Rules of Engagement and Bugcrowd (2022): NDA for Private Engagements

[138] For example, Karen Gullo (2024): Draft UN Cybercrime Treaty Could Make Security Research a Crime, Leading 124 Experts to Call on UN Delegates to Fix Flawed Provisions that Weaken Everyone's Security and Katitza Rodriguez (2024): The UN Cybercrime Draft Convention Remains Too Flawed to Adopt

The issue of legal uncertainty versus protection requires special attention. Governments may argue that their legal frameworks function correctly because no innocent researcher has ever been convicted for correctly reporting vulnerabilities. However, this is insufficient when considering a finder's and reporter's incentives and the potentially very narrow legal definitions of the correct investigation and reporting of vulnerabilities. Researchers may still receive threatening letters from lawyers, incur legal defense costs, and endure weeks or months of mental strain and uncertainty before a court makes a final decision. This creates a chilling effect that deters vulnerability reporting and research altogether.

IV. Security Contact and Disclosure Practice

Role/s: **Code Owner; System Owner**
Phase/s: **Disclosure**

Action: **Governments could require code owners and system owners to implement security contacts and vulnerability disclosure policies to simplify and facilitate initial contact.**

Vulnerability finders must be able to identify contact points of affected code owners and system owners with reasonable effort. The best way for code owners and system owners to facilitate this is to place contact details in an easily accessible place following existing conventions. A good way to do this is to implement the recommendations of RFC 9116; this defines a file, security.txt, that is "placed in a known location that provides information about vulnerability disclosure practices of a particular organization."[139]

For code owners and system owners to have a security.txt with integrated or linked Vulnerability Disclosure Policy is an efficient and effective way to facilitate Coordinated Vulnerability Disclosure. Yet "only about a half of a percent of the world's top one million websites publish a security.txt file"[140] and "among domains that have adopted the standard, Security.txt files are often out of date, expired, or invalid."[141] Government should therefore encourage all code owners and system owners to have up-to-date security.txt implemented in accordance with RFC 9116. For code owners and

[139] Edwin Foudil and Yakov Shafranovich (2022): A File Format to Aid in Security Vulnerability Disclosure and Tobias Hilbig, Thomas Geras, Erwin Kupris, and Thomas Schreck (2022): security.txt Revisited: Analysis of Prevalence and Conformity in 2022

[140] Sandy Radesky (2023): security.txt: A Simple File with Big Value referencing William P. Findlay and AbdelRahman Abdou (2022): Characterizing the Adoption of Security.txt Files And their Applications to Vulnerability Notification

[141] William P. Findlay and AbdelRahman Abdou (2022): Characterizing the Adoption of Security.txt Files And their Applications to Vulnerability Notification

system owners that are considered critical infrastructures under national legislation, as well as for government code owners and system owners, the government may want to consider mandating this measure instead, for example, through government procurement guidelines. Additionally, code owners should be encouraged to include links to their security contact and disclosure practice in their code and/or product.

V. Guidance and Services

Role/s: **Finder; Reporter; Code Owner; System Owner; Coordinator**
Phase/s: **Discovery; Disclosure; Verification; Preparation; Notification; Publication; Post-Processing**

Action: **Governments should leverage existing expertise and resources to offer comprehensive guidance and services to stakeholders involved in Coordinated Vulnerability Disclosure.**

Governments, through their coordinators, should provide tailored guidance and services to stakeholders to simplify the implementation and execution of Coordinated Vulnerability Disclosure.[142]

Initial Steps: Finders and reporters must have easy access to information on how to report discovered vulnerabilities. Guidance should ensure that government coordinators act as a fallback option for reporting if contact information for the affected code or system owners is unavailable or if reporters prefer to submit information directly to the government.[143]

Provision of Templates: Support should be extended to code and system owners, particularly those with limited resources or who are non-traditional code owners, in establishing security.txt files,[144] vulnerability disclosure policies, and internal vulnerability handling processes. Government coordinators could provide templates and good practices[145] to facilitate this process.

[142] For details, see NIS Cooperation Group (2023): Guidelines on Implementing National Coordinated Vulnerability Disclosure Policies

[143] Tiina Havana (2003): Communication in the Software Vulnerability Reporting Process and Mika Kerttunen and Eneken Tikk (2021): PUTTING CYBER NORMS IN PRACTICE: Implementing the UN GGE 2015 recommendations through national strategies and policies

[144] EdOverflow and Yakov Shafranovich (2024): security.txt

[145] For example, Tassilo Thieme (2021): Heureka! Von der Schwachstellenfindung bis zur Veröffentlichung: Entwicklung eines Coordinated Vulnerability Disclosure Prozesses für kleine und mittelständische IT-Unternehmen

Vulnerability Assessment Support: Accurate assessment of vulnerability severity, threat models, and impacts is critical for further vulnerability handling[146] – especially vis-à-vis an increasing number of low-severity vulnerabilities. Government coordinators should aid finders and code owners in these assessments, offering support through webinars, training, and, where appropriate, direct hands-on assistance if requested.[147]

Monitoring and Supporting Patch Adoption: Following the development of a patch, it is essential to ensure its prompt and careful deployment, as patches can reveal vital information to malicious actors.[148] Government coordinators should monitor patch adoption rates and promote awareness through supplementary advisories,[149] based on the criticality of the code and vulnerability.[150]

Common Vulnerabilities and Exposures Numbering Services: Government coordinators should consider registering as Common Vulnerabilities and Exposures Numbering Authority, enabling them to provide Common Vulnerabilities and Exposures number application services to reporters and code owners.

Guidance on Forever Day Vulnerabilities: Government coordinators should transparently outline their approach to managing forever day vulnerabilities – for which patches will never become available[151] – and provide guidance to code and system owners on handling cases where patching is extremely slow or unfeasible, such as in vehicles, processors, satellites, and similar scenarios.

Scanning for N-Day Vulnerabilities: Competent authorities could be authorized by governments to scan systems for N-day vulnerabilities, informing system owners of the findings to bolster their security measures.[152]

[146] Bart Hogeveen (2022): The UN norms of responsible state behaviour in cyberspace Guidance on implementation for Member States of ASEAN

[147] Mika Kerttunen and Eneken Tikk (2021): PUTTING CYBER NORMS IN PRACTICE: Implementing the UN GGE 2015 recommendations through national strategies and policies

[148] Kim Schaffer, Peter Mell, Hung Trinh, and Isabel Van Wyk (2023): NIST SP 800-216 – Recommendations for Federal Vulnerability Disclosure Guidelines

[149] Kim Schaffer, Peter Mell, Hung Trinh, and Isabel Van Wyk (2023): NIST SP 800-216 – Recommendations for Federal Vulnerability Disclosure Guidelines

[150] Mika Kerttunen and Eneken Tikk (2021): PUTTING CYBER NORMS IN PRACTICE: Implementing the UN GGE 2015 recommendations through national strategies and policies

[151] Allen Householder and Jonathan Spring (2021): A State-Based Model for Multi-Party Coordinated Vulnerability Disclosure (MPCVD)

[152] For example, Emma Woollacott (2019): In Run-Up To Olympics, Japan Plans To Hack Citizens' IoT Devices

4.2 Enhanced Implementation

VI. Government Disclosure Decision Process

Role/s: **Finder; Reporter**
Phase/s: **Discovery; Disclosure**

Action: **Governments could implement a process that allows temporary withholding from Coordinated Vulnerability Disclosure for vulnerabilities that are found by or reported to government entities other than cybersecurity agencies and deemed strategic assets.**

Government entities may find vulnerabilities, or receive them through reporting by other stakeholders, which they may want to temporarily retain and potentially exploit as part of their mandate.[153] This includes, for example, law enforcement agencies, the intelligence community, and the military. They will therefore not report the vulnerabilities immediately through Coordinated Vulnerability Disclosure to the code owners or system owners. Additionally, there are stakeholders such as companies peddling stalkerware, ransomware and malware developers, and military intelligence agencies of systemic rival states where it may be detrimental to cybersecurity and national security to disclose vulnerabilities to their system owner or code owner. Therefore, states need a policy on how to deal with vulnerabilities in these instances. Such a policy is known as a "Vulnerabilities Equities Process", "Equities Process", "Government Disclosure Decision Process" or "Government Vulnerability Disclosure," and has been implemented by several countries.[154]

Getting a Government Disclosure Decision Process right is no easy feat as it requires a nuanced multi-stakeholder approach, managing a variety of interests. The author of this paper outlined a possible blueprint for a Government Disclosure

[153] Organisation for Economic Co-operation and Development (2021): Encouraging Vulnerability Treatment – Overview for policy makers

[154] Sven Herpig and Ari Schwartz (2019): The Future of Vulnerabilities Equities Processes Around the World and The White House (2017): Vulnerabilities Equities Policy and Process for the United States Government and Marietje Schaake, Lorenzo Pupillo, Afonso Ferreira, and Gianluca Varisco (2018): Software Vulnerability Disclosure in Europe — Technology, Policies and Legal Challenges and Nathaniel Fick, Jami Miscik, Adam Segal, and Gordon M. Goldstein (2022): Confronting Reality in Cyberspace — Foreign Policy for a Fragmented Internet and Government Communications Headquarters (2024): The Equities Process and Australian Signals Directorate (2024): Responsible Release Principles for Cyber Security Vulnerabilities and Communications Security Establishment (2024): CSE's Equities Management Framework

Decision Process in a 2018 study.[155] While a Government Disclosure Decision Process is not part of the Coordinated Vulnerability Disclosure process,[156] there is one key intersection. National Computer Security Incident Response Teams and similar stakeholders should funnel all their found and received vulnerabilities immediately and exclusively through Coordinated Vulnerability Disclosure and not a Government Disclosure Decision Process to avoid increasing the trust deficit between them and non-government stakeholders. In other words:[157]

> "Governments need to ensure that agencies and processes can be trusted by stakeholders. Government agencies which may receive vulnerability information, for example in a co-ordinator capacity or as a regulatory body, should provide assurance that vulnerability information will only be shared with or accessed by the vulnerability owner (i.e. who can fix the vulnerability) and not with any other party, including those who could stockpile it or use it for offensive purposes."

In this way, finders who want to leverage a government coordinator in a Coordinated Vulnerability Disclosure can be assured that these vulnerabilities will be handled appropriately to increase cybersecurity and not end up as a strategic asset for security agencies or the military. The latter can always be achieved by the finders reporting their vulnerabilities directly to a security agency or the military.

Government disclosure decision processes are designed in such a way that vulnerability assessments will lead either directly to Coordinated Vulnerability Disclosure or will do so after a period of temporary retention and possibly exploitation. Either way, these vulnerabilities will eventually reach Coordinated Vulnerability Disclosure, offering an improvement to the alternative of government entities not reporting their strategic assets at all.

[155] For a government-independent policy blueprint, see Sven Herpig (2018): Governmental Vulnerability Assessment and Management — Weighing Temporary Retention versus Immediate Disclosure of 0-Day Vulnerabilities

[156] In Allen Householder and Jonathan Spring (2021): A State-Based Model for Multi-Party Coordinated Vulnerability Disclosure (MPCVD) the authors describe this in this way: "for each vulnerability that enters the process, the VEP results in a decision to disseminate or restrict the information. [...] VEP policy does not explicitly touch on any other aspect of the CVD process. By solely addressing [vendor is aware of vuln], VEP is mute regarding intentionally triggering the [public is aware of vulnerability] or [exploit has been made public] transitions. It also makes no commitments about [fix is ready] or [fix is deployed], although obviously these are entirely dependent on [vendor is aware of vuln] having occurred. However, preserving the opportunity to exploit the vulnerability implies a chance that such use would be observed by others, thereby resulting in the [attacks have been observed] transition."

[157] Organisation for Economic Co-operation and Development (2021): Encouraging Vulnerability Treatment – Overview for policy makers

VII. Government Vulnerability Reward Programs

Role/s: **Finder; Reporter; Code Owner; System Owner; Coordinator**
Phase/s: **Discovery; Disclosure**

Action: **Governments could promote the establishment of Vulnerability Reward Programs by selected government entities to enhance reporting incentives.**

Government entities should be encouraged to set up Vulnerability Reward Programs either separately or through their *government-wide coordinator*. Reporters are likely to disclose vulnerabilities to government code owners and system owners due to intrinsic motivation, and government entities should offer some kind of reward as an additional incentive. This can be through recognition in communities and acknowledgments,[158] non-purchasable products,[159] or monetary compensation[160].

The Vulnerability Rewards Program should be integrated into or based on a Vulnerability Disclosure Policy to manage expectations. This is crucial because "even though vulnerability reward programs are generally perceived as a positive development that has brought discoverers and vendors closer together, the market must be approached with caution as it can over-incentivise the search and lead to a flood of vulnerabilities, potentially diverting attention and resources away from the most critical challenges."[161]

Governments could provide their entities with guidelines on how to implement reward programs, a centralized "Hall of Fame", or dedicated financial resources, either for monetary compensation or to procure and offer special products.

