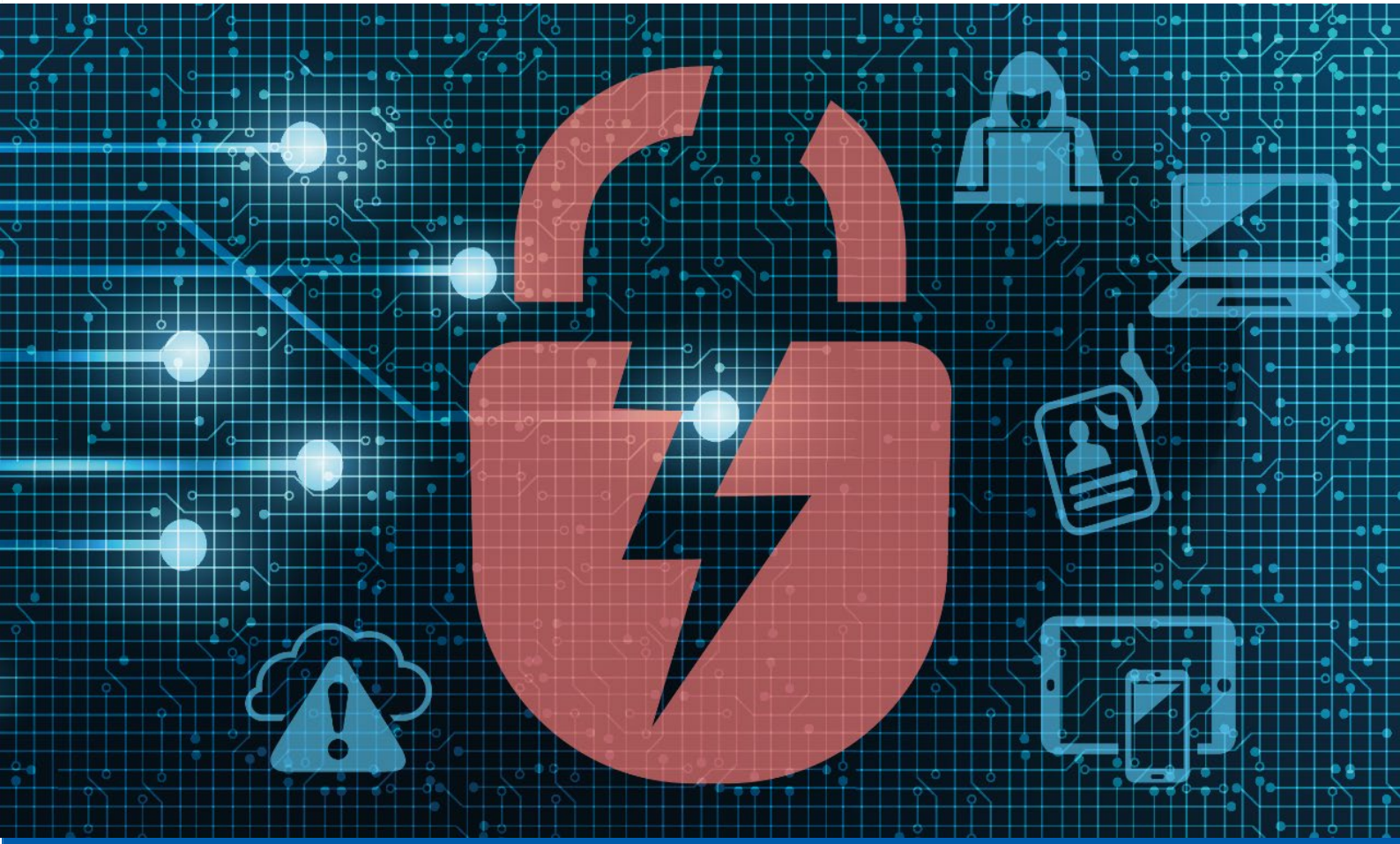
enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY



COORDINATED VULNERABILITY DISCLOSURE POLICIES IN THE EU

APRIL 2022

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: http://www.enisa.europa.eu/

CONTACT

To contact the authors, please use resilience@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu

CONTRIBUTORS

Débora Di Giacomo (Wavestone), Nick Conway (Wavestone), Aude Thirriot (Wavestone), Thiago Barbizan (Wavestone), Solène Drugeot (Wavestone), Cristian Michael Tracci (Wavestone), Lorenzo Pupillo (Centre for European Policy Studies (CEPS)), Carolina Polito (CEPS), Francesco Campoli (CEPS)

EDITORS

Evangelos Kantas (ENISA), Marnix Dekker (ENISA)

ACKNOWLEDGEMENTS

ENISA would like to thank the members of the Computer Security Incident Response Teams (CSIRTs) network and national competent authorities for participating in the interviews and providing valuable input and comments. Their contribution was essential in the development of this report.

LEGAL NOTICE

COPYRIGHT NOTICE

PDF	ISBN 978-92-9204-575-3	doi:10.2824/983447	TP-05-22-071-EN-N
Print	ISBN 978-92-9204-574-6	doi:10.2824/42129	TP-05-22-071-EN-C

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report analyses information and presents an overview of coordinated vulnerability disclosure (CVD) policies at the national level within the EU. Aside from offering a comprehensive overview of the EU CVD state of play, it also provides high-level key findings and recommendations for future improvements.

As shown by the recent Apache Log4j vulnerability, a single software flaw can put hundreds of millions of devices around the world at risk, leaving organizations struggling to patch affected systems before the vulnerability turns into a security incident. This is yet another vulnerability with global repurcussions that shows the importance of security research, communication between stakeholders, patching and good security practices.

A national CVD policy is a framework under which security researchers are allowed and encouraged to research ICT products and services, following a set of rules, and report any vulnerabilities they find to the national authorities or the product vendor. A national CVD policy helps to increase the overall level of cybersecurity in a country; it increases transparency, and this helps to build trust in the ICT services and products used in that country. In addition, it allows for valuable time and cooperation between stakeholders for patch development, which can potentially reduce the time for exploitation.

A national CVD policy helps to increase the overall level of cybersecurity in a country it increases transparency, and this helps to build trust in the ICT services and products used in that country.

At the national level, the research shows that, while evolving in a fragmented EU environment, multiple EU Member States are making progress in the development of national CVD policies. Currently, only Belgium, France, Lithuania and the Netherlands are undertaking CVD policy work and have implemented policy requirements. Among these four countries, policy initiatives strongly differ. In parallel, four other Member States are on the point of implementing a policy. In these cases, the proposal is either being examined at the level of policymakers or is being tested in pilot projects. Another set of ten EU Member States are considering implementing a national CVD policy or are on the point of doing so. However, failure to reach a consensus at the political or legislative levels hampered the process. Finally, another group of Member States (nine) has not implemented a CVD policy and the process for establishing one has not yet started.

This EU market heterogeneity could be explained by various challenges faced by national governments when considering CVD initiatives. These challenges include legal, economical and political aspects which are further addressed in this report. Additionally, the lack of alignment of CVD practices, terminology, understanding and assessment of a CVD process is perceived as an obstacle for the implementation of national CVD policies and cooperation between Member States.

More specifically, it turned out that the comprehensive CVD process is often, but not always, supported by national CSIRTs, which many countries see as the natural focal point for these activities. Good practices related to CVD policies and authorities' involvement have been shared by Member States representatives and collected in this report.

CVD policy initiatives carried out in China, Japan and the United States were also reported. These non-EU players presented various methods of creating and adapting a CVD national policy, and maintaining and working on vulnerability registries. These notions are further detailed aside from EU practices and illustrated with inspiring inputs from experts.

Furthermore, there are several challenges that were identified by the Member States and are presented for discussion, along with relevant recommendations that can help mitigate them and

support the implementation of national vulnerability disclosure policies. These challenges were identified and categorized based on their nature as legal, economic or political, and include findings such as:

- legal risks faced by researchers;
- limited economic incentives for vulnerability research;
- political challenges related to the role of the government and 'safe harbour' for researchers.

Lastly, following the analysis, several recommendations and concrete suggestions were presented for the role of the European Union Agency for Cybersecurity (ENISA) in supporting CVD in the EU. Some of the most important recommendations and suggested objectives are listed below.

Major recommendations

- Take the necessary steps to develop and implement national CVD policies.
- Define the role of ethical hackers in relevant national laws to establish a framework for ethical security research around vulnerabilities.
- Develop incentives for security researchers to actively participate in CVD research.

Role for ENISA and the European Commission

- Provide clear guidance to Member States on how to establish a CVD policy.
- Promote knowledge building and information exchange on CVD at the EU level.
- Encourage the harmonization of CVD initiatives across countries.

The information regarding the state of play of EU Member States presented herein was collected between Q2 and Q3 2021. Any updates to that status since then will be presented in future ENISA work.

1. INTRODUCTION

This ENISA study primarily aims to draw a comprehensive overview of the background and current state of play of coordinated vulnerability disclosure (CVD) practices across the EU Member States and outside the EU. First, the study presents a summary of the existing or planned national CVD policy initiatives along with good practices, challenges and recommendations on policy attempts. Second, the study offers an analysis of national, regional and global vulnerability databases, and presents the different practices on vulnerability and registry management along with the formats, metrics and procedures used in these databases.

National CVD policies

A national CVD policy is a framework under which security researchers are allowed and encouraged to research ICT products and services, following a set of rules, and report any vulnerabilities they find to the national authorities or the product vendor. A national CVD policy helps to increase the overall level of cybersecurity in a country and increases transparency. This helps to build trust in the ICT services and products used in that country.

Intended audience

The study is meant to be a source of information for any CVD stakeholder having an interest in the latest thinking on this topic. The intended audience for this report can be segmented into different CVD expert groups. These groups include policymakers and national authorities involved in coordinated vulnerability management initiatives; national Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs); and actors from the private sector owning an open-source or commercial database who want to learn about current CVD developments and good practices. Lastly, vendors and researchers are invited to treat the study as a support document in their activities.

Policy context

The current policy and legal context concerning CVD policies and vulnerability databases at the EU and international levels are framed by key developments such as the Budapest Convention on Cybercrime (2001), the Cybersecurity Act (2019) and the upcoming Network and Information Security 2 (NIS2) directive, where the proposal specifically states the involvement of CSIRTs in the national coordinated vulnerability processes. Nevertheless, further clarification and harmonisation actions are currently being discussed.

In addition, the NIS2 directive proposal describes the development of a European vulnerability database to support organizations and suppliers in registering, disclosing and monitoring vulnerabilities in ICT products and services. This vulnerability database will provide all interested parties with access to information describing the vulnerabilities; the affected products or services; the severity of vulnerabilities and the circumstances under which they can be exploited; and the availability of a patch or, in the absence of one, guidance regarding what steps must be taken by system administrators or users in order to mitigate the risks.

Methodology

The data collected through desk research related to CVD policy and registries helped contextualise findings and draw observations. Furthermore, 19 interviews were conducted with national competent authorities and CERTs. These interviews enriched secondary research and enabled the extrapolation of key findings with evidence-based input. An in-depth analysis and triangulation of the data collected resulted in key findings, a detailed description of analysis outcomes on the current CVD state of play in the EU and recommendations on planned EU CVD initiatives.

Structure

The report includes the following main sections.

- 'Coordinated vulnerability disclosure policies in the EU', which focuses on national vulnerability management policies, including information gathered from 19 interviews with national competent authorities and EU Member States' CERTs.
- 'Coordinated vulnerability disclosure policies outside the EU', which focuses on vulnerability disclosure policies and practices in the United States, China and Japan
- 'CVD policy practices', which analyses desired elements of CVD processes based on interviews with EU Member States, good practices observed within EU Member States and an analysis of the challenges involved in developing a national CVD Policy
- 'Recommendations', which provides comprehensive recommendations related to the issues addressed, aiming to improve the current state of play within the EU.

The information regarding the state of play of EU Member States presented herein was collected between Q2 and Q3 of 2021. Any updates to that status since then will be presented in future ENISA work.

2. COORDINATED VULNERABILITY DISCLOSURE POLICIES

2.1 STATE OF PLAY CVD POLICIES IN THE EU AND RELEVANT COUNTRIES AND REGIONS OUTSIDE THE EU

This Section presents an assessment of the state of play, good practices and challenges in the establishment of CVD policies across the European Union, and in some non-European countries, namely China, Japan, and the United States.

The findings are based on analysis and complemented with inputs from interviews shared by representatives from the Member States that either have a CVD policy in place, are in the process of implementing one or do not have any CVD policy in place. In particular, the interviews covered all countries that have established a CVD policy, most countries in the process of establishing a CVD policy or on the point of establishing one and a selection of countries with no CVD policy in place. The representatives to be interviewed were selected in such a way as to guarantee an adequate representation while taking into account the various regions and countries' sizes. This information was complemented with a detailed analysis of the best practices and challenges, particularly legal challenges, that should be highlighted in the context of the establishment of CVD policies across the EU.

More specifically, this overview encompasses:

- the state of play CVD policies in the EU and a number of relevant non-EU countries and regions outside the EU;
- an overview of good practices in CVD, including a template CVD policy and procedure, bringing together the good practices and ideas collected from the different countries;
- an overview of challenges and issues, including technical, policy, economic and legal issues;
- possible solutions and recommendations to address these challenges and issues.

2.2 STATUS OF CVD POLICIES IN THE EU

The state of implementation of national CVD policies across the Member States shows that substantial differences exist among them. The research shows that while evolving in a fragmented EU environment, **multiple Member States are making progress in the development of national CVD policies but at different rates.**

The Netherlands lead the EU's efforts in establishing CVD policies. Together with the Netherlands, France, Belgium and Lithuania are the only countries which have a fully established national CVD policy. Some Member States (4) are on the point of implementing a policy. In these cases, the proposal is either being examined at the level of policymakers or is being tested in pilot projects. Several Member States (10) are in the process of implementing a national CVD policy or are on the point of doing so. However, failure to reach a consensus at the political or legislative levels hampered the process. Finally, another group of Member States (9) has not implemented a CVD policy and the process for establishing one has not yet commenced.

Most of the Member States without a CVD policy in place expressed the intention of establishing one in the future, especially in the context of the national transposition of the NIS2 directive. Very few Member States seem to be opposed to implementing a CVD policy. In some cases, this is because current practices or legal frameworks in place in the countries already allow CVD processes to take place even without a formal policy. Figure 1 and Table 1 provide an overview of the implementation of CVD policy at the national level in the EU.