[158] For example, Bundeswehr (2020): Vulnerability Disclosure Policy der Bundeswehr

[159] For example, Veshraj Ghimire (2021): Hacking Dutch Government For a lousy T-shirt

[160] For example, Government Technology Agency of Singapore (2024): Factsheet about Government Crowdsourced Vulnerability Discovery Programmes

[161] ENISA (2016): Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations

VIII. Mitigation Sharing

Role/s: **Code Owner; System Owner; Coordinator**
Phase/s: **Preparation; Notification; Publication; Post-Processing**

Action: **Governments should improve both private and public sharing of vulnerability mitigations by establishing secure information sharing networks and encouraging the public release of mitigations for high-risk and forever day vulnerabilities.**

For scenarios when the development of a patch is not (immediately) possible, The CERT® Guide to Coordinated Vulnerability Disclosure suggests mitigations as a stopgap in scenarios where it may not [be] possible to develop a timely fix, a vendor or third party will sometimes provide advice on actions that can be taken to mitigate the effects of the vulnerability. Sometimes this advice is as simple as instructions for disabling the affected features of the system. In other cases, mitigation advice might include detailed configuration changes to be made by deployers. However, in nearly all cases a full fix for the vulnerability is preferable to mitigation advice, which should at best be treated as a temporary solution to the problem."[162] Additionally, "a temporary or intermediary remediation that consists of a mitigation or workaround can be necessary in cases when a vulnerability poses a high risk to users. A non-comprehensive remediation that works in most scenarios can also be necessary in high-risk circumstances."[163] However, so far it has been uncommon for mitigation methods for reported vulnerabilities to be shared more broadly or publicly before a patch is released – even if such mitigation methods exist.

Various reasons are given for not actively promoting public mitigation sharing despite their obvious use cases. These reasons include not wanting to alert criminals or adversarial nation state actors to the existence of a vulnerability before a patch is ready, sharing mitigations only privately with customers as part of contracts or the concern that system owners may ignore the subsequent patch if they have already applied mitigation methods. Additionally, mitigations may be based on classified information – both by industry and government – or are classified themselves, making government entities "reluctant to share information into the public collection."[164] In some instances, government entities cannot

[162] Allen D. Householder, Garret Wassermann, Art Manion, and Chris King (2017): The CERT® Guide to Coordinated Vulnerability Disclosure

[163] ISO (2019): ISO/IEC 30111:2019 — Information technology — Security techniques — Vulnerability handling processes

[164] Office of the Director of National Intelligence (2023): Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015

even share information with each other because “[defensive measures] obtained from classified sources could not be ingested and utilized to mitigate risks on unclassified systems because agencies lacked a capability to transfer them to unclassified environments [...] or lacked appropriate facility security clearance to receive the information.”[165] While these concerns are understandable, the failure to widely share known mitigation methods for reported vulnerabilities without an available patch limits the agency of system owners.

Mitigations shared by cybersecurity agencies,[166] code owners, and third parties[167] empower system owners, enabling them to conduct risk assessments and positively impact overall cybersecurity – especially when vulnerabilities are already actively exploited or, in the case of forever day vulnerabilities, sharing mitigation methods widely may be the only viable option.

Moreover, the increasing use of machine-learning enabled systems may necessitate the rethinking of the current practice of limited mitigation sharing.[168] Vulnerabilities in these systems are often addressed using guardrails and similar methods, which are akin to mitigation, rather than retraining or making models forget these vulnerabilities, which is similar to traditional patching and poses challenges for code owners.

Thus, governments should enhance both non-public and public sharing of mitigation methods. For wider non-public sharing, governments could collaborate with industry to create sharing circles of government and non-government entities and enable them to ingest information classified under the Traffic Light Protocol (TLP).[169] Governments should encourage code owners and other stakeholders to share mitigations through these channels. At the same time, they should consider reviewing mitigations shared under the Traffic Light Protocol to determine whether a stripped-down version could be disclosed to the public. Furthermore, public sharing of mitigations should be the default for forever day vulnerabilities and those already actively exploited, including Indicators of Compromise (IOCs).

[165] Office of the Director of National Intelligence (2023): Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015

[166] For example, Cybersecurity & Infrastructure Security Agency (2021): Mitigate Microsoft Exchange Server Vulnerabilities

[167] For example, HiSolutions (2021): HAFNIUM – SELF-HELP GUIDE

[168] For an overview, see Sven Herpig (2020): Understanding the Security Implications of the Machine-Learning Supply Chain

[169] Forum of Incident Response and Security Teams (2022): TRAFFIC LIGHT PROTOCOL (TLP) — FIRST Standards Definitions and Usage Guidance — Version 2.0

IX. Vulnerability Information Sharing

Role/s: **Reporter; Code Owner; System Owner; Coordinator**
Phase/s: **Verification; Preparation; Notification; Publication**

Action: **Governments should create information sharing channels and could support existing information sharing programs to enhance vulnerability assessment, risk management and remediation identification.**

First off, a government point of contact could set up secure threat intelligence-sharing communication channels on vulnerability information with other government agencies, relevant threat intelligence stakeholders, for example, from industry, and with international government contacts.

With the rising number of vulnerabilities in complex supply chains, programs offering better insights into these vulnerabilities and the impacted code stacks are essential for effective risk management and identifying necessary remediations. Therefore, governments may consider leveraging, participating in, and supporting existing initiatives (listed alphabetically below).

> **Common Platform Enumeration (CPE)**: "CPE is a structured naming scheme for information technology systems, software, and packages. Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name."[170] It is hosted and maintained by the United States National Institute of Standards and Technology (NIST).
>
> **Common Security Advisory Framework (CSAF)**: "Common Security Advisory Framework (CSAF) is a language to exchange Security Advisories. It plays a crucial role in the cybersecurity arena since it allows stakeholders to automate the creation and consumption of security vulnerability information and remediation."[171] The development is driven by Germany's Federal Office for Information Security (BSI).
>
> **Common Vulnerabilities and Exposures (CVE Program)**: "The mission of the CVE® Program is to identify, define, and catalog publicly

[170] National Institute of Standards and Technology (2023): Official Common Platform Enumeration (CPE) Dictionary

[171] OASIS CSAF TC (2023): Common Security Advisory Framework (CSAF)

disclosed cybersecurity vulnerabilities. There is one CVE Record for each vulnerability in the catalog. The vulnerabilities are discovered then assigned and published by organizations from around the world that have partnered with the CVE Program."[172] The program is run by the MITRE Corporation and supported by the United States Cybersecurity and Infrastructure Security Agency (CISA).

Common Vulnerability Scoring System (CVSS): "The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes."[173] The Common Vulnerability Scoring System is developed and maintained by the Forum of Incident Response and Security Teams.

Common Weakness Enumeration (CWE): "CWE is a community-developed list of common software and hardware weakness types that could have security ramifications. [...] The CWE List and associated taxonomies and classification schemes serve as a language that can be used to identify and describe these weaknesses in terms of 'CWEs'".[174] It is sponsored by the United States Department of Homeland Security (DHS) and the United States Cybersecurity and Infrastructure Security Agency and managed by the Homeland Security Systems Engineering and Development Institute (HSSEDI), which is operated by The MITRE Corporation.

Exploit Prediction Scoring System (EPSS): "The Exploit Prediction Scoring System (EPSS) is a data-driven effort for estimating the likelihood (probability) that a software vulnerability will be exploited in the wild."[175] It is developed and maintained by the Forum of Incident Response and Security Teams.

Software Bill of Materials (SBOM): "An SBOM is a nested inventory, a list of ingredients that make up software components."[176] Efforts are currently advanced by the United States Cybersecurity and Infrastructure Security Agency.

[172] The MITRE Corporation (2024): About the CVE Program

[173] Forum of Incident Response and Security Teams (2024): Common Vulnerability Scoring System SIG

[174] The MITRE Corporation (2024): Common Weakness Enumeration

[175] Forum of Incident Response and Security Teams (2023): EPSS – Exploit Prediction Scoring System

[176] Cybersecurity and Infrastructure Security Agency (2024): Software Bill of Materials (SBOM)

> **Stakeholder-Specific Vulnerability Categorization (SSVC)**: "[...] a vulnerability analysis methodology that accounts for a vulnerability's exploitation status, impacts to safety, and prevalence of the affected product in a singular system."[177] It was developed by Carnegie Mellon University's Software Engineering Institute (SEI) in cooperation with the United States Cybersecurity and Infrastructure Security Agency.
>
> **Vulnerability Exploitability eXchange (VEX)**: "A VEX document is an attestation, a form of a security advisory that indicates whether a product or products are affected by a known vulnerability or vulnerabilities."[178] The development was led by the United States National Telecommunications and Information Administration (NTIA).
>
> **Vultron**: "A formal protocol specification for Multi-Party Coordinated Vulnerability Disclosure (MPCVD) with the goal of improving the interoperability of both CVD and MPCVD processes."[179] The Vultron protocol is spearheaded by Allen D. Householder at Carnegie Mellon University's Software Engineering Institute.

Special attention should be given to vulnerability databases, such as the National Vulnerability Database (NVD)[180] run by the US National Institute of Standards and Technology (NIST) and based on the Common Vulnerabilities and Exposures database. The National Vulnerability Database "serves as a repository and distribution point for software and hardware flaws that can compromise computer security. It is arguably the world's most widely used vulnerability database."[181] A machine-readable, searchable, API-offering centralized distribution point of enriched vulnerability information is a great asset for code owners and system owners alike.[182] Unfortunately, in 2024 the National Vulnerability Database was

[177] Cybersecurity & Infrastructure Security Agency (2024): Stakeholder-Specific Vulnerability Categorization (SSVC)

[178] Cybersecurity and Infrastructure Security Agency (2024): Software Bill of Materials (SBOM) and for additional information, see National Telecommunications and Information Administration (2021): Vulnerability-Exploitability eXchange (VEX) – An Overview

[179] Allen D. Householder (2022): Designing Vultron: A Protocol for Multi-Party Coordinated Vulnerability Disclosure (MPCVD) and Allen D. Householder (2022): Vultron: A Protocol for Coordinated Vulnerability Disclosure

[180] National Institute of Standards and Technology (2024): National Vulnerability Database

[181] Hacking Policy Council (2024): Transformative changes needed for vulnerability infrastructure and the National Vulnerability Database

[182] Hacking Policy Council (2024): Transformative changes needed for vulnerability infrastructure and the National Vulnerability Database and Ben Edwards (2024): Evaluating dependence on NVD

not able to keep up with its work for several months, creating a large backlog.[183] This illustrates the number of resources needed to keep an asset that relies on manual assessments running for the benefit of all. Working with several vulnerability databases will require governments to also invest in supporting coordination efforts for vulnerability IDs across databases.[184]

Governments may want to consider supporting existing vulnerability databases, such as the Common Vulnerabilities and Exposures database, the National Vulnerability Database or Japan Vulnerability Notes (JVN),[185] run by JPCERT/CC and IT Promotion Agency (IPA), instead of developing new ones.[186] If governments want to set up their own separate vulnerability databases, syncing them with existing databases, using established file and exchange formats and working with and toward unique vulnerability identifiers would be an efficient way of doing so.

A first step for the cybersecurity agency or Computer Security Incident Response Teams to get involved could be to become a Common Vulnerabilities and Exposures Numbering Authority[187] and provide high quality Common Vulnerabilities and Exposures to the database. Additionally, efforts such as the Cybersecurity & Infrastructure Security Agency's Vulnrichment program could be supported.[188] As a Common Vulnerabilities and Exposures Numbering Authority, governments can also assist researchers and code owners, such as open source projects, in acquiring Common Vulnerabilities and Exposures numbers, in resorting disputes, and in further developing good practices and norms.

Establishing a vulnerability database as part of a "UN-run repository"[189] or "Global Cyber Security Cooperation Portal,"[190] in which several member states have conveyed interest over the years, does not seem feasible. Such a database would

[183] Patrick Garrity (2024): The Real Danger Lurking in the NVD Backlog and Chris Hughes (2024): Death Knell of the NVD?

[184] Allen D. Householder, Garret Wassermann, Art Manion, and Chris King (2017): The CERT® Guide to Coordinated Vulnerability Disclosure

[185] JPCERT/CC and IPA (2024): JVN Japan Vulnerability Notes

[186] Alexander Martin (2024): EU cyber agency will not create active vulnerability database, says chief cybersecurity officer

[187] The MITRE Corporation (2024): CVE Numbering Authorities (CNAs)

[188] Eduard Kovacs (2024): CISA Announces CVE Enrichment Project 'Vulnrichment' and Ben Edwards (2024): Evaluating dependence on NVD

[189] Government of Kenya (2023): DRAFT WORKING PAPER ON THE ESTABLISHMENT OF A THREAT REPOSITORY WITHIN THE UNITED NATIONS

[190] Indian Ministry of External Affairs (2022): GLOBAL CYBER SECURITY COOPERATION PORTAL – CONCEPT NOTE

require a vast amount of staffing, technical expertise, and financial resources. A simple secretariat would not be able to handle it. Therefore, member states may want to work together with others that have already set up such vulnerability information sharing infrastructures or set up one in regional cooperation within a host country.

X. Internal Norm-Socialization

Role/s: **Finder; Reporter; Code Owner; System Owner; Coordinator**
Phase/s: **Discovery; Disclosure**

Action: **Governments could socialize the vulnerability disclosure norm nationally.**

It is crucial for governments to raise awareness and highlight the relevance of this norm among all relevant stakeholders within their jurisdiction, starting with a government's own security authorities – such as national cybersecurity agencies or intelligence agencies – to ensure comprehensive understanding and engagement across various sectors. Ultimately, implementing the disclosure norm could be a whole-of-government approach that is streamlined in all relevant areas of government action.

A starting point could be for the Ministry of Foreign Affairs – or whichever agency represented its government during the relevant United Nations debates – to provide all relevant government stakeholders with a publication that summarizes the relevance of cyber norms and each individual norm in the national language. Additionally, government agencies could be asked to map those of their tasks that contribute to the implementation of those norms.

XI. No Government-Introduced Vulnerabilities

Role/s: **Reporter; Code Owner**
Phase/s: **Discovery; Disclosure**

Action: **Governments should not introduce additional vulnerabilities to code or prohibit stakeholders from reporting them.**

Governments should not encourage code owners to change their code in any area that could result in the code being less secure. Designing and developing secure code is sufficiently difficult without also accommodating government requests that may affect the security of the code (e.g., by building law enforcement access mechanisms into the code). Asking code owners to (systematically) change their code in those areas would likely result in less secure code. Ultimately, it would decrease global cybersecurity.

Concrete examples of what governments should not do include legislation mandating code owners to introduce lawful access mechanisms,[191] intentionally promoting weak cryptographic algorithms,[192] running companies selling intentionally-backdoored code to non-criminal entities,[193] or requiring code owners of security software to whitelist government-developed malicious software.[194]

Additionally, governments should not prohibit stakeholders from reporting vulnerabilities to code owners, regardless of whether government agencies have planted those vulnerabilities or mandated code owners or others to integrate the vulnerabilities in the code or not.[195]

4.3 Advanced Implementation

XII. Unmaintained Code

Role/s: **Code Owner; Coordinator**
Phase/s: **Disclosure; Verification; Preparation; Notification; Publication; Post-Processing**

Action: **Governments should support vulnerable end of life or abandoned code to address the risk stemming from potential forever day vulnerabilities.**

There are various reasons leading to code owners not preparing and publishing a mitigation or patch. Along with lack of capacity and capabilities or unwillingness to work on a remediation, the primary reason is that the affected code products

[191] For example, Meredith Whittaker (2023): Standing firm against threats to private and safe communication and Sven Herpig (2022): Recht auf Verschlüsselung – nur mit Abhörschnittstelle?

[192] For example, Nadiya Kostyuk and Susan Landau (2022): Dueling over Dual_EC_DRGB: The Consequences of Corrupting a Cryptographic Standardization Process

[193] For example, Joseph Cox (2024): Dark Wire – The Incredible True Story of the Largest Sting Operation Ever and Ulrich Stoll und Peter F. Müller (2023): Crypto AG: Wie BND & CIA die Welt belauschten

[194] Mathew J. Schwartz (2013): Do Antivirus Companies Whitelist NSA Malware?

[195] See the debate around Google’s action taking down a counter-terrorism operation: Patrick Howell O’Neill (2021): Google’s top security teams unilaterally shut down a counterterrorism operation and Ivan (2024): The case for burning counterterrorism operations

are no longer supported, either because they have reached end of life or have been abandoned.[196]

To mitigate the possible impact of the resulting forever day vulnerabilities, governments "should offer guidelines for software recycling and responsible sunsetting,"[197] point toward existing platforms, such as adopt-a-package initiatives and end-of-life platforms, and inform downstream code owners about end-of-life dependencies.[198]

However, in rare cases, forever day vulnerabilities may potentially exist in code that is deemed high priority for the government – for example, because it is used in a government or critical infrastructure software stack. For those cases, governments may want to consider providing funding for the ongoing maintenance of code, assuming temporary responsibility and commissioning mitigation[199] or patch development – including rewrites or forks for open source software[200] – to third parties. Prerequisites for code changes to unmaintained code – patches and mitigations alike – is that the source code is available and that there is a secure automatic mechanism for security updates. However, the latter is challenging, as sensitive information (for example, keys for signing the update) would have to be stored in advance with a trusted entity. Otherwise, there may be an updated version of the code, but it remains the responsibility of the end users to be aware of it and apply it.[201]

XIII. Specialized International Government Coordinators

Role/s: **Reporter; Coordinator**
Phase/s: **Discovery; Disclosure; Verification; Preparation; Notification; Publication; Post-Processing**

Action: **Governments should be accessible to international stakeholders and could leverage international cooperation for further specialization of actions and services.**

[196] Sven Herpig (2024): Was kommt nach dem Ende des Lebenszyklus?

[197] Sven Herpig (2023): Fostering Open Source Software Security — Blueprint for a Government Cybersecurity Open Source Program Office

[198] Sven Herpig (2023): Fostering Open Source Software Security — Blueprint for a Government Cybersecurity Open Source Program Office

[199] For an example of third party mitigation development, see Hive Pro (2022): Microsoft's privilege escalation vulnerability that refuses to go away

[200] Sven Herpig (2023): Fostering Open Source Software Security — Blueprint for a Government Cybersecurity Open Source Program Office

[201] Sven Herpig (2024): Was kommt nach dem Ende des Lebenszyklus?

Governments' actions should be inclusive and their services broadly accessible to international stakeholders when it comes to enhancing Coordinated Vulnerability Disclosures. Thus, governments should strive to offer their services in English and possibly other official United Nations languages in addition to their own national language(s). Clearly indicating the individual governments' languages and scope enables government coordinators to take in vulnerability reports for international reporters and coordinate among their counterparts in other countries and international stakeholders. Additionally, reporters to governments without their own national government coordinator would have a place to turn to, as "in many cases, the nationality of the co-ordinator does not matter, as long as it is trusted by stakeholders."[202]

International accessibility allows government coordinators to specialize. Thus, the government coordinator of one country could specialize in the assessment and coordination of vulnerabilities in industrial control system (ICS) code while another could specialize in vulnerabilities in machine learning (ML) code, and so on. Organizations such as the European Union Agency for Cybersecurity or the Open CSIRT Foundation could help bring awareness to such a network of competent (government) coordinators that specializes in certain areas and topics of Coordinated Vulnerability Disclosure.

XIV. Capability Building and Cooperation

Role/s: **Finder; Reporter; Code Owner; System Owner; Coordinator**
Phase/s: **Discovery; Disclosure; Verification; Preparation; Notification; Publication; Post-Processing**

Action: **Governments could enhance each other's capabilities and cooperate on day-to-day norm implementation depending on their level of alignment.**

Governments can gain from other governments' abilities to coordinate vulnerability disclosures, as the underlying vulnerabilities may also impact code owners and system owners in their own jurisdictions. National counterparts facilitate cross-jurisdictional cooperation, strengthening the government administration's self-interest to assist in building each other's capabilities for Coordinated Vulnerability Disclosure. This capability building and international cooperation can be scaled based on the level of alignment in matters of security and defense policies between states:

[202] Organisation for Economic Co-operation and Development (2021): Encouraging Vulnerability Treatment – Overview for policy makers

Loosely Aligned: Governments connect their I. Points of Contact, share best practices and templates, exchange data on vulnerabilities and related information about system owners and code owners. They may also avail themselves of each other's V. Guidance and Services and IX. Vulnerability Information Sharing infrastructure.

Aligned: Governments share skill sets and tools, facilitate expert exchanges, engage in sensitive sharing of mitigations to a certain extent, and draft joint advisories and cooperate on international aspects of the vulnerability disclosure norm implementation, for example, on instruments such as III. Legal Protection and Certainty, XV. Non-Compliance naming and shaming, or curbing the XVI. Vulnerability Trading.

Closely Aligned: Governments cooperate closely on sharing classified vulnerability information and mitigations in critical areas such as infrastructures or government systems. They also collaborate on sensitive national implementations of the vulnerability disclosure norm, such as VI. Government Disclosure Decision Processes or IX. Vulnerability Information Sharing infrastructures, and may allow vulnerability intake for each other's government code owners and system owners when special expertise or lack of resources necessitates it.

XV. Non-Compliance

Role/s: **Code Owner; System Owner**
Phase/s: **Disclosure; Verification; Preparation; Notification; Publication; Post-Processing**

Action: **Governments could resort to publicly naming and shaming code owners and system owners that repeatedly neglect their responsibilities.**

Code owners and system owners have long been a weak link in the Coordinated Vulnerability Disclosure process, often due to unclear contact instructions, inadequate vulnerability policies, mishandled communications, and ineffective or problematic remediation efforts.

Governments may need to adopt a strategy of publicly naming and shaming those code and system owners who repeatedly neglect their responsibilities in the Coordinated Vulnerability Disclosure process. This may lead to negative incentives for code owners and system owners who neglect their responsibility and thereby strengthen the implementation of actions in line with the vulnerability disclosure norm.

An example of a “naming and shaming” practice at the international level would be the PWNIE Awards.[203] Naming and shaming can be implemented directly at the national level through an existing or dedicated platform, or indirectly, for example, through product warnings by stakeholders such as Germany’s Federal Office for Information Security[204] or through a public report of an investigation by an entity such as the US Cyber Safety Review Board.[205] International cooperation could borrow from existing efforts in other domains, such as global finance governance.[206]

XVI. Vulnerability Trading

Role/s: **Finder**
Phase/s: **Disclosure**

Action: **Governments could consider banning the trade of selected vulnerabilities and pursue international agreements in this regard.**

Entities that offer compensation for vulnerabilities without channeling them into Coordinated Vulnerability Disclosure - going forward referred to as vulnerability trading - create negative incentives for finders to report vulnerabilities properly, leading to companies or governments using these vulnerabilities in intrusive tools that harm cybersecurity.

To counter this, governments could make trading of selected vulnerabilities illegal within their jurisdictions and collaborate with other nations on international agreements to ban this practice. Governments with an established Government Disclosure Decision Process already possess an approach to identifying vulnerabilities that should be disclosed immediately rather than temporarily retained. They may wish to apply this same framework to categorizing vulnerabilities whose proliferation through trading they seek to limit.

By doing so, governments can harmonize their national policies, implement the vulnerability disclosure norm, and consider the requirements of law enforcement, intelligence, and military sectors.

[203] Pwnie Awards (2024): Pwnies

[204] Federal Office for Information Security (2024): Archive of Past BSI Warnings Issued Pursuant to Section 7 of the BSIG

[205] For example, Sven Herpig (2024): Cyber Safety Review for Webex-Vulnerability Handling?

[206] For example, Aija Rusina (2020): Name and shame? Evidence from the European Union tax haven blacklist

Enforcement efforts should target the purchasing entities rather than the finders selling vulnerabilities. While it may be easier to pursue individual security researchers selling their vulnerabilities, this would be neither an efficient nor an effective approach.

While international efforts are on the way to focusing on outlawing vulnerabilities in commercial cyber intrusion capabilities, this may be too shortsighted for improving global cybersecurity.[207]

[207] Sven Herpig and Alexandra Paulus (2024): The Pall Mall Process on Cyber Intrusion Capabilities

5. Sharing Implementation Efforts

States implementing the vulnerability disclosure norm may consider sharing their experiences and practices with other states.[208] Such sharing not only reinforces political commitment but also serves to **highlight national achievements and build mutual confidence among states**, potentially extending to the broader international community. On a systemic level, concrete examples of how states interpret and implement the United Nations cyber norms can enhance collective understanding, shaping the norms' meaning and scope. This is critical since the "success of a norm rests not just in what it says, but in who accepts it, not to mention where, when, and how they do so," considering norms' "inherently dynamic nature".[209] Sharing implementation efforts can thus function as **a strategic tool for promoting norm acceptance and inspiring other states** to take similar, or even coordinated, actions. Nonetheless, given that the norms are voluntary and non-binding, the decision to participate in such activities and allocate resources is entirely at a state's discretion.