Table 1 – Implementation of CVD policy at the national level in the EU

Country	Status	CVD policy at the national level
Belgium	Belgium has an established CVD policy that envisages full protection of the researcher acting in the scope of an existing policy.	Implemented
Bulgaria	Bulgaria hasn't yet implemented a CVD policy, but the national CERT is involved in the establishment of CVD practices.	Not implemented
Czechia	Czechia does not have a CVD policy in place. The national CERT is assessing different options for reducing vulnerabilities, including creating a national CVD policy.	In progress
Denmark	Denmark is in the initial phase of its pilot CVD project.	On the point of implementing
Germany	Germany does not have a national regulation on CVD. A CVD policy by the Bundesamt für Sicherheit in der Informationstechnik (BSI) is about to be published. It should be regarded as the German national policy.	On the point of implementing
Estonia	Estonia hasn't yet implemented a CVD policy. Vulnerabilities are handled through an array of strategies that the country has in place.	Not implemented
Ireland	Ireland does not have a policy in place, and implementing one is not regarded as a priority.	Not implemented
Greece	Greece hasn't yet implemented a CVD policy but takes a positive stance on the idea of establishing one.	In progress
Spain	Spain does not have a national CVD policy. A CVD framework has been partially established at the level of the Spanish	In progress

	Government National Cryptologic Center - Computer Security Incident Response Team (CCN-CERT) and INCIBE-CERT.	
France	France has an established CVD policy. Art 47 (art. L 2321-4 Code de la défense) creates a safe harbour for vulnerability reporters when certain legal criteria are met.	Implemented
Croatia	Croatia hasn't yet implemented a CVD policy and there is no plan to implement one at this stage.	Not implemented
Italy	Italy does not have a CVD policy in place. Discussions on amendments to the criminal code might be pushed forward in light of the NIS2 directive.	In progress
Cyprus	Cyprus does not have a formal policy for CVD in place. A policy might be established in response to the more formal obligation stemming from the NIS2 directive.	Not implemented
Latvia	Latvia does not have a CVD policy in place, but by the end of the year the country will put in place a formal voluntary CVD policy for state institutions.	On the point of implementing
Lithuania	Lithuania has a national CVD policy in place, formalised in the amendment to the law on cybersecurity of the Republic of Lithuania.	Implemented
Luxembourg	Luxembourg has no formal CVD policy in place. A CVD policy has been released by the national CERT and there are ongoing discussions on a CVD policy.	In progress
Hungary	Hungary hasn't yet implemented a CVD policy. There are ongoing negotiations regarding amendments to the Hungarian cybersecurity act ,specifically to include vulnerability disclosure requirements.	In progress
Malta	Malta hasn't yet implemented a CVD policy and there is no plan to implement one at this stage.	Not implemented
The Netherlands	The Netherlands has an established CVD policy that guarantees full protection for researchers.	Implemented

Austria	Austria does not have a CVD policy in place at this time but is considering whether to include a CVD policy in the national transposition of the NIS2 directive.	In progress
Poland	Poland does not have a CVD policy in place. In 2017, security breaches were partially decriminalised to improve the protection of researchers.	Not implemented
Portugal	Portugal does not have a CVD policy in place but a task force has been established to develop a CVD policy. The task force presented a proposal with a comprehensive list of legislative amendments. The proposal is now being examined by decision-makers.	On the point of implementing
Romania	Romania hasn't yet implemented a CVD policy and no progress in this direction has been made.	Not implemented
Slovenia	Slovenia hasn't yet implemented a CVD policy. The country is planning to include a CVD policy in the next cybersecurity strategy.	In progress
Slovakia	There is no CVD policy in place, while at the legislative level there are implicitly established processes regarding CVD.	In progress
Finland	Finland has no CVD policy in place but it has begun efforts in this direction. Besides, a CVD policy has been released by the national CERT.	In progress
Sweden	No CVD policy in place at the national level and there is no plan to implement one at this stage.	Not implemented

Figure 1 presents a mapping of the state of play in the implementation of CVD policies in the EU Member States. The map divides countries based on a scale of (1) to (4), where (1) indicates that the country has a policy in place and (4) indicates that the country has no policy in place. The values in between indicate either that the process of implementing a policy is in progress, or that the country is just on the point of implementing one.

From the mapping of the state of play of CVD implementation, a geographical consideration that could be drawn is the relative greater maturity of western European countries compared to other European regions. Conversely, southern European countries and central and eastern European countries are lagging behind in this process.

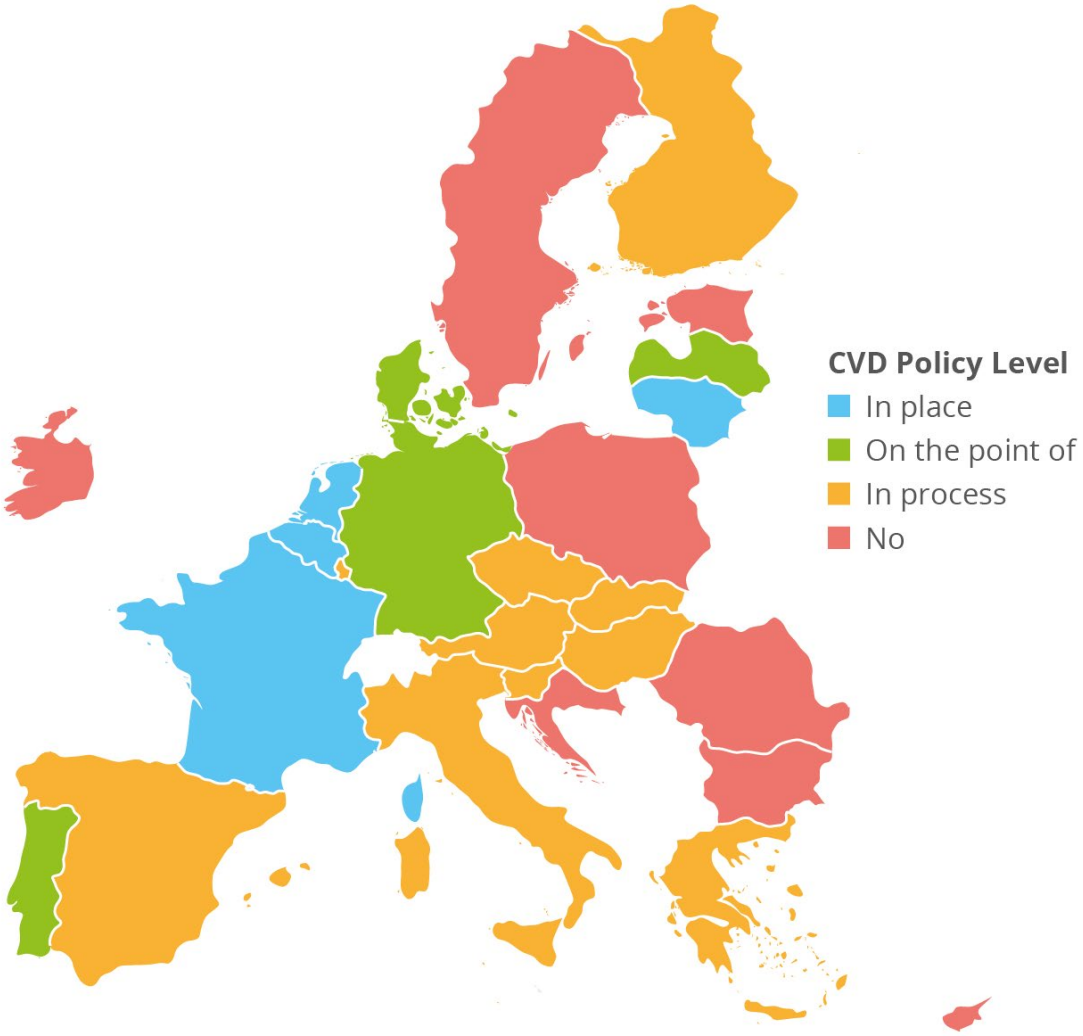


Figure 1 – Implementation of CVD policy at the national level in Europe

2.3 CVD WITHIN EACH MEMBER STATE

2.3.1 Belgium

IMPLEMENTED

Since 2018, the **Centre for Cyber Security Belgium (CCB)** has worked in collaboration with the Public Prosecution Service, the vulnerability reporter community, the private sector and public authorities on the development of a national approach to CVD policies. The national CVD policy is a formal policy explicitly included in the Belgian cybersecurity strategy (adopted by the National Security Council and the Prime Minister's Office) and in the CCB baseline security guidelines (adopted by the CCB management). In 2019, the CCB adopted, as an example to

other organisations, a CVD policy for its website[1]. In December 2020, the CCB published national guidelines to encourage all Belgian organisations to adopt a CVD policy or a bug bounty[2].