Before sharing implementation efforts, a **systematic mapping exercise regarding the ongoing efforts is essential**. Governments need to identify, assess, and possibly track their implementation activities, such as those related to the vulnerability disclosure norm, using tools[210] like a A. Checklist. While the mapping process requires coordination across multiple governmental entities, Ministries of Foreign Affairs are generally best suited to handle international sharing efforts – whether through public engagement or private channels. Publicizing these efforts also allows for tailored feedback from various stakeholders.[211]

[208] Such activities can also contribute to a behavior called "norm entrepreneurship" in International Relations literature; see Martha Finnemore and Kathryn Sikkink (2005): International Norm Dynamics and Political Change.

[209] Martha Finnemore and Duncan B. Hollis (2017): Constructing Norms for Global Cybersecurity

[210] The United Nations Institute for Disarmament Research (2024): National Survey of Implementation of United Nations recommendations on responsible use of ICTs by states in the context of international security can guide states' review of their norm implementation efforts. Governments may also decide to commission third parties to assess their state of implementation. For instance, the Australian Strategic Policy Institute has produced reports on the implementation of the United Nations cyber norms for Vietnam, the Philippines, Malaysia and Indonesia; see Bart Hogeveen (2022): The UN norms of responsible state behaviour in cyberspace.

[211] Stiftung Neue Verantwortung (2022): The Role of Norms Implementation in Strengthening the Framework of Responsible State Behavior in Cyberspace – Submission to the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025 (OEWG)

States may therefore opt to make their implementation efforts publicly available by responding to surveys like those displayed on the United Nations Institute for Disarmament Research Cyber Policy Portal,[212] issuing national reports on their adherence to United Nations cyber norms, or collaborating on like-minded papers addressing specific norms. To date, only Czechia has publicized its answers to the norms implementation survey,[213] a few states – Australia,[214] Canada,[215] South Korea,[216] and the United Kingdom[217] – have published papers on their national implementation, with a cross-regional paper on the due diligence norm (norm c) being the only collaborative initiative in this area.[218] States may also communicate their approaches in multilateral fora, either during live-streamed interventions or through available meeting records, such as in the United Nations Open-ended Working Group[219] or cybercrime-related discussions or negotiations.[220] They may also include such efforts in contributions to the UN Secretary-General's report[221] or relevant national documents, such as evaluations of cybersecurity strategies.

Conversely, states have the option to share details of their implementation efforts with other states through private channels. This information exchange can occur informally during multilateral forums or in discussions related to vulnerability disclosure, such as those held by the United Nations Open-ended Working Group,

[212] United Nations Institute for Disarmament Research (2024): Cyber Policy Portal

[213] United Nations Cyber Policy Portal (2024): Czechia

[214] Australian Department of Foreign Affairs and Trade (2020): Australian Implementation of Norms of Responsible State Behaviour in Cyberspace

[215] Government of Canada (2019): Canada's implementation of the 2015 GGE norms

[216] Republic of Korea (2020): Implementation of the 2015 UNGGE Norms

[217] United Kingdom Foreign & Commonwealth Office (2019): Non-Paper on Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015

[218] Governments of Belgium, Czech Republic, Estonia, Finland, France, Germany, Ireland, Italy, Latvia, Portugal, Slovakia, and Spain (2024): Multiple States' views on best practices relating to the implementation of norm 13(c)

[219] For example, French Representative (2024): (2nd meeting) Open-ended working group on Information and Communication Technology (ICT) - Seventh Substantive Session and Representative of the United Kingdom (2024): (2nd meeting) Open-ended working group on Information and Communication Technology (ICT) - Seventh Substantive Session

[220] The United Nations Office on Drugs and Crime (2024): Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes could have been a venue to address legal risks and uncertainty for security researchers within the framework of Coordinated Vulnerability Disclosure, thereby enabling a more effective implementation of the vulnerability disclosure norm.

[221] United Nations Office for Disarmament Affairs (2024): Developments in the field of information and telecommunications in the context of international security

the Group of Seven,[222] or within the context of bilateral or like-minded cyber consultations focusing on norm implementation. As acknowledged by all UN member states, “regional and sub-regional organizations [...] play an important role in implementing the framework for responsible State behaviour in the use of ICTs,”[223] making these organizations particularly effective channels for sharing implementation strategies. Several of these organizations have also explicitly endorsed the UN cyber norms in the past.[224] The sharing of implementation practices can involve placing vulnerability disclosure on the agendas of regular regional meetings, for instance, in the framework of the European Union, the Organization for Security and Co-operation in Europe, the Organisation for Economic Co-operation and Development,[225] the Association of Southeast Asian Nations Regional Forum, or the Organization of American States, as well as organizing dedicated workshops,[226] creating regional norms implementation checklists and/or overviews,[227] and **making use of channels provided for in the context of implementing regionally agreed confidence-building measures (CBMs)**. The elevation of Coordinated Vulnerability Disclosure as a dedicated confidence-building measure within the Organization for Security and Co-operation in Europe’s Participating States,[228,229] as well as its consideration as a

[222] For example, Group of Seven (2016): G7 Principles and Actions on Cyber and Group of Seven (2017): G7 Declaration on Responsible State Behavior in Cyberspace and Group of Seven (2019): Cyber Norm Initiative – Synthesis of Lessons Learned and Best Practices

[223] For example, United Nations (2023): Developments in the field of information and telecommunications in the context of international security (A/78/265)

[224] Camino Kavanagh (2019): New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?

[225] Organisation for Economic Co-operation and Development (2023): Good Practice Guidance on the Co-ordination of Digital Security Vulnerabilities

[226] For example, Cybil Portal (2024): Norms Implementation Checklist Workshops and Organization for Security and Co-operation in Europe (2023): OSCE gathers experts to discuss coordinated vulnerability disclosure, one of the cyber/ICT security confidence-building measures

[227] For example, Association of Southeast Asian Nations (2022): ASEAN CYBERSECURITY COOPERATION STRATEGY (2021 - 2025) – DRAFT

[228] Organization for Security and Co-operation in Europe (undated): OSCE cyber/ICT security CBM 16: Coordinated Vulnerability Disclosure.

[229] The Organization for Security and Co-operation in Europe (OSCE) established the “Adopt-a-CBM” initiative, inviting OSCE Participating States to “champion the implementation of specific CBMs [... by] explor[ing] concrete modalities for achieving national- and regional-level CBM implementation”; see Organization for Security and Co-operation in Europe (2023): 10 Years of Cyber/ICT Security Confidence-Building Measures. For CBM 16 on Coordinated Vulnerability Disclosure, this function is assumed by the Netherlands together “with the OSCE Secretariat and a number of States,” and has culminated, for instance, in the development of a respective e-learning course; see Argentina, Australia, Brazil, Canada, Chile, Colombia, Czech Republic, Fiji, Germany, Israel, Republic of Korea, Mexico, The Netherlands, Singapore, Uruguay (2023): Working paper on Cyber Confidence-Building Measures in Action.

global confidence-building measure within the Open-ended Working Group,[230] exemplifies such initiatives.

States may also integrate best practice sharing into capacity-building activities, especially those aimed at developing or enhancing the capabilities of National Computer Security Incident Response Teams, which may act as focal points for Coordinated Vulnerability Disclosure. Embedding these discussions into training programs, workshops,[231] side events, or fellowships can be a further means of promoting effective vulnerability disclosure norm implementation.

Monitoring and reporting on the implementation of the normative framework remain central to the ongoing debate on the structure and functions of a potential future permanent mechanism for the corresponding discussions on cybersecurity within the United Nations. Among the competing proposals – the **Program of Action** (PoA) and a permanent Open-ended Working Group – only the Program of Action explicitly includes voluntary reporting as a key pillar to support norm implementation. The cross-regional group backing the Program of Action, led by France, emphasizes that "States would be encouraged to conduct voluntary reporting on their efforts to implement the framework. This voluntary reporting could be based either on creating a dedicated reporting system or by promoting existing mechanisms [...]. This would enable a precise mapping of the needs and challenges States face through progress reports, hence informing discussions in review conferences and plenary discussions."[232] The group further underlines that "reporting will facilitate dedicated capacity-building activities and exchanges on best practices."[233]

[230] For example, United Nations (2024): (7th meeting) Open-ended working group on Information and Communication Technology (ICT) - Seventh Substantive Session and Burhan Gafoor (2024): OPENING REMARKS BY THE CHAIR OF THE OPEN-ENDED WORKING GROUP ON SECURITY OF AND IN THE USE OF ICTS 2021-2025, AMBASSADOR BURHAN GAFOOR, PERMANENT REPRESENTATIVE OF THE REPUBLIC OF SINGAPORE TO THE UNITED NATIONS, AT THE SEVENTH SUBSTANTIVE SESSION OF THE OEWG, 4 MARCH 2023

[231] For example, Institute for Peace Research and Security Policy at the University of Hamburg (2022): Cybersecurity Workshop on Government Vulnerabilities Disclosure

[232] Governments of Albania, Armenia, Belgium, Chile, Colombia, Côte d'Ivoire, Croatia, Czech Republic, Denmark, Estonia, France, Finland, Gabon, Georgia, Greece, Hungary, Ireland, Italy, Japan, Latvia, Luxembourg, Moldova, Netherlands, North Macedonia, Norway, Poland, Portugal, Republic of Korea, Romania, Senegal, Slovakia, Slovenia, Spain, Sweden, and Ukraine (2024): Cross-regional working paper – Proposal on the structure of the future mechanism for regular institutional dialogue on cyber issues

[233] Governments of Albania, Armenia, Belgium, Chile, Colombia, Côte d'Ivoire, Croatia, Czech Republic, Denmark, Estonia, France, Finland, Gabon, Georgia, Greece, Hungary, Ireland, Italy, Japan, Latvia, Luxembourg, Moldova, Netherlands, North Macedonia, Norway, Poland, Portugal, Republic of Korea, Romania, Senegal, Slovakia, Slovenia, Spain, Sweden, and Ukraine (2024): Cross-regional working paper – Proposal on the structure of the future mechanism for regular institutional dialogue on cyber issues

In addition to states, various stakeholders stressed the importance of incorporating voluntary reporting into the Program of Action, while some also highlighted the fact that "reporting for reporting's sake alone" should be avoided.[234] The latest agreement by states on elements of the future mechanism in the framework of the Open-ended Working Group's third Annual Progress Report does not touch upon the issue, but specifies "advanc[ing] implementation of the cumulative and evolving framework for responsible State behaviour in the use of ICTs" and "[...] discussions [...] on voluntary, non-binding norms of responsible State behaviour and the ways for their implementation,"[235] among other issues, as its intended scope and functions.

[234] See, for example, United Nations Institute for Disarmament Research (2023): Drawing Parallels: A Multi-Stakeholder Perspective on the Cyber PoA Scope, Structure and Content

[235] United Nations (2024): Developments in the field of information and telecommunications in the context of international security (A/79/214)

6. Conclusion

Governments have a vested interest in incentivizing all stakeholders to manage vulnerabilities in a way that enhances cybersecurity, recognizing that "vulnerability discovery, disclosure, and remediation is important to national interests"[236] for everyone. Central to this effort is Coordinated Vulnerability Disclosure, a process well understood in both theory and practice. Thus, governments aiming to improve vulnerability disclosure can draw from a wide range of international standards, tested policies, best practices, templates, and more.

However, "each government is responsible for its own pathway to implementation and for informing other states of its efforts."[237] As a first step, governments need to understand Coordinated Vulnerability Disclosure and the various roles government entities may play in this process. Secondly, government entities must lead by example, encouraging other stakeholders to participate in Coordinated Vulnerability Disclosure instead of engaging in actions that could harm cybersecurity. Lastly, governments must shape an enabling policy ecosystem, creating a transparent and reliable framework with the right incentives for all stakeholders involved. These incentives range from creating legal certainty about security research to offering rewards for vulnerability submissions and having government entities step in as a last resort when Coordinated Vulnerability Disclosure processes risk failure or when vulnerable abandoned code poses a critical security issue. Central to these activities should be a designated Point of Contact, a government coordinator who orchestrates operational actions and informs policymaking.

Governments implementing the vulnerability disclosure norm will likely begin by building national capabilities, potentially with the support of other stakeholders or states, and then refine the ecosystem before collaborating on other international activities and assisting other states in their implementation efforts.

[236] Allen D. Householder, Garret Wassermann, Art Manion, and Chris King (2017): The CERT® Guide to Coordinated Vulnerability Disclosure

[237] Bart Hogeveen (2022): The UN norms of responsible state behaviour in cyberspace Guidance on implementation for Member States of ASEAN

A possible starting point for governments interested in advancing the vulnerability disclosure norm could be to map their already implemented activities against the 4. Implementation Actions and then share their findings with other governments and non-government actors through the channels indicated in 5. Sharing Implementation Efforts. For think tanks and academia, it may be useful to work on in-depth analyses of countries and regions with existing policy ecosystems, both in policy and practice. This includes, but is not limited to, China, the United States, and the European Union post Cyber Resilience Act.