The policy promotes the adoption of coordinated vulnerability disclosure guidelines for private and public entities and is divided into the following different documents: Guide part I – Good practices; Guide part II – Legal aspects; an example of policy; a folder; and FAQs. The CCB is in charge of the implementation of the national CVD policy and it provides a template of policy. The national CVD policy attributes a role to the CCB (with its CERT team) as a CVD coordinator by default (even when there is no CVD policy put in place by the concerned organisation). If a vulnerability is not yet known and threatens to have a direct or indirect impact elsewhere, the organisation responsible for identifying it must inform the CCB and the other organisations potentially concerned, even if it does not want the vulnerability to be made public.

Without modification of the existing legal framework, those guidelines clarify the legal situation of the researchers when the organisation has adopted a CVD policy and attributes a role to the CCB (with its CERT team) [3] as a CVD coordinator by default (even when there is no CVD policy in place).

In Belgium, a CVD policy or a bug bounty is considered as a type of accession agreement, which is usually published on a website, outlining the contractual provisions between the responsible organisation and the researchers (accepted by them when they freely decide to participate in the policy). Subject to compliance with the mutual obligations described in the policy, the adoption of such a policy implies an authorisation from the responsible organisation for the researchers to access or to try to access, with good intentions, the concerned IT systems to identify possible vulnerabilities or to provide any relevant information about the security of its IT systems. Therefore, the access or the attempts to access those IT systems by the researchers are lawful, as long as the pre-determined rules of the CVD are met. These rules should ensure, among other things, the confidentiality of the information exchanged and provide a responsible and coordinated framework for any disclosure of discovered vulnerabilities. The term ‘disclosure’ does not necessarily mean that the vulnerability will be made public, but rather that the participant communicates it to the responsible organisation. The participant is obliged to communicate the vulnerability to the responsible organisation, but the public disclosure of the vulnerability (by the participant or the organisation concerned) is optional and must be coordinated. If a vulnerability is not yet known and threatens to have a direct or indirect impact elsewhere, the organisation concernedmust inform the CCB and the other organisations that are potentially involved, even if it does not want the vulnerability to be made public.

The CCB policy is presented in detail in the Annex.

There are quite a few organisations in Belgium that have a CVD or a bug bounty policy in place: Roximus, Telenet, Voo, Base, SNCB, Brussels Airlines, Port of Antwerp, VRT, Kinepolis, KUL, Randstad, Itsme, New pharma, Cybersecurity coalition, Tomorrowland, Torfs and Dpg Media. Furthermore, there is an important bug bounty platform (Intigriti) that is based in Belgium and has coordinated some of those policies.

[1] Centre for Cyber Security Belgium, ‘CCB coordinated vulnerability disclosure policy’. Available at: https://ccb.belgium.be/en/vulnerability-policy
[2] Centre for Cyber Security Belgium, ‘Coordinated vulnerability disclosure policy and vulnerability detection reward program (bug bounty)’. Available at: https://ccb.belgium.be/fr/politique-de-divulgation-coordonnée-de-vulnérabilités-et-programme-de-récompense-pour-la-découverte
[3] The CCB plays the role of national CSIRT in the sense of the NIS directive.

2.3.2 Bulgaria

NOT IMPLEMENTED

Bulgaria has not yet implemented a CVD policy, although as of 2018, the national CERT was hopeful to start a discussion on CVD as soon as possible[4].

CERT Bulgaria is, nonetheless, already involved in the establishment of CVD practices. CERT Bulgaria uses an internal portal to which each of the users has access. The portal includes an 'installation database', in which each user has indicated the type of software and hardware employed. Daily information is collected from the US National Vulnerabilities Database (NVD) on newly discovered vulnerabilities. This information is matched with the installation database and the constituents receive an email with vulnerabilities relevant to the software and hardware it uses. The constituents can see the same information on their profiles by entering the portal.

In fulfilment of its proactive obligations, CERT Bulgaria prepares and sends monthly bulletins. It publishes brief statistical information on the most recent attacks and/or threats with the most important recommendations on how to counteract them and information on the published vulnerability bulletins of Microsoft, CISCO, Adobe and others popular vendors used by our constituents.

In this respect, while the 2020 national cybersecurity strategy[5] does not mention CVD, the document lays down the main measures that will need to be achieved to meet the security objectives set out in the NIS directive. Among others, the strategy put forward the 'development of the minimum required capacity of the individual CERT/CSIRTs' and 'the expansion of the scope, capabilities and functions of the Security Operations Center (SOC)'. In addition to incident and attack response activities, SOCs cover all aspects related to cybersecurity, such as awareness raising, resilience, detection, disclosure, crisis reporting and management.

2.3.3 Czechia

IN PROGRESS

While there is no CVD policy currently in place, the **National Cyber and Information Security Agency (NÚKIB)** is continuously assessing ways of reducing vulnerabilities, including creating a national CVD policy. In 2018, the governmental CERT (part of NÚKIB) mentioned CVD as a topic that the country needs to catch up with and in the *National Cyber Security Strategy of the Czech Republic* (2021), there is a reference to a 'coordinated approach of private and public entities in cybersecurity'. In the proposal of the *Action plan for the national cyber security strategy of the Czech Republic for the period from 2021 to 2025*, there is a task to prepare a proposal for a national CVD policy in 2021. Also, in the *25 Years of the Czech Republic's OECD Membership* report, the country pledged to include CVD as a tool that should be adopted in national programs and standards.

Furthermore, the Czech National Cyber and Information Security Agency has established close cooperation with selected private companies to exchange information about cybersecurity threats, trends and best practices. The National Security Agency has an agreement on the government's security programme with Microsoft and Cisco, under which 'the parties can share and exchange cybersecurity information, which means that the NSA has access to these

[4] Pupillo, L., Ferreira, A. and Varisco, G. (2018). Software Vulnerability Disclosure in Europe: Technology, policies and legal challenges – Report of a CEPS Task Force, CEPS Task Force Reports, 28 June 2018.
[5] Republic of Bulgaria Council of Ministers (2016), National Cyber Security Strategy 'Cyber Sustainable Bulgaria 2020' (Национална стратегия за киберсигурност 'Киберустойчива България 2020'). Available at: https://www.strategy.bg/StrategicDocuments/View.aspx?lang=bg-BG&Id=1120

companies' products' source codes and documentation'. However, by no means could this memorandum of understanding substitute establishing a CVD mechanism.

2.3.4 Denmark

ON THE POINT OF IMPLEMENTING

Denmark has not yet implemented a CVD policy; however, the country is in the initial phase of its pilot CVD project.

As part of the *Danish Cyber and Information Security Strategy 2018–2021* (initiative 1.7), a draft on a governmental CVD policy framework has been prepared. The strategy mentions that communications concerning cyber threats are the responsibility of the **Danish Centre for Cyber Security** in collaboration with the relevant sectoral authority. Communication will need to be coordinated in the event of a major, cross-sectoral incident, under the responsibility of the central operational communication staff (DCOK). 'The DCOK is responsible for ensuring rapid disclosure and coordination of relevant information to the general public, including to the media' [6]. No further details are provided in the strategy.

2.3.5 Germany

ON THE POINT OF IMPLEMENTING

Formally, Germany does not have a national regulation on CVD. The **German Federal Office for Information Security (BSI)** has, nonetheless, a policy in place which will be published after approval by BSI management and the relevant ministries. Processes related to reporting within the federal administration to the BSI and by the BSI have been established for dealing with vulnerabilities (cf. § 4 Paragraph 2-4 BSIG). According to this, all federal authorities must report to the BSI any information in connection with newly identified vulnerabilities that are important for the performance of tasks or the security of the information technology of other authorities.

All the vulnerabilities found are reported to the affected manufacturer via the BSI so that they can act accordingly. The aim of the procedure is to minimise damages resulting from the possible exploitation of vulnerabilities. On the one hand, the coordinated participation of affected manufacturers enables functioning security updates to be provided. On the other hand, the temporary retention of vulnerability and attack details reduces the potential damages.