However, given the observed shortcomings, delays, and concerning policy developments in countries like **China**, it remains uncertain whether governments within the international community are genuinely committed to reducing risks tied to vulnerabilities by fostering the coordinated disclosure of these vulnerabilities in their policy ecosystems. The lack of robust vulnerability disclosure-oriented policy ecosystems would be detrimental to IT infrastructures globally as well as the overall stability of cyberspace, especially vis-à-vis the existing integration and future deployment of (emerging) technologies. Several **United Nations member states,**[238] among them **Switzerland,**[239] recently highlighted the need to pay close attention to vulnerabilities in specific technologies such as Artificial Intelligence (AI), Quantum Computing (QC), and Operational Technology (OT).

By fostering a robust and coordinated approach to vulnerability disclosure through enabling policy ecosystems, governments can significantly enhance national and global cybersecurity. This proactive stance not only mitigates risks but also sets a strong precedent for international cooperation and trust in handling cybersecurity threats.

[238] United Nations (2024): Developments in the field of information and telecommunications in the context of international security (A/79/214) and Open-ended Working Group on security of and in the use of information and communications technologies 2021-2025 (2024): (2nd meeting) Open-ended working group on Information and Communication Technology (ICT) - Seventh Substantive Session

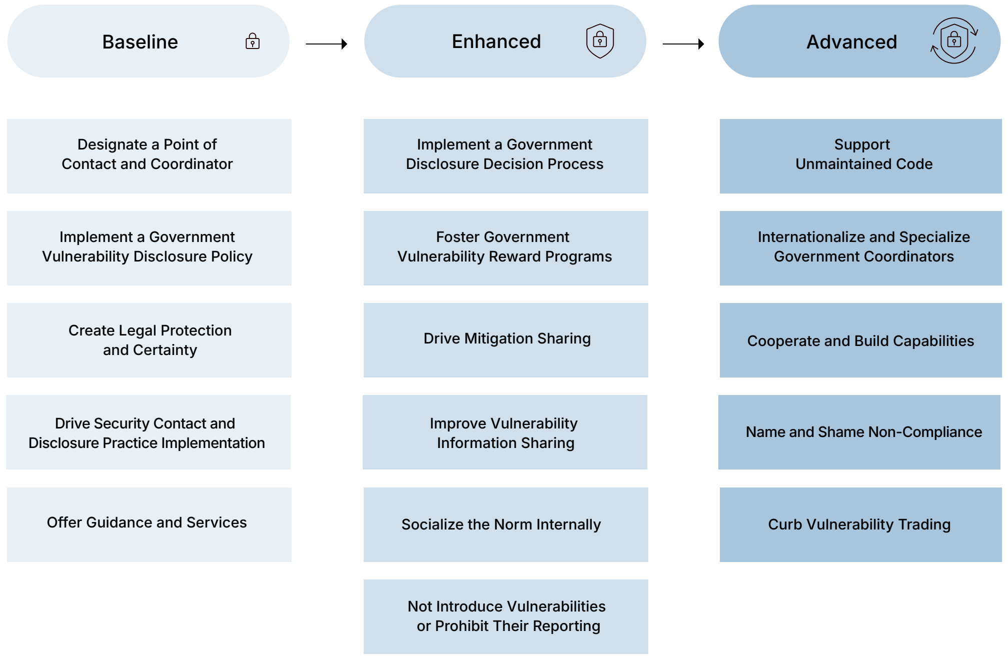
[239] Swiss Representative (2024): (3rd meeting) Open-ended working group on Information and Communication Technology (ICT) - Seventh Substantive Session

ANNEX

A. Vulnerability Disclosure Norm Implementation Checklist

Building upon the interest and utility expressed by states in condensing ways to implement the United Nations cyber norms in a checklist-like format, the implementation actions for the vulnerability disclosure norm examined in this study are listed below in a similarly checklist-like format, This could potentially guide governmental implementation efforts and serve as a contribution to the development of a voluntary checklist of practical implementation actions currently under consideration by states in the Open-ended Working Group on security of and in the use of information and communications technologies.[240]

3 **Vulnerability Disclosure Norm Implementation Actions Checklist**



Baseline → Enhanced → Advanced

Baseline

- Designate a Point of Contact and Coordinator
- Implement a Government Vulnerability Disclosure Policy
- Create Legal Protection and Certainty
- Drive Security Contact and Disclosure Practice Implementation
- Offer Guidance and Services

Enhanced

- Implement a Government Disclosure Decision Process
- Foster Government Vulnerability Reward Programs
- Drive Mitigation Sharing
- Improve Vulnerability Information Sharing
- Socialize the Norm Internally
- Not Introduce Vulnerabilities or Prohibit Their Reporting

Advanced

- Support Unmaintained Code
- Internationalize and Specialize Government Coordinators
- Cooperate and Build Capabilities
- Name and Shame Non-Compliance
- Curb Vulnerability Trading

[240] Open-ended working group on security of and in the use of information and communications technologies 2021-2025 (2024): Draft Annual Progress Report

Baseline Implementation

I. Governments should establish a well-resourced point of contact to manage all phases of Coordinated Vulnerability Disclosure and act as a coordinator between government and non-government entities.

II. Governments should adopt a comprehensive vulnerability disclosure policy to manage expectations of involved stakeholders.

III. Governments should prioritize comprehensive legal reform and protections for researchers to eliminate the legal uncertainties and repercussions that deter reporting and potentially lead to malicious use of unreported vulnerabilities.

IV. Governments could require code owners and system owners to implement security contacts and vulnerability disclosure policies to simplify and facilitate initial contact.

V. Governments should leverage existing expertise and resources to offer comprehensive guidance and services to stakeholders involved in Coordinated Vulnerability Disclosure.

Enhanced Implementation

VI. Governments could implement a process that allows temporary withholding from Coordinated Vulnerability Disclosure for vulnerabilities that are found by or reported to government entities other than cybersecurity agencies and deemed strategic assets.

VII. Governments could promote the establishment of Vulnerability Reward Programs by selected government entities to enhance reporting incentives.

VIII. Governments should improve both private and public sharing of vulnerability mitigations by establishing secure information sharing networks and encouraging the public release of mitigations for high-risk and forever day vulnerabilities.

IX. Governments should create information sharing channels and could support existing information sharing programs to enhance vulnerability assessment, risk management and remediation identification.

X. Governments could socialize the vulnerability disclosure norm nationally.

XI. Governments should not introduce additional vulnerabilities to code or prohibit stakeholders from reporting them.

Advanced Implementation

XII. Governments should support vulnerable end of life or abandoned code to address the risk stemming from potential forever day vulnerabilities.

XIII. Governments should be accessible to international stakeholders and could leverage international cooperation for further specialization of actions and services.

XIV. Governments could enhance each other's capabilities and cooperate on day-to-day norm implementation depending on their level of alignment.

XV. Governments could resort to publicly naming and shaming code owners and system owners that repeatedly neglect their responsibilities.

XVI. Governments could consider banning the trade of selected vulnerabilities and pursue international agreements in this regard.

4 **Vulnerability Disclosure Norm Implementation Actions – Role-Centric**

□ Baseline ▨ Enhanced ■ Advanced

	Finder	Reporter	Code Owner	System Owner	Coordinator
Designate a Point of Contact and Coordinator					✓
Implement a Government Vulnerability Disclosure Policy	✓	✓	✓	✓	✓
Create Legal Protection and Certainty	✓	✓			
Drive Security Contact and Disclosure Practice Implementation			✓	✓	
Offer Guidance and Services	✓	✓	✓	✓	✓
Implement a Government Disclosure Decision Process	✓	✓			
Foster Government Vulnerability Reward Programs	✓	✓	✓	✓	✓
Drive Mitigation Sharing			✓	✓	✓
Improve Vulnerability Information Sharing	✓	✓	✓	✓	✓
Socialize the Norm Internally	✓	✓	✓	✓	✓
Not Introduce Vulnerabilities or Prohibit Their Reporting		✓	✓		
Support Unmaintained Code			✓		✓
Internationalize and Specialize Government Coordinators		✓			✓
Cooperate and Build Capabilities	✓	✓	✓	✓	✓
Name and Shame Non-Compliance			✓	✓	
Curb Vulnerability Trading	✓				

5 Vulnerability Disclosure Norm Implementation Actions – Phase-Centric

▫ Baseline ▨ Enhanced ■ Advanced

	Discovery	Disclosure	Verification	Preparation	Notification	Publication	Post-Processing
Designate a Point of Contact and Coordinator	✓	✓	✓	✓	✓	✓	✓
Implement a Government Vulnerability Disclosure Policy		✓	✓	✓	✓	✓	✓
Create Legal Protection and Certainty	✓	✓					
Drive Security Contact and Disclosure Practice Implementation		✓					
Offer Guidance and Services	✓	✓	✓	✓	✓	✓	✓
Implement a Government Disclosure Decision Process	✓	✓					
Foster Government Vulnerability Reward Programs	✓	✓					
Drive Mitigation Sharing				✓	✓	✓	✓
Improve Vulnerability Information Sharing			✓	✓	✓	✓	
Socialize the Norm Internally	✓	✓					
Not Introduce Vulnerabilities or Prohibit Their Reporting	✓	✓					
Support Unmaintained Code		✓	✓	✓	✓	✓	✓
Internationalize and Specialize Government Coordinators	✓	✓	✓	✓	✓	✓	✓
Cooperate and Build Capabilities	✓	✓	✓	✓	✓	✓	✓
Name and Shame Non-Compliance		✓	✓	✓	✓	✓	✓
Curb Vulnerability Trading		✓					

B. Perspectives on the United Nations Vulnerability Disclosure Norm[241]

B.1 Coordinated Vulnerability Disclosure

Governments often refer to Vulnerability Disclosure Processes, Vulnerability Disclosure Policies, Vulnerability Disclosure Programs, Vulnerability Management, or Coordinated Vulnerability Disclosure. Without shedding light on its own efforts, **Pakistan** asked states "to commit to responsible and timely reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities."[242] **Canada** mentioned coordination mechanisms between the public and private sectors as one of its implementation-related efforts but remained vague as to their nature.[243]

Colombia highlighted its efforts toward "a procedure to promote responsible reporting of vulnerabilities in the information systems and technological infrastructure of State entities so that they can be remedied by the relevant entity."[244] In its national contribution to the same report,[245] **France** stated on a similar note that it "has taken various steps to allow the responsible disclosure of computer vulnerabilities." The **Kingdom of the Netherlands** "emphasize[d] the importance of developing coordinated vulnerability disclosure policies" and considered "develop[ing] national Coordinated Vulnerability Disclosure policies" as "an important first step in promoting regional cooperation among States" in the framework of the Organization for Security and Co-operation in Europe's Cyber/

[241] The following perspectives form a non-exhaustive list of actions that various government and non-government stakeholders directly or semi-directly consider part of implementing the vulnerability disclosure norm. The actions are derived from statements and contributions by governments as part of United Nations debates, contributions by states to the United Nations Secretary-General's annual reports on developments in the field of information and telecommunications in the context of international security, governmental activities in the framework multilateral organizations, and third parties, such as non-government organizations or private sector entities, addressing or touching upon the vulnerability disclosure norm. Given the confidential nature of deliberations within past GGEs, the consideration of United Nations debates is limited to discussions taking place in the framework of OEWG I and OEWG II.