Currently, the BSI policy should be regarded as the German national policy, as this authority is the focal point for CVD. In this context, it is not expected for other public entities in Germany to publish another formal CVD policy.

The **Bundeswehr** (German armed forces) has also published, on 21 October 2020, its vulnerability disclosure policy [7]. The policy applies to Bundeswehr IT systems and web applications that are connected to and accessible over the internet, particularly the websites of the Bundeswehr [8]. The program affects all digitally accessible systems of the Bundeswehr, i.e. their hospitals (Berlin, Koblenz, etc.), universities (Munich and Hamburg) and others.

This policy cannot be used to prepare or transmit vulnerability reports in third-party programs without the consent of the Bundeswehr. The Bundeswehr guarantees that researchers will be

[6] The Danish Government Ministry of Finance (2018), Danish Cyber and Information Security Strategy, May. Available at: https://digst.dk/media/16943/danish_cyber_and_information_security_strategy_pdfa.pdf
[7] Bundeswehr (2021), 'Vulnerability disclosure policy der Bundeswehr (VDPBw)'. Available at: https://www.bundeswehr.de/de/security-policy
[8] Bannister, A. (2020), 'German armed forces launch security vulnerability disclosure program', The Daily Swig, 27 October. Available at: https://portswigger.net/daily-swig/german-armed-forces-launch-security-vulnerability-disclosure-program

kept informed about the validity and remediation of any bugs reported, with successful submissions being recognised on an acknowledgements page. At present, there are no plans to offer bug bounties for successful submissions.

GERMANY – Bundeswehr vulnerability disclosure policy [9]

The Bundeswehr published its vulnerability disclosure policy on 21 October 2020. Whenever a vulnerability is discovered, researchers should proceed as follows.

- Before you report, find out about the cases that do not fall within the scope of our Bundeswehr vulnerability disclosure policy and are not dealt with in this context.
- Use the contact form to get in touch with us about the security problem or send your results by email to security@bundeswehr.org. Encrypt your documentation with our Pretty Good Privacy (PGP) key so that this sensitive information does not fall into the wrong hands. To optimise communication between you and the central reporting office in the Bundeswehr, we ask you to use the format template provided.
- Do not exploit the vulnerability or problem by, for example, downloading, changing or deleting data, or uploading code.
- Do not pass on information about the vulnerability to third parties or institutions unless this has been approved by the Bundeswehr.
- Do not carry out any attacks on our IT systems that compromise, change or manipulate infrastructure and people.
- Do not carry out social engineering (e.g. phishing), (distributed) denial of service, spam or other attacks on the Bundeswehr.
- Provide us with sufficient information so that we can reproduce and analyse the problem. Also, provide a contact option for questions.

Bundeswehr commitments include the following.

- We will try to end the vulnerability as soon as possible.
- You will receive feedback from us on the receipt of your report and on your report.
- If you follow the instructions of the Bundeswehr security policy, the law enforcement authorities will not be informed of your connection to the findings. This does not apply if it is evident that criminal or intelligence intentions are being pursued.
- We will treat your report confidentially and will not pass your personal data on to third parties without your consent.
- We will inform you of the receipt of your report, as well as the validity of the vulnerability / IT security gap and the elimination of the problem during the processing period.
- The finder is judged according to his abilities and not according to age, education, gender, origin or social rank. That is why we show this respect publicly and recognise this achievement. In addition, if nothing else is desired, we will describe the closed vulnerability and the name (or alias) of the discoverer on our ‘thank you’ page, to publicly express our good cooperation with the Bundeswehr.

[9] This section draws from the vulnerability disclosure policy of the Bundeswehr (VDPBw). Available at: https://www.bundeswehr.de/de/security-policy

Qualified reporting of weak points:

- Cross-site request forgery (CSRF)
- Cross-site scripting (XSS)
- Insecure direct object reference
- Remote code execution (RCE) – Injection flaws
- Information leakage and improper error handling
- Unauthorised access to properties or accounts and much more

The Bundeswehr also provide the format template to be followed to report a vulnerability.

2.3.6 Estonia

NOT IMPLEMENTED

Estonia has not yet implemented a CVD policy and the *Cybersecurity Strategy for 2019–2022 of the Republic of Estonia* does not elaborate on possible mechanisms for CVD [10].

However, vulnerabilities are handled through the array of strategies and institutions that the country has in place. For example, the Department of Standards and Supervision has overseen the development of a new standard on information security (which should be enforced in January 2022). The supervisory authority regularly oversees public sector institutions on standards' implementations. Besides, the Department of Analysis and Prevention carries out cybersecurity analysis based on the data gathered by the national CERT and conducts prevention campaign (e.g. yearly awareness-raising campaign on cyber hygiene). Estonian private companies and academia are active in vulnerability disclosure, but the cooperation between these actors and the governmental agencies is not formalised.

In 2018, after the Return of Coppersmith's Attack (ROCA) vulnerability in the eID systems was discovered, the **Estonian Information System Authority** (EISA) suggested vulnerability disclosure as a possible solution to prevent these types of incidents from happening again. In particular, EISA mentioned that 'anticipated sources of information – international notification mechanisms and notification from vendors – failed Estonia this time while the information provided by an international group of researchers allowed to address the issue'. The notification mechanisms are designed for incidents with significant impact and thus not ideal when addressing vulnerabilities in earlier stages of crises, as in the case of ROCA. According to EISA, the episode could have allowed to revisit the notification mechanism, involving vulnerability sharing to be addressed jointly [11].

2.3.7 Ireland

NOT IMPLEMENTED

Ireland does not have a policy in place and does not consider implementing such a policy as a priority. According to the Irish government, the matter should be regulated at the EU level rather

[10] Republic of Estonia Ministry of Economic Affairs and Communications (2019), *2019–2022 Cybersecurity Strategy – Republic of Estonia*. Available at: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf
[11] Republic of Estonia Information System Authority (2018), 'Estonia offers recommendations in the light of eID vulnerability', May. Available at: https://www.ria.ee/en/news/estonia-offers-recommendations-light-eid-vulnerability.html

than at the national level. The *National Cyber Security Strategy* for 2019–2024 does not mention CVD [12].

2.3.8 Greece

IN PROGRESS

Greece has not yet implemented a CVD policy. However, the country takes a positive stance on the idea of establishing one.

Besides, the *National Cybersecurity Strategy* (2020–2025), envisages establishing a trusted information-sharing mechanism through, among others: the 'installation of an open-source platform for vulnerability assessment and conduction of Penetration Tests (Flagship activity 3.A.8)' [13]. No further indication is provided.

2.3.9 Spain

IN PROGRESS

Spain does not have a formal national CVD policy. However, a vulnerability disclosure policy framework has been partially established at the level of **CCN-CERT** and **INCIBE-CERT** (i.e., National Institute of Cybersecurity of Spain).

Art. 37.1(a)(d) of the Royal Decree regulating the National Security Framework in the area of e-government establishes the role of CCN-CERT as 'vulnerability coordinator' for the public sector institutions' IT systems [14]. According to the issued decree, the CCN-CERT will provide the public administrations with the following services.

- Support and coordination for treating vulnerable aspects and solving security incidents taking place in the General State Administration, regional administrations, entities comprising local administrations and public law entities with their legal status, that are linked to or depend on any of the preceding administrations.
- Information about vulnerable aspects, alerts and warnings of new threats to information systems, gathered from different sources of renowned prestige, including own sources.

INCIBE-CERT is the reference security incident response centre in Spain. Art. 11.1 a) 2º and b) of the decree-law for the NIS transposition[15] establishes the role of INCIBE-CERT as the reference CERT/CSIRT for private companies and the citizens. Among the different services that INCIBE-CERT provides to these subjects, there is the coordination of vulnerabilities. Art. 11.2 of the decree-law establishes that the CERTs/CSIRTs will coordinate with each other and with the rest of the national and international CSIRTs in responding to incidents and managing security risks. The security risks include the managing and coordination of vulnerabilities. INCIBE-CERT provides support to those who want to provide information on vulnerabilities detected in either INCIBE-CERT or third-party systems, for private companies and citizens. INCIBE-CERT also acts as the Spanish CNA (CVE numbering authority) for

[12] Government of Ireland (2019), *National Cyber Security Strategy*, December. Available at: https://www.gov.ie/en/publication/8994a-national-cyber-security-strategy/
[13] National Cyber Security Authority (2018), *National Cyber Security Strategy – Version 3.0*. Available at: https://ccdcoe.org/uploads/2018/10/Greece_National-Cyber-Security-Strategy-ver.3.0_EN.pdf
[14] Gobierno de España Ministerio de la Presidencia, Relaciones con las cortes y memoria democrática (2010), Royal Decree 3/2010, of 8 January, regulating the National Security Framework in the area of e-Government, Agencia Estatal Boletín Oficial del Estado. Available at: https://www.boe.es/eli/es/rd/2010/01/08/3/con
[15] Gobierno de España Ministerio de la Presidencia, Relaciones con las cortes y memoria democrática (2018),Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, Agencia Estatal Boletín Oficial del Estado. Available at: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-12257

management and vulnerability discovery practices, under MITRE and CVE program and statements[16].

SPAIN – INCIBE-CERT CVD policy[17]

INCIBE-CERT sets out the actions that are not allowed in the search for vulnerabilities.

- Using social engineering.
- Compromising the system and persistently maintaining access to it.
- Changing the data accessed by exploiting the vulnerability.
- Using malware.
- Using the vulnerability in any way beyond proving its existence. To demonstrate that the vulnerability exists, the reporter could use non-intrusive methods. For example, listing a system directory.
- Using brute force to gain access to systems.
- Sharing vulnerability with third parties.
- Performing DoS or DDoS attacks.

The INCIBE-CERT also sets out the steps that should be followed to report a vulnerability, i.e. send the (ideally) encrypted information to incidencias@incibe-cert.es

The following information is required to report a vulnerability.

- A clear and detailed description of the vulnerability.
- Clear and detailed information on how the vulnerability was discovered. The objective is to be able to reproduce it.
- Other information that may be useful when reporting the vulnerability, such as proof of the existence of the vulnerability (screenshot, link, etc.); timeline or some information about the moment the vulnerability was discovered; any type of information deemed necessary to locating and resolving the vulnerability in the fastest and most efficient way possible.

Once the notification is received, INCIBE-CERT will confirm receipt and begin communication with the interested party. If the vulnerability involves a Critical Infrastructure Operator, INCIBE-CERT also has different contact points to facilitate communication and ensure the notification has been correctly received. In addition, its specialised technical team offers support to mitigate and resolve the vulnerability as soon as possible. Once the vulnerability is communicated, periodic follow-ups are carried out until the standard term set by the INCIBE-CERT. Whether the management of the vulnerability is successful, or if the actor responsible for managing the vulnerability has not taken sufficient measures to remedy it within 60 days, INCIBE-CERT will issue a notice publishing the vulnerability together with the reporter if he wants. Researchers are not

[16] CVE numbering authorities (CNAs) are organisations from around the world that are authorised to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities. These CVE IDs are provided to researchers, vulnerability disclosers and information technology vendors. See CVE, 'CVE numbering authorities'. Available at: https://cve.mitre.org/cve/cna.html

[17] This Section draws from INCIBE-CERT, 'Vulnerability disclosure policy'. Available at: https://www.incibe-cert.es/en/what-is-incibe-cert/vulnerability-disclosure-policy

economically rewarded by INCIBE-CERT. Nonetheless, if the person reporting the vulnerability desires, it will offer its communication channels as a promotion for the disclosure.

2.3.10 France

IMPLEMENTED

France has established a CVD policy in 2016. If a researcher reports a suspected vulnerability to theAgence nationale de la sécurité des systèmes d'information (ANSSI)[18], Art. 47 of the Law for a Digital Republic supersedes Art. 40[19]. Art. 47 exempts the researcher ('goodwill person') who reports the vulnerability from the provisions contained in Art. 40. The agency must also protect the confidentiality of the identity of the researcher who reports the vulnerability[20].

Art. 47 (art. L 2321-4 Code de la défense) creates a safe harbour for vulnerability reporters when two legal criteria are strictly met, constituting a statutory derogation to French criminal law (Art. 40 Code de procédure pénale).

1. Researchers reporting a vulnerability must act in good faith i.e., either knowing that they act within the boundaries of the legal framework, or that they reasonably ignore that they are acting outside of the legally authorised scope.
2. Vulnerabilities must be reported to ANSSI exclusively – no other public institution can receive a vulnerability notification and meet Art. 47's legal criteria to create a safe harbour.

When those two criteria are strictly met, the following applies.

1. Vulnerability discovery will not be prosecuted even if it should normally amount to a crime.
2. ANSSI can protect the vulnerability's owner identity and anonymise the vulnerability report and any information relating to the vulnerability's discovery.

ANSSI oversees the implementation of the law and provides guidance and procedures allowing researchers to benefit from the safe harbour. Besides, ANSSI contribute to the registration of vulnerabilities to MITRE when coordinating vulnerability disclosures with both researchers and vendors. CERT FR provides a list of security alerts, including vulnerability information, however, vulnerability reporting is limited to a set of organisations operating in France and having incident response teams.

Notably, a comprehensive CVD policy inspired by current state-of-the-art recommendations (ISO norms, etc.) is currently under review by ANSSI.

2.3.11 Croatia

NOT IMPLEMENTED

[18] The country's computer security service, created in 2009.
[19] Art. 47 and Art. 40, Available at: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000033206854/
[20] Pupillo, L., Ferreira, A., & Varisco, G. (2018). Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges. Report of a CEPS Task Force. CEPS Task Force Reports 28 June 2018

Croatia has not yet implemented a CVD policy and there is no plan to implement one at this stage. The latest *National Cyber Security Strategy of the Republic of Croatia* is from 2015 and does not mention responsible disclosure or CVD[21].

2.3.12 Italy

IN PROGRESS

Currently, Italy does not have a CVD policy in place. The **Department for the Digital Transformation within the Presidency of the Council of Ministries** in 2018 (named Digital Transformation Team at that time) drafted a CVD policy that aimed to be general and potentially able to cover both the private and public sectors. The work has been carried out in collaboration with the national CERT. A pilot programme aimed at supporting private companies in implementing CVD policies and improving internal/external processes has been prepared, but since then no progress has been made due to the lack of legal certainty regarding the protection of researchers.

Within the discussion around the NIS2 directive, the discussion on CVD picked up and some players that were against changing the legal code seem now to be more inclined towards introducing a CVD policy. Italy is proposing an amendment to the text of NIS2 directive aiming at facilitating the establishment of a CVD policy within Member States, by the time the NIS2 will be received for the national transposition. The proposed amendment to the NIS2 text states that the Member States should define the conditions according to which the identification and disclosure of vulnerabilities would not entail a breach of criminal law. According to Italy, leaving the discretion to the judges in deciding what constitutes unauthorised access to a system would be alarming as every judge would have the freedom to establish, according to his parameters, what should be considered ethical hacking and what should not

Many private companies, such as the TIM Group (formerly Telecom Italia Mobile), have CVD policies in place and published on their website. However, according to the current penal code in Italy, these companies would still be able to sue the security researchers.

2.3.13 Cyprus

NOT IMPLEMENTED

Cyprus does not have a formal policy for CVD in place, although a policy might be established in response to the more formal obligation stemming from the NIS2. The country has consolidated the **national CSIRT** through the development of appropriate procedures and information exchange interfaces for the effective response to and management of incidents.