[242] Unnamed (2021): Non-paper listing specific language proposals under agenda item "Rules, norms and principles" from written submissions by delegations and Pakistan (2023): Fourth Substantive Session of the UN Open-Ended Working Group (OEWG) on Security of and in the Use of Information and Communication Technologies (ICTs) in the Context of International Security – Agenda Item 2: On the Development of rules, norms, and principles of responsible behavior of States and Pakistan Representative (2024): (5th meeting) Open-ended working group on Information and Communication Technology (ICT) - Seventh Substantive Session

[243] Canada (2021): Updated norms guidance text with additions from States and stakeholders

[244] United Nations (2020): Developments in the field of information and telecommunications in the context of international security (A/75/123)

[245] United Nations (2020): Developments in the field of information and telecommunications in the context of international security (A/75/123)

ICT Security confidence-building measures.[246] **Czechia** highlighted Coordinated Vulnerability Disclosure policy as a measure to implement the vulnerability disclosure norm in its publicized response to the United Nations Institute for Disarmament Research norms implementation survey.[247] Similar to the Netherlands, Czechia also referred to the intersection of the vulnerability disclosure norm with the OSCE confidence-building measure on Coordinated Vulnerability Disclosure[248] and further stated that Coordinated Vulnerability Disclosure provides a concrete opportunity for implementing the norms.[249]

Mauritius stated that "with regard to coordinated approach to vulnerability disclosure, Mauritius supports that such approach will help to identify and remediate vulnerabilities in critical systems [...] before they can be exploited by cyber threat actors. Many international cybersecurity frameworks and standards such as ISO 29147 and ISO 30111 recommend or require the establishment of coordinated vulnerability disclosure processes as part of good cybersecurity practice."[250]

[246] Dutch Representative (2021): 8th plenary meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – First substantive session and Kingdom of the Netherlands (2022): "National intervention under agenda item 5: Discussions on substantive issues" – Statement by Kingdom of the Netherlands and Dutch Representative (2022): (5th meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session and Dutch Representative (2022): (7th meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session and Organization for Security and Co-operation in Europe (2024): Cyber/ICT Security

[247] United Nations Cyber Policy Portal (2024): Czechia

[248] In 2016, the Participating States of the Organization for Security and Co-operation in Europe (OSCE) adopted CBM 16, asking OSCE Participating States to "encourage responsible reporting of vulnerabilities affecting the security of and in the use of ICTs and share associated information on available remedies to such vulnerabilities, including with relevant segments of the ICT business and industry, with the goal of increasing co-operation and transparency within the OSCE region," employing wording very similar to that of the UN vulnerability disclosure norm. In this respect, they also emphasized the importance of exchanging information between Points of Contact. See Organization for Security and Co-operation in Europe (2016): DECISION No. 1202 OSCE CONFIDENCE-BUILDING MEASURES TO REDUCE THE RISKS OF CONFLICT STEMMING FROM THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES. In the framework of the United Nations Open-ended Working Group, member states also discussed adding Coordinated Vulnerability Disclosure to the list of voluntary global Confidence-Building Measures. See, for example, United Nations Open-ended working group Chair (2024): (1st meeting) Open-ended working group on Information and Communication Technology (ICT) - Seventh Substantive Session

[249] Czech Representative (2023): (6th meeting) Open-ended working group on Information and Communication Technology (ICT) - Fourth Substantive Session and Czech Republic (2023): Statement by Mr. Richard Kadlčák and Czech Representative (2024): (7th meeting) Open-ended working group on Information and Communication Technology (ICT) - Seventh Substantive Session

[250] Mauritius Representative (2024): (7th meeting) Open-ended working group on Information and Communication Technology (ICT) - Seventh Substantive Session

Kuwait remarked that vulnerability management would be one of the 10 most important tools for countries with fewer resources to improve cybersecurity.[251]

Switzerland shared that it had already implemented a Coordinated Vulnerability Disclosure mechanism[252] and highlighted its support for the Geneva Manual as vulnerability disclosure norm implementation effort.[253] The **United Kingdom** reported on its efforts to implement the vulnerability disclosure norm, highlighting that its National Cyber Security Centre is advising public and private organizations on vulnerability disclosure processes and is centrally coordinating vulnerability disclosure for government online services.[254] **Singapore** alluded to having implemented a similar process, stating that it "has issued public advisories to guide enterprises and the general public on managing and navigating cyber-related vulnerabilities [...] when they arise."[255]

The **Group of Seven** countries (Canada, France, Germany, Italy, Japan, United Kingdom, and United States) listed their assistance in creating vulnerability disclosure processes as a concrete action for implementing the vulnerability disclosure norm in their 2019 Cyber Norm Initiative statement.[256]

The **Organization for Security and Co-operation in Europe** highlighted Coordinated Vulnerability Disclosure as a key element for its work on implementing Confidence-Building Measure 16.[257]

ICT4Peace and The Hague Program on Cyber Norms at **Leiden University** compiled a detailed analysis of the vulnerability disclosure norm in the context of a commentary on all United Nations cyber norms.[258] To implement the vulnerability

[251] Kuwaiti Representative (2023): (8th meeting) Open-ended working group on Information and Communication Technology (ICT) - Sixth Substantive Session

[252] United Nations (2021): Advancing responsible State behaviour in cyberspace in the context of international security (A/76/187)

[253] Swiss Representative (2024): (7th meeting) Open-ended working group on Information and Communication Technology (ICT) - Seventh Substantive Session

[254] United Kingdom Foreign & Commonwealth Office (2019): Non-Paper on Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015

[255] United Nations (2022): Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies (A/77/92)

[256] G7 Cyber Norm Initiative (2019): Cyber Norm Initiative – Synthesis of Lessons Learned and Best Practices

[257] Organization for Security and Co-operation in Europe's Representative (2023): (9th meeting) Open-ended working group on Information and Communication Technology (ICT) - Sixth Substantive Session

[258] Nicholas Tsagourias (2017): Recommendation 13 (j)

disclosure norm, the commentary recommends “national policies on responsible reporting based on generally agreed standards and good practices” and that governments “encourage software companies to introduce responsible reporting policies.”[259]

In response to a 2019 public consultation on responsible state behavior in cyberspace in the context of international security at the United Nations, run by the Australian Department of Foreign Affairs and Trade, **Global Partners Digital** called for the implementation of Coordinated Vulnerability Disclosure, referencing respective International Standards.[260] In their response, **Tech Accord** signatories highlighted vulnerability management policies and vulnerability disclosure policies.[261] **Kaspersky’s** suggestion was to “establish transparent policies for responsible vulnerability disclosure.”[262] Kaspersky further requested states to have “clear institutional frameworks on vulnerability disclosure” and “transparency in vulnerability handling by both Member State and nonstate actors,” as well as “guidelines for requiring baseline vulnerability management and disclosure processes for private sector entities” in a later statement.[263]

The **Australian Strategic Policy Institute** issued a “Guidance on implementation for Member States of ASEAN” with observed best practices.[264] On the vulnerability disclosure norm, its guidance endorsed vulnerability disclosure policies and vulnerability assessments. A report commissioned by the **Global Forum on Cyber Expertise**[265] mentioned international cooperation on vulnerability disclosure and highlighted India’s Responsible Vulnerability Disclosure Program. It also proposed that “those who develop or produce critical products take reasonable measures to ensure […] they are effectively and timely

[259] Nicholas Tsagourias (2017): Recommendation 13 (j)

[260] Global Partners Digital (2020): DFAT Public Consultation: Responsible state behaviour in cyberspace in the context of international security at the United Nations

[261] Department of Foreign Affairs and Trade (2020): Public Consultation: responsible state behaviour in cyberspace in the context of international security – Summary of public submissions on developing best practice guidance on implementation of the 11 norms of responsible state behaviour in cyberspace articulated in the 2015 GGE Report (A/70/174), as endorsed by the UN General Assembly (A/RES/70/237)

[262] Kaspersky (2020): Submission on ‘Responsible state behaviour in cyberspace in the context of international security at the United Nations

[263] Kaspersky (2020): Submission to the Open-Ended Working Group (‘OEWG’) on developments in the field of information and telecommunications in the context of international security – Private Sector Technical Perspective to Best Practice Implementation of 2015 UN GGE Norms (A/70/174)

[264] Bart Hogeveen (2022): The UN norms of responsible state behaviour in cyberspace – Guidance on implementation for Member States of ASEAN

[265] The report was co-authored by Mika Kerttunen and Eneken Tikk; see Mika Kerttunen and Eneken Tikk (2021): PUTTING CYBER NORMS IN PRACTICE: Implementing the UN GGE 2015 recommendations through national strategies and policies

mitigated and, when appropriate, disclosed when discovered. The process used should be transparent to create a predictable and stable environment."

B.2 Equities Process

In its paper on the implementation of the United Nations cyber norms, **Canada** stated the existence of a "Equities Management Framework" as part of its vulnerability disclosure norm implementation efforts.[266] The **United Kingdom**[267] acknowledged that it is also running an "Equities Process" in its paper on national norm implementation efforts.[268] During deliberations in the Open-ended Working Group, **India** stated that "states should create procedurally transparent frameworks to assess whether and when to disclose, not publicly known vulnerabilities or flaws that they are aware of with regard to information systems and technologies."[269] **Egypt**[270] and **Pakistan,**[271] however, expressed serious concerns about "stockpiling vulnerabilities," which is an expression used to refer to equity processes by those opposing it.

The Pall Mall Process,[272] co-led by the **United Kingdom** and **France** and involving several other countries and referred to multiple times by both during United Nations debates,[273] acknowledged explicitly that there is a responsible way to exploit vulnerabilities,[274] thereby implicitly requiring the existence of an equities process.

[266] Government of Canada (2019): Canada's implementation of the 2015 GGE norms

[267] United Kingdom Foreign & Commonwealth Office (2019): Non-Paper on Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015

[268] United Kingdom Foreign & Commonwealth Office (2019): Non-Paper on Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015

[269] Indian Representative (2021): 6th plenary meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – First substantive session

[270] Delegation of Egypt (2020): Working Paper submitted by the Delegation of Egypt To the Open-Ended Working Group on Developments in The Field of Information and Telecommunications in The Context of International Securitya

[271] Pakistan (2020): Working Paper by Pakistan – Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and Pakistan Representative (2021): 5th plenary meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – First substantive session

[272] Pall Mall Process (2024): Tackling the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities

[273] French Representative (2024): (2nd meeting) Open-ended working group on Information and Communication Technology (ICT) - Seventh Substantive Session and Representative of the United Kingdom (2024): (2nd meeting) Open-ended working group on Information and Communication Technology (ICT) - Seventh Substantive Session

[274] Sven Herpig and Alexandra Paulus (2024): The Pall Mall Process on Cyber Intrusion Capabilities

In the commentary published by **ICT4Peace** and **Leiden University,** the authors suggested that governments "promulgate laws or reinforce existing laws with regard to disclosure, retention or use of vulnerabilities" to implement the vulnerability disclosure norm.[275] Similarly, in response to the 2019 Australian public consultation on responsible state behavior in cyberspace in the context of international security at the United Nations, **Global Partners Digital** demanded that states "should make public the criteria and processes used in determining whether the government discloses a vulnerability they have discovered."[276]

Microsoft[277]**,** the **Tech Accord** signatories,[278] the **Australian Strategic Policy Institute,**[279] **the** authors of the **Global Forum on Cyber Expertise** report,[280] the **Institute for International Cyber Stability,**[281] and the authors of the **Global Commission on the Stability of Cyberspace**[282] report all recommended the implementation of a "Vulnerabilities Equities Process," the name the United States has given to its equity process.

[275] Nicholas Tsagourias (2017): Recommendation 13 (j)

[276] Global Partners Digital (2020): DFAT Public Consultation: Responsible state behaviour in cyberspace in the context of international security at the United Nations

[277] Microsoft (2020): Microsoft's contribution to Australia's engagement in the United Nations' dialogues on information security

[278] Department of Foreign Affairs and Trade (2020): Public Consultation: responsible state behaviour in cyberspace in the context of international security – Summary of public submissions on developing best practice guidance on implementation of the 11 norms of responsible state behaviour in cyberspace articulated in the 2015 GGE Report (A/70/174), as endorsed by the UN General Assembly (A/RES/70/237)

[279] Department of Foreign Affairs and Trade (2020): Public Consultation: responsible state behaviour in cyberspace in the context of international security – Summary of public submissions on developing best practice guidance on implementation of the 11 norms of responsible state behaviour in cyberspace articulated in the 2015 GGE Report (A/70/174), as endorsed by the UN General Assembly (A/RES/70/237)

[280] Mika Kerttunen and Eneken Tikk (2021): PUTTING CYBER NORMS IN PRACTICE: Implementing the UN GGE 2015 recommendations through national strategies and policies

[281] Department of Foreign Affairs and Trade (2020): Public Consultation: responsible state behaviour in cyberspace in the context of international security – Summary of public submissions on developing best practice guidance on implementation of the 11 norms of responsible state behaviour in cyberspace articulated in the 2015 GGE Report (A/70/174), as endorsed by the UN General Assembly (A/RES/70/237)

[282] Global Commission on the Stability of Cyberspace (2019): Advanced Cyberstability

The **International Committee of the Red Cross** (**ICRC**)**,** together with the **Australian Red Cross,** were more critical of such a process, implying that an equities process is better than not having one, but also emphasizing that "the risks entailed by a decision not to disclose vulnerabilities in view of the specific characteristics of cyber space should be duly considered in these kinds of decision-making frameworks."[283]

Global Partners Digital mentioned that an equities process can be implemented as part of the vulnerability disclosure norm, while it also highlighted the negative impact of "stockpiling vulnerabilities" in a separate statement, together with the **Association for Progressive Communications**.[284]

B.3 Guidance

During Open-ended Working Group discussions, **Fiji** welcomed guidance and information materials on vulnerability disclosure policies and programs to be shared as implementation of existing norms.[285] In relation to guidance, **Switzerland** mentioned that "[...] exchange on good practices, lessons learned, or the use of an online course on coordinated vulnerability disclosure [...] will help implement Norm 13J."[286] On a broader level, Switzerland also suggested that states "[could] develop cooperative measures for responsible vulnerability disclosures."[287] **Cuba** requested permission to "publish vulnerability studies on platforms of ICTs without this entailing compromising infrastructures or services of states."[288] The **Netherlands** elaborated that it provides e-learning modules and policy papers, and organizes workshops on Coordinated Vulnerability Disclosure.[289]

[283] Department of Foreign Affairs and Trade (2020): Public Consultation: responsible state behaviour in cyberspace in the context of international security – Summary of public submissions on developing best practice guidance on implementation of the 11 norms of responsible state behaviour in cyberspace articulated in the 2015 GGE Report (A/70/174), as endorsed by the UN General Assembly (A/RES/70/237)

[284] Deborah Brown, Anriette Esterhuysen, and Sheetal Kumar(2019): Unpacking the GGE's framework on responsible state behaviour: Cyber norms

[285] Fiji Representative (2024): (4th meeting) Open-ended working group on Information and Communication Technology (ICT) - Eighth Substantive Session (8-12 July 2024)

[286] Switzerland Representative (2024): (7th meeting) Open-ended working group on Information and Communication Technology (ICT) - Seventh Substantive Session

[287] Swiss Representative (2021): 2nd plenary meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – First substantive session and Swiss Representative (2021): 6th plenary meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – First substantive session

[288] Cuban Representative (2023): (7th meeting) Open-ended working group on Information and Communication Technology (ICT) - Fourth Substantive Session

[289] Dutch Representative (2023): (7th meeting) Open-ended working group on Information and Communication Technology (ICT) - Sixth Substantive Session

In their 2017 report, the authors from **ICT4Peace** and **Leiden University** commentary recommended that governments "publish and disseminate standards and best practices for responsible reporting and invite ICT stakeholders to voluntarily abide by them."[290] Similarly, the **Australian Strategic Policy Institute** suggested "endors[ing] relevant ISO standards" and good practices.[291] Identifying and sharing good practices is also something suggested by the authors of the **Global Forum on Cyber Expertise**'s report.[292] Additionally, the authors suggested considering concrete actions, such as sector-specific vulnerability reporting mechanisms and running awareness campaigns, and highlighted the Dutch vulnerability reporting guidelines and the Australian guidelines on patching.[293]

B.4 Information Exchange

Sharing information on vulnerabilities seems to be an obvious action to take for implementing the vulnerability disclosure norm. **Colombia** highlighted the importance of the timely exchange of information on vulnerabilities[294] along with **Argentina,**[295] **Canada,**[296] **Egypt,**[297] **France,**[298] **Kazakhstan,**[299] **Pakistan,**[300]

[290] Nicholas Tsagourias (2017): Recommendation 13 (j)

[291] Department of Foreign Affairs and Trade (2020): Public Consultation: responsible state behaviour in cyberspace in the context of international security – Summary of public submissions on developing best practice guidance on implementation of the 11 norms of responsible state behaviour in cyberspace articulated in the 2015 GGE Report (A/70/174), as endorsed by the UN General Assembly (A/RES/70/237) and Bart Hogeveen (2022): The UN norms of responsible state behaviour in cyberspace – Guidance on implementation for Member States of ASEAN

[292] Mika Kerttunen and Eneken Tikk (2021): PUTTING CYBER NORMS IN PRACTICE: Implementing the UN GGE 2015 recommendations through national strategies and policies

[293] Mika Kerttunen and Eneken Tikk (2021): PUTTING CYBER NORMS IN PRACTICE: Implementing the UN GGE 2015 recommendations through national strategies and policies

[294] Nohra Quintero (2020): SEGUNDA SESIÓN SUSTANTIVA GRUPO DE COMPOSICIÓN ABIERTA SOBRE DESARROLLOS EN EL CAMPO DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES EN EL CONTEXTO DE LA SEGURIDAD INTERNACIONAL – INTERVENCION DE COLOMBIA

[295] Argentinian Representative (2021): 5th plenary meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – First substantive session

[296] Canada (2021): Updated norms guidance text with additions from States and stakeholders

[297] Delegation of Egypt (2020): Working Paper submitted by the Delegation of Egypt To the Open-Ended Working Group on Developments in The Field of Information and Telecommunications in The Context of International Security and Egyptian Representative (2021): 8th plenary meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – First substantive session

[298] United Nations (2020): Developments in the field of information and telecommunications in the context of international security (A/75/123)

[299] Kazakh Representative (2024): (3rd meeting) Open-ended working group on Information and Communication Technology (ICT) - Eighth Substantive Session (8-12 July 2024)

[300] Pakistan Representative (2022): (7th meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session and Pakistan Representative (2024): (3rd meeting) Open-ended working group on Information and Communication Technology (ICT) - Eighth Substantive Session (8-12 July 2024)

and **India.**[301] **Türkyie** remarked that its "national CERT is constantly communicating information regarding malicious cyber activity or possible vulnerabilities to institutional and sectoral CERTs and the public."[302] **Honduras** stated that it manages and remedies vulnerabilities through an "addition to information asset inventories of data relating to the software provider, version, current deployment status and the officer responsible for the software," which appears to be a basic vulnerabilities database.[303] In a similar vein, the **Republic of Korea** stated that its responsible government entity has "uploaded major vulnerabilities on its websites on a regular basis in order to share relevant information."[304] In terms of cross-jurisdictional information exchange, **Brazil** pointed toward the benefit of regional cooperation in the Americas and South America regarding vulnerability information exchange.[305]

Kenya suggested establishing a United Nations-wide repository that can include vulnerability information,[306],supported by the **Philippines,**[307] **Albania,**[308] and **Mauritius.**[309] Over a dozen states supported the idea of a threat repository, though did not specify whether it should serve as a

[301] Indian Representative (2021): 6th plenary meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – First substantive session and Indian Representative (2022): (3rd meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session and Indian Representative (2023): (2nd meeting) Open-ended working group on Information and Communication Technology (ICT) - Fourth Substantive Session

[302] Turkish Representative (2022): (4th meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session

[303] United Nations (2020): Developments in the field of information and telecommunications in the context of international security (A/75/123)

[304] Republic of Korea (2020): Implementation of the 2015 UNGGE Norms

[305] Brazilian Representative (2024): (4th meeting) Open-ended working group on Information and Communication Technology (ICT) - Seventh Substantive Session

[306] Government of Kenya (2023): DRAFT WORKING PAPER ON THE ESTABLISHMENT OF A THREAT REPOSITORY WITHIN THE UNITED NATIONS

[307] Philippine Representative (2023): (7th meeting) Open-ended working group on Information and Communication Technology (ICT) - Fourth Substantive Session

[308] Albanian Representative (2024): (7th meeting) Open-ended working group on Information and Communication Technology (ICT) - Seventh Substantive Session

[309] Mauritius Representative (2024): (3rd meeting) Open-ended working group on Information and Communication Technology (ICT) - Seventh Substantive Session

vulnerability database.[310] **India** suggested a Global Cyber Security Cooperation Portal that could, for example, serve as a "platform for member states for voluntarily sharing and exchanging information on ICT-related vulnerabilities."[311]

Kenya ICT Action Network, Red en Defensa de los Derechos Digitales (R3D), Global Partners Digital, Derechos Digitales, and **Fundacion Karisma** supported the idea of a United Nations-wide threat repository, database, or cybersecurity portal.[312] However, only **Hitachi America** mentioned that it should include vulnerability information.[313]

The authors of the **ICT4Peace** and **Leiden University** commentary recommended the promotion of "international collaboration to devise and inculcate best practices or rules and regulations on [...] sharing of information" in 2017.[314] The authors of the **Global Forum on Cyber Expertise** report[315] mentioned international cooperation on vulnerability disclosure and highlighted the "Japan Vulnerability Notes,"[316] a vulnerability database.

[310] See, for example, Open-ended working group on Information and Communication Technology (2023): (1st meeting) Open-ended working group on Information and Communication Technology (ICT) - Fifth Substantive Session and Open-ended working group on Information and Communication Technology (2023): (2nd meeting) Open-ended working group on Information and Communication Technology (ICT) - Fifth Substantive Session and Open-ended working group on Information and Communication Technology (2023): (8th meeting) Open-ended working group on Information and Communication Technology (ICT) - Fifth Substantive Session and Open-ended working group on Information and Communication Technology (2023): (1st meeting) Open-ended working group on Information and Communication Technology (ICT) - Sixth Substantive Session and Open-ended working group on Information and Communication Technology (2023): (2nd meeting) Open-ended working group on Information and Communication Technology (ICT) - Sixth Substantive Session and Open-ended working group on Information and Communication Technology (2023): (3rd meeting) Open-ended working group on Information and Communication Technology (ICT) - Sixth Substantive Session and Open-ended working group on Information and Communication Technology (2023): (8th meeting) Open-ended working group on Information and Communication Technology (ICT) - Sixth Substantive Session

[311] Indian Ministry of External Affairs (2022): GLOBAL CYBER SECURITY COOPERATION PORTAL – CONCEPT NOTE and Indian Representative (2021): 7th plenary meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – First substantive session

[312] Open-ended working group on Information and Communication Technology (2023): (6th meeting) Open-ended working group on Information and Communication Technology (ICT) - Fifth Substantive Session

[313] Hitachi America Representative (2023): (6th meeting) Open-ended working group on Information and Communication Technology (ICT) - Fifth Substantive Session

[314] Nicholas Tsagourias (2017): Recommendation 13 (j)

[315] Mika Kerttunen and Eneken Tikk (2021): PUTTING CYBER NORMS IN PRACTICE: Implementing the UN GGE 2015 recommendations through national strategies and policies

[316] JPCERT/CC and IPA (2024): JVN Japan Vulnerability Notes

B.5 Legal Protection

In response to the 2019 public consultation on responsible state behavior in cyberspace in the context of international security at the United Nations, the **Forum of Incident Response and Security Teams** advocated against the criminalization of security research and for ease of exchange of information on vulnerabilities internationally.[317] In its response, **Kaspersky** highlighted the need for a "safe harbor for security researchers."[318] The **Tech Accord** supported this aspect by arguing that there is a need for legal frameworks to be in place that "allow security researchers to find and report vulnerabilities without negative sanctions."[319] The **Australian Strategic Policy Institute** highlighted "adequate legal provisions to support, encourage and protect responsible reporters" in its response.[320] It reiterated this aspect in its 2022 "Guidance on implementation for Member States of ASEAN."[321] In another response to the Australian public consultation, **Global Partners Digital** called for the legal protection of security researchers as well.[322] Together with the **Association for Progressive Communications,** they mentioned legal protection and certainty as an important part of vulnerability disclosure norm implementation.[323] The authors of the **ICT4Peace** and **Leiden University** commentary also suggested the creation of "an enabling legal framework to facilitate responsible reporting."[324] **Access Now** highlighted the role of the legal protection of security researchers in the implementation of the vulnerability disclosure norm.[325]

[317] FIRST (2020): Position paper on cybersecurity developments within the UN context

[318] Kaspersky (2020): Submission on 'Responsible state behaviour in cyberspace in the context of international security at the United Nations

[319] Department of Foreign Affairs and Trade (2020): Public Consultation: responsible state behaviour in cyberspace in the context of international security – Summary of public submissions on developing best practice guidance on implementation of the 11 norms of responsible state behaviour in cyberspace articulated in the 2015 GGE Report (A/70/174), as endorsed by the UN General Assembly (A/RES/70/237)

[320] Department of Foreign Affairs and Trade (2020): Public Consultation: responsible state behaviour in cyberspace in the context of international security – Summary of public submissions on developing best practice guidance on implementation of the 11 norms of responsible state behaviour in cyberspace articulated in the 2015 GGE Report (A/70/174), as endorsed by the UN General Assembly (A/RES/70/237)

[321] Bart Hogeveen (2022): The UN norms of responsible state behaviour in cyberspace – Guidance on implementation for Member States of ASEAN

[322] Global Partners Digital (2020): DFAT Public Consultation: Responsible state behaviour in cyberspace in the context of international security at the United Nations

[323] Deborah Brown, Anriette Esterhuysen, and Sheetal Kumar (2019): Unpacking the GGE's framework on responsible state behaviour: Cyber norms

[324] Nicholas Tsagourias (2017): Recommendation 13 (j)

[325] Access Now Representative (2024): (6th meeting) Open-ended working group on Information and Communication Technology (ICT) - Seventh Substantive Session

B.6 Mitigation Sharing

In addition to exchanging information, states can share concrete mitigation or remedies. In this context, **Pakistan** asked states "to commit to responsible and timely reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities."[326] **Mexico** stated that it will "promote [...] the creation of a global cyber incident repository in which member states can voluntarily share experiences [...] also on mitigation and recovery measures."[327]

Canada mentioned in 2019 that the Canadian Centre for Cyber Security issues alerts and advisories regarding threats affecting its critical infrastructure.[328] It furthermore proposed more sharing of technical information in serious incidents, bilaterally and regionally.[329] Canada highlighted how it integrates identifying and mitigating vulnerabilities into its capacity building efforts.[330] **France** also stated that it "regularly exchanges [...] available solutions with its counterparts and partners."[331] **India** highlighted the role of states in requesting code owners to provide patches and notify system owners of vulnerabilities, as well as to facilitate mitigation sharing.[332]