Incident response mechanisms have been identified and codified in relevant secondary legislation, but no CVD is envisaged[22]. The *Cyber Security Strategy of the Republic of Cyprus 2020* mentions that 'in addition to exchanging information regarding threats and cyber incidents, information exchange about systems' vulnerabilities should also be promoted, offered by the Cypriot market, in coordination with companies and customers vulnerability disclosure'[23].

[21] Republic of Croatia Ministers of Interior (2015), 'The National Cyber Security Strategy of the Republic of Croatia' (*Official Gazette* No 108/2015). Available at: https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian20National20Cyber20Security20Strategy20(2015).pdf
[22] The Network Law on Security of Networks and Information Systems of 2018 Third Annex (Part II) of the *Official Journal of the European* Union (2019), 7 June. Available at: https://dsa.cy/wp-content/uploads/Decision-218-2019.pdf
[23] Authors' translation in English from the original text, Ministry of Research, Innovation and Digital Politics (2020), *Government Security Strategy of the Republic of Cyprus Cybersecurity Strategy of the Republic of Cyprus 2020* (ΥΦΥΠΟΥΡΓΕΙΟ ΕΡΕΥΝΑΣ, ΚΑΙΝΟΤΟΜΙΑΣ ΚΑΙ ΨΗΦΙΑΚΗΣ ΠΟΛΙΤΙΚΗΣ ΑΡΧΗ ΨΗΦΙΑΚΗΣ ΑΣΦΑΛΕΙΑΣ έγγραφο Πολιτικής Στρατηγική Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας 2020).

If a CVD policy is to be established, it will most likely be developed by the Digital Security Authority (DSA) – which includes the national CSIRT. The handling and management processes will instead be implemented by the national CSIRT.

2.3.14 Latvia

ON THE POINT OF IMPLEMENTING

Latvia does not have yet a CVD policy in place, but the country is in a transition phase. Indeed, by the end of the year, Latvia will put in place a formal policy encouraging state institutions to implement a CVD policy. This will provide state institutions with a policy template and will designate responsible entities that will be in charge of the implementation of the policy. For now, there are some institutions and organisations that have voluntary CVD published. **CERT Latvia** has led by example with the publication of its vulnerability disclosure policy.

Initially, the policy will be voluntary and **CERT.LV** will provide support during the implementation and act as a coordinator among the involved parties in the CVD process. After the report is published, the implementation steps will continue in close cooperation between the Ministry of Defence (MoD) and **CERT.LV**.

Besides, the latest *Cybersecurity Strategy of Latvia* (2019) envisages the definition of a CVD policy. 'Following the principles described in National Defence Concept,' the strategy reads, 'it is necessary to develop regulations on responsible security vulnerability disclosure, which are important for ICT security, addressing of gaps and vulnerabilities and encouraging system designers and operators be more responsible (Activity 2.1)'[24].

Already since 2016 Latvia has been taking steps towards the definition of a CVD policy. In 2016 the MoD proposed to address the responsible disclosure policy (RDP) / CVD process via legislation. In particular, the proposal intended to specify the responsible disclosure process in the law on IT security. This proposal attempted to address the lack of a framework establishing the steps to take after a vulnerability was discovered by a researcher, and the lack of protection for researchers. A multi-stakeholder working group was established to discuss the best approach to include RDP in the law. Legal experts, security researchers, cyber policy experts, CERT.LV and several other groups and institutions were represented in this working group. Unfortunately, the proposal failed to convince all involved parties and was not accepted. Retrospectively, according to representatives from the MoD of the Republic of Latvia, it can be admitted that the proposal was cumbersome. This is also one of the reasons why the policy framework that is currently being proposed is voluntary.

Some organisations in Latvia have published their CVD policies, for instance, in the banking sector JSC Swedbank (as early as 2015) and JSC SEB Banka. CERT.LV has led by example with the publication of its vulnerability disclosure policy.

LATVIA – CERT.LV responsible disclosure policy [25]

We support responsible security vulnerability disclosure policy and principles and welcome any security researchers to report security flaws in the CERT.LV services and resources (cert.lv domain). We expect reports about vulnerabilities such as XSS, encryption flaws, remote code execution, etc.

[24] Latvian Defence Ministry (2019), Informative report 'Latvian cyber security strategy for 2019–-2022', (Informatīvais ziņojums'Latvijas kiberdrošības stratēģija 2019.–2022. gadam'). Available at: https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf
[25] CERT.LV, 'Responsible disclosure policy'. Available at: https://cert.lv/en/about-us/responsible-disclosure-policy

How can you report? If you believe you have discovered a vulnerability in the CERT.LV services, please contact us at cert@cert.lv and include the following information:

- a detailed description of the vulnerability;
- detailed information about the exploitation of the vulnerability;
- if applicable, a link, screenshot or any other information that could help to identify the vulnerability you have found.

We prefer that you use CERT.LV PGP key (https://cert.lv/en/contacts) to protect the information you are sending. We will keep you updated while we solve the issue and inform you when the vulnerability is fixed.

What do we expect from you? It is important that you follow good practices.

- You should not use the vulnerability to access or attempt to access information that does not belong to you (only to prove the existence of the vulnerability).
- You should not use the vulnerability to remove or modify the information.
- You should not affect the availability of our services through denial of service (DoS) attacks.
- You should not make any social engineering attacks.
- We would appreciate you letting us fix the reported vulnerability before going public with it.

What does CERT.LV offer?

- We do not offer monetary compensation, but when the issue is solved CERT.LV can help to prepare information for publication and promote the researcher's contribution if that is mutually agreed upon.

If you found a vulnerability in other institutions' services, please contact us at cert@cert.lv (please use CERT.LV public PGP key: https://cert.lv/en/contacts).

2.3.15 Lithuania

IMPLEMENTED

Lithuania has a national CVD policy in place which has been adopted through the Republic of Lithuania Law on Cyber Security and its amendments regarding CVD policy formalisation. The law entered into force on 28 June 2021. All ministries were involved in the approval of the law. For example, the Ministry of Justice, Prosecutor General's Office and Police department provided indications on the conditionalities for the researchers' activities to be established. They asked in particular to set not only the right to search for vulnerabilities but also to set an obligation to notify the relevant organisation about the search being performed. Concerning the implementation of the law, the MoD designated the **National Cybersecurity Centre (NCSC – national CERT)** as coordinator.

It is important to note that the CVD policy in Lithuania does not apply to vendors but only to cybersecurity entities (CSEs) that are the owners of assets that the vulnerabilities are being found on. The NCSC does contact the vendor though, in case a vulnerability is found in a product that might be used by other parties (and the essence of the vulnerability is not a misconfiguration or a vulnerability that is already known). Nevertheless, the NCSC has no right to oblige the vendor to take any action if the vendor is not a CSE.

Voluntary vulnerability disclosure mechanisms were already applied by organisations in Lithuania (e.g. JSC Ignitis group or the Vilnius municipality administration). According to a report facilitated by the Global Cyber Security Capacity Center (GCSCC), a (voluntary) vulnerability disclosure framework was already in place in 2017, based on which 'organisations have established their processes and mechanisms to receive, disseminate and share information on vulnerabilities'[26].

Furthermore, the Order on the approval of the rules on the insurance of security and integrity of public communications networks and public electronic communications services already required that 'providers of public communications networks report certain types of security incidents'. In this context, different CSIRTs in the country, such as CERT-LT, were provided with 'mechanisms in place to share information including specific timeframes'[27].

Nonetheless, there was no vulnerability disclosure practice applied on a national level, which is why ordinary citizens or 'white hackers' had limited opportunities to share or report such vulnerabilities found in other information systems, especially from a legal point of view.

As such, in 2020, the Ministry of National Defence started drafting an amendment to the Republic of Lithuania Law on Cyber Security (hereinafter 'the amendment'). The amendment determines the following restrictions, that apply to a search of vulnerabilities, and that define what makes it legitimate.