The **Australian Strategic Policy Institute** observed the issuing of advisories as practice for the implementation of the vulnerability disclosure norm from member states of the Association of Southeast Asian Nations.[333]

[326] Unnamed (2021): Non-paper listing specific language proposals under agenda item "Rules, norms and principles" from written submissions by delegations and Pakistan (2023): Fourth Substantive Session of the UN Open-Ended Working Group (OEWG) on Security of and in the Use of Information and Communication Technologies (ICTs) in the Context of International Security – Agenda Item 2: On the Development of rules, norms, and principles of responsible behavior of States

[327] Mexican Representative (2021): 3rd plenary meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – First substantive session

[328] Government of Canada (2019): Canada's implementation of the 2015 GGE norms

[329] Canada (2021): Updated norms guidance text with additions from States and stakeholders

[330] Canadian Representative (2024): (9th meeting) Open-ended working group on Information and Communication Technology (ICT) - Seventh Substantive Session

[331] United Nations (2020): Developments in the field of information and telecommunications in the context of international security (A/75/123)

[332] Unnamed (2021): Non-paper listing specific language proposals under agenda item "Rules, norms and principles" from written submissions by delegations

[333] Bart Hogeveen (2022): The UN norms of responsible state behaviour in cyberspace – Guidance on implementation for Member States of ASEAN

B.7 Harmful Hidden Functions and Proliferation Risks

From the government perspectives addressing vulnerability disclosure, the **Republic of Belarus** highlighted "the potential for undeclared capabilities and vulnerabilities to appear in information security products."[334] During Open-ended Working Group deliberations, the **Islamic Republic of Iran** asked states to "refrain from [...] creat[ing] or assist[ing] development of vulnerability in products, services and maintenance [...]," calling it out as "back-doors"[335] and reiterated its point multiple times[336] – also calling for it to be considered as an additional norm. **Cuba** even proposed publishing studies "related to vulnerabilities and hidden functions identified in ICTs."[337] **Pakistan** asked states "to reach agreement on prohibiting the creation of harmful hidden functions or accumulation of vulnerabilities in ICT products"[338] and suggested an additional norm covering it.[339]

Colombia asked states to "prevent the proliferation of malicious ICT tools, techniques and harmful hidden functions", encouraging regional action on

[334] United Nations (2017): Developments in the field of information and telecommunications in the context of international security (A/72/315)

[335] Islamic Republic of Iran (2020): Open-ended working group on: Developments in the field of information and telecommunications in the context of international security – Second substantive session- February 2020 – Second submission by the Islamic Republic of Iran and Iranian Representative (2021): 6th plenary meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – First substantive session and Iranian Representative (2022): (5th meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session

[336] Unnamed (2021): Non-paper listing specific language proposals under agenda item "Rules, norms and principles" from written submissions by delegations and Islamic Republic of Iran Representative (2022): (3rd meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session and Delegation of Islamic Republic of Iran (2022): Statement by Delegation of the Islamic Republic of Iran to the Second Substantive Session of the Open-ended Working Group on Security of and in the Use of information and telecommunications technologies and Heidar Ali Balouji (2023): Statement – Norms, Rules and Principles

[337] Delegation of Cuba (2020): WORKING PAPER SUBMITTED BY THE DELEGATION OF CUBA TO THE OPEN-ENDED WORKING GROUP ON DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY (OEWG) and Cuban Representative (2021): 7th plenary meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – First substantive session and Cuban Representative (2023): (8th meeting) Open-ended working group on Information and Communication Technology (ICT) - Sixth Substantive Session

[338] Unnamed (2021): Non-paper listing specific language proposals under agenda item "Rules, norms and principles" from written submissions by delegations and Pakistan (2023): Fourth Substantive Session of the UN Open-Ended Working Group (OEWG) on Security of and in the Use of Information and Communication Technologies (ICTs) in the Context of International Security – Agenda Item 2: On the Development of rules, norms, and principles of responsible behavior of States

[339] Pakistan Representative (2024): (5th meeting) Open-ended working group on Information and Communication Technology (ICT) - Seventh Substantive Session

this issue.[340] **Egypt** highlighted the challenge posed by the proliferation of "malicious ICT tools and techniques" as well, though not particularly specifying vulnerabilities or hidden functions.[341] Similar to **Egypt**, the **Netherlands** also referred only to curbing the commercial distribution of vulnerabilities, without referring to harmful hidden functions.[342] In their individual national capacities, the **United Kingdom** and **Cuba** also remarked on the risks stemming from the proliferation of vulnerabilities, for example, through accessible marketplaces.[343]

The **Russian Federation** declared that the vulnerability disclosure norm – along with the norm on secure supply chains – is to be understood as the state's role in discouraging hidden functions in software and hardware products and recognizing the negative impact of those functions, along with vulnerability exploitation on international peace and security.[344] This remark on hidden functions is in line with an earlier statement within the context of the Open-ended Working Group that advocated against "integrating undeclared capabilities in ICTs, as well as concealing by manufacturers of information on vulnerabilities in their products" but does not explicitly reference the vulnerability disclosure norm.[345] The Russian Federation also included this issue as part of its 2023 proposal for a United Nations Convention on ensuring international information security in the proposal's section on "main threats to international information security and related factors."[346] Their proposal was co-sponsored by the **Republic of Belarus**, the **Democratic People's Republic of Korea**, the **Republic of Nicaragua**, the **Syrian Arab Republic**, and the **Bolivarian Republic of Venezuela**.

[340] United Nations (2021): Advancing responsible State behaviour in cyberspace in the context of international security (A/76/187)

[341] Delegation of Egypt (2020): Working Paper submitted by the Delegation of Egypt To the Open-Ended Working Group on Developments in The Field of Information and Telecommunications in The Context of International Security

[342] Dutch Representative (2021): 6th plenary meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – First substantive session

[343] United Kingdom Representative (2024): (2nd meeting) Open-ended working group on Information and Communication Technology (ICT) - Seventh Substantive Session and Cuban Representative (2024): (2nd meeting) Open-ended working group on Information and Communication Technology (ICT) - Seventh Substantive Session

[344] Permanent Mission of the Russian Federation to the United Nations (2023): STATEMENT – BY THE RUSSIAN INTERAGENCY DELEGATION AT THE FIFTH SESSION OF THE UN OPEN-ENDED WORKING GROUP ON SECURITY OF AND IN THE USE OF ICTS 2021-2025 and Russian Representative (2023): (1st meeting) Open-ended working group on Information and Communication Technology (ICT) - Fifth Substantive Session

[345] Permanent Mission of the Russian Federation to the United Nations (2021): STATEMENT – BY THE REPRESENTATIVE OF THE RUSSIAN FEDERATION AT THE FOURTH SESSION OF THE UN OPEN-ENDED WORKING GROUP ON SECURITY OF AND IN THE USE OF ICTS 2021-2025

[346] Russian Federation (2023): UPDATED CONCEPT OF THE CONVENTION OF THE UNITED NATIONS ON ENSURING INTERNATIONAL INFORMATION SECURITY

In 2024, the **United Kingdom** reiterated that states outlined the role of the private sector in preventing the introduction of harmful hidden functions during the discussions on the norms within the Open-Ended Working Group,[347] a point that was supported by **France** in the same session.[348]

Global Partners Digital, together with the **Association for Progressive Communications,** remarked on the negative impact of "inserting backdoors into ICT software or hardware" for human rights.[349] The authors of the **Global Commission on the Stability of Cyberspace** report recognized the need for an adjacent norm that focused on "not tamper[ing] with products and services in development and production."[350]

B.8 Point of Contact

Canada suggested setting up national structures for implementing the vulnerability disclosure norm, though it remained vague about what kind of structure for what specific purpose this entailed.[351] In a similar vein, **Türkiye** alluded to the fact that it had registered as a Common Vulnerabilities and Exposures Numbering Authority, without adding more context.[352]

With regard to the role that government stakeholders play in implementing the vulnerability disclosure norm, the **Group of Seven** countries portrayed national cybersecurity agencies as central actors.[353]

ICT4Peace and **Leiden University's** commentary[354] suggested the establishment of Points of Contact as "platforms where policies, guidelines or standards concerning the process of discovery, reporting, and disclosure are discussed and endorsed by key stakeholders" and "focal points to receive information about

[347] United Kingdom Representative (2024): (2nd meeting) Open-ended working group on Information and Communication Technology (ICT) - Eighth Substantive Session (8-12 July 2024)

[348] French Representative (2024): (3rd meeting) Open-ended working group on Information and Communication Technology (ICT) - Eighth Substantive Session (8-12 July 2024)

[349] Deborah Brown, Anriette Esterhuysen, and Sheetal Kumar(2019): Unpacking the GGE's framework on responsible state behaviour: Cyber norms

[350] Global Commission on the Stability of Cyberspace (2019): Advanced Cyberstability

[351] Canada (2021): Updated norms guidance text with additions from States and stakeholders

[352] United Nations (2022): Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies (A/77/92)

[353] G7 Cyber Norm Initiative (2019): Cyber Norm Initiative – Synthesis of Lessons Learned and Best Practices

[354] Nicholas Tsagourias (2017): Recommendation 13 (j)

remedies." Additionally, the commentary recommended creating "a focal point to receive and assess reports and decide on further action [...] also establish troubleshooting processes." The report by the **Global Commission on the Stability of Cyberspace**[355] mentions something akin to the focal point suggested by the ICT4Peace and Leiden University's commentary – the creation of a central body for vulnerability disclosure. In this vein, the report highlighted the role of **Japan's** JPCERT/CC setup as a vulnerability disclosure coordinator, particularly its function as the Common Vulnerabilities and Exposures Numbering Authority.

B.9 Reward Programs

The **Republic of Korea** named "bug bounty programs to encourage individuals to report bugs and vulnerabilities in software" as one of its efforts to implement the vulnerability disclosure norm.[356]

In response to the 2019 Australian public consultation on responsible state behavior in cyberspace in the context of international security at the United Nations, **Kaspersky** suggested a "bug bounty program running together with a third party."[357] In its response, the **Australian Strategic Policy Institute** highlighted "legitimate bug bounty programmes" and "hacking sessions" as actions to implement the vulnerability disclosure norm.[358] **Global Partners Digital** recommended that governments "fund defensive vulnerability discovery and research and invest in building security researcher communities."[359]

The authors of the **Global Forum on Cyber Expertise** report recommended considering "support[ing] and creat[ing] 'bug bounty' programs"[360] and the **Australian Strategic Policy Institute** observed "government vulnerability disclosure reward programs" as well as "bug bounty programs" as practiced in the Association of Southeast Asian Nations region.[361]

[355] Global Commission on the Stability of Cyberspace (2019): Advanced Cyberstability

[356] Republic of Korea (2020): Implementation of the 2015 UNGGE Norms

[357] Kaspersky (2020): Submission on 'Responsible state behaviour in cyberspace in the context of international security at the United Nations

[358] Department of Foreign Affairs and Trade (2020): Public Consultation: responsible state behaviour in cyberspace in the context of international security – Summary of public submissions on developing best practice guidance on implementation of the 11 norms of responsible state behaviour in cyberspace articulated in the 2015 GGE Report (A/70/174), as endorsed by the UN General Assembly (A/RES/70/237)

[359] Global Partners Digital (2020): DFAT Public Consultation: Responsible state behaviour in cyberspace in the context of international security at the United Nations

[360] Mika Kerttunen and Eneken Tikk (2021): PUTTING CYBER NORMS IN PRACTICE: Implementing the UN GGE 2015 recommendations through national strategies and policies

[361] Bart Hogeveen (2022): The UN norms of responsible state behaviour in cyberspace – Guidance on implementation for Member States of ASEAN

About the Author

Dr. Sven Herpig

Dr. Sven Herpig is interface’s Lead for Cybersecurity Policy and Resilience. He analyses the roles of government in various areas of cybersecurity policy, including operational parameters of cyber campaigns, responses to cyber operations, vulnerability management, securing machine learning and fostering open source software security.

Contact

Dr. Sven Herpig
Lead for Cybersecurity Policy and Resilience
sherpig@interface-eu.org
+49 (0) 30 81 45 03 78 91
bsky.app/profile/z-edian.bsky.social
github.com/z-edian/publications

Imprint

interface – Tech analysis and policy ideas for Europe
(formerly Stiftung Neue Verantwortung)

W www.interface-eu.org
E info@interface-eu.org

T +49 (0) 30 81 45 03 78 80
F +49 (0) 30 81 45 03 78 97

interface – Tech analysis and policy ideas for Europe e.V.
Ebertstraße 2
D-10117 Berlin

Layout & Infographics
Alina Siebert

Design by Make Studio
www.make.studio

Code
Convoy Interactive