1. The operation, functionality, services and data availability or integrity of the communication and information system may not be disrupted or altered.
2. When a vulnerability is identified, the search activity is terminated.
3. Within 24 hours of the start of the search activity, information on search results must be submitted to the NCSC under the Ministry of National Defence or CSE.
4. It is not unnecessarily sought to validate, monitor, record, intercept, acquire, store, disclose, copy, modify, corrupt, delete, destroy data managed by a cybersecurity entity.
5. No attempts are made to guess passwords. Passwords obtained illegally are not used and employees of the CSE or other persons who have the right to use non-public information relevant to the search for loopholes are not exploited or manipulated in order to obtain the information.
6. Information about the detected vulnerability is shared only with the NCSC under the Ministry of National Defence or CSE and made public according to the amendment.

Only if all those requirements are met would the search for vulnerabilities be regarded as lawful. Failure to comply with at least one of those requirements would lead to an application of criminal liability.

2.3.16 Luxembourg

IN PROGRESS

For now, Luxembourg has no formal CVD policy in place. The *National Cybersecurity Strategy IV*, covering 2021 to 2024, states under Strategic Objective I: Building trust in the digital world and protecting human rights online – I.5 Pen-testing, bug bounties and responsible disclosure of vulnerabilities that 'the government will propose the necessary legislative changes and initiatives to make possible or deepen different approaches in order to improve cybersecurity by using the collective intelligence of security researchers, private companies

[26] Global Cyber Security Capacity Center (GCSCC) (2017), *Cybersecurity Capacity Review – Republic of Lithuania*, August. Available at: https://www.nrdcs.lt/file/repository/resources/Lithuania_Report_10_8_2017_FINAL.pdf
[27] Pupillo, L., Ferreira, A., & Varisco, G. (2018). Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges. Report of a CEPS Task Force. CEPS Task Force Reports 28 June 2018

active in the search for vulnerabilities and any users who discover a security breach. The possibility of creating, in the near future, a platform at GOVCERT.LU that encourages researchers to report bugs, especially those associated with vulnerabilities, will be analysed'.

The strategy defines the strategic objectives that should be achieved in the next 4 years and will be complemented by an action plan outlining concrete measures to be implemented following a definite time frame, and the actors called on to contribute to their implementation. The High Commission for National Protection will provide the action plan to interested parties upon request.

Besides, the national CERTs have been charged with the operational objective to monitor threats and vulnerabilities and to make the results available to all Luxembourg actors [28]. The **Computer Incident Response Center Luxembourg (CIRCL)**, in its role as CERT for the Luxembourg economy and municipalities, sets out the procedure for vulnerability disclosure for its constituency [29], receives reports about new vulnerabilities in software and hardware products or discovers them.

In the context of the public sector, i.e. governmental and institutional actors and critical infrastructures, designated according to national legislation, **Luxembourg's governmental CERT (GOVCERT)** launched in 2019 a hall of fame[30] and implemented an informal policy on disclosure[31] in alignment with the *National Cybersecurity Strategy III* [32]. However, in GOVCERT's experience, the hall of fame has not provided sufficient incentives to encourage widespread reporting. Indeed, since the service is online, only a few vulnerability reporters reached out and even fewer vulnerabilities have officially been brought to the attention of GOVCERT.

LUXEMBOURG – CIRCL step for responsible vulnerability disclosure[33]

The Computer Incident Response Center Luxembourg (CIRCL), in its role as CERT for the Luxembourg economy and municipalities, sets out the procedure for vulnerability disclosure for its constituency, receives reports about new vulnerabilities in software and hardware products or discovers them. CIRCL can receive vulnerability notifications from named or anonymous reporters. In some cases, CIRCL discovers the vulnerability within the frame of a specific incident analysis or report. Notifications can only be received by the standard report process of CIRCL. The use of PGP[34] is recommended while exchanging information about the vulnerability. CIRCL expects from a clear statement from the reporters on whether they want to remain anonymous. By default, the reporters will be mentioned to the software or hardware vendor.

CIRCL expects from reporters a reasonable effort to ensure that the report is complete and includes enough information for the vendor to evaluate the vulnerability report.

Notification to the vendor by CIRCL

[28] Government of Luxembourg (2015), National Cybersecurity Strategy II – Approved and made enforceable by the Government Council on 27 March 2015. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf
[29] Pupillo, L., Ferreira, A., & Varisco, G. (2018). Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges. Report of a CEPS Task Force. CEPS Task Force Reports 28 June 2018
[30] GOVCERT.LU, 'Hall of Fame'. Available at: https://www.govcert.lu/en/hall_of_fame/
[31] GOVCERT.LU (2019), Responsible Disclosure Policy (Public) – Version 1.0 – 2019-12-02 (Final), December. Available at: https://www.govcert.lu/docs/POL226_Responsible_Disclosure_Policy_(Public)_1.0.pdf
[32] Government of Luxembourg (2019), National Cybersecurity Strategy III – Approved and made enforceable by the Government Council on 26.01.2018. Available at: https://hcpn.gouvernement.lu/dam-assets/fr/publications/brochure-livre/national-cybersecurity-strategy-3/national-cybersecurity-strategy-iii-en-.pdf
[33] This Section draws form Computer Incident Response Center Luxembourg, Responsible vulnerability disclosure (Version 1.0). Available at: https://www.circl.lu/pub/responsible-vulnerability-disclosure/
[34] PGP is an encryption system used for sending encrypted emails and encrypting sensitive files.

If the vulnerability report is complete, CIRCL (as coordinator or reporter) notifies the vendor via the available security channels. This notification is considered the initial notification. The default delay for the vendor to resolve the vulnerability is 30 days, starting from the initial notification. If the vendor cannot fulfil within 30 days, the vendor must provide to CIRCL an explanation why he cannot correct the vulnerability within that time frame. Under such a condition, an additional grace period can be requested. CIRCL and/or the reporter will review the explanation and CIRCL will find an agreement with the vendor if possible. A request for Common Vulnerabilities and Exposures (CVE) assignment is done at the National Institute of Standards and Technology (NIST) by CIRCL if the vendors are not known to have an existing CVE assignment procedure.

Publication by the vendor

If the grace period is over, the vendor publishes the vulnerability, along with patches or updates to correct the vulnerability. The publication can be done via the official public vendor channels or security channels.

Publication by CIRL or/and the reporter

If the grace period is over and the vendor does not provide an acceptable answer, CIRCL and/or the reporter will publish the information of the vulnerability.

2.3.17 Hungary

IN PROGRESS

Currently, in Hungary there is no CVD policy in place. Last year, the National Cyber Security Centre of Hungary (**NCSC HU)** has suggested initiating a process for establishing a CVD policy, but the proposal faced opposition from the government.

At the moment, there are ongoing negotiations about amending Act L of 2013 on electronic information security of state and local government bodies (Hungarian cybersecurity act) to include vulnerability disclosure requirements for institutions falling within the scope of the act [35]. Currently, system owners are obliged to undertake vulnerability scanning on their systems and to manage the mitigation process, along with maintaining a database about their vulnerabilities. Automatic black-box vulnerability scan systems[36] help these system owners in the process. The system owners are mandated to share the relevant information with the CSIRT only if an incident occurs. The National Cyber Security Center of Hungary is also publishing a recommendation about vulnerability disclosure requirements.

Besides, due to COVID-19, the NCSC HU developed a vulnerability scan process on healthcare applications. The NCSC HU is operating this process by connecting the medical institutions and the application developers and by ensuring cooperation between the parties in the mitigation process. Public disclosure is not part of the NCSC HU coordination process, and it depends on the willingness of the developers.

Notably, together with the Netherlands and Romania, Hungary launched the **Global Forum on Cyber Expertise (GFCE)** initiative for CVD. The objective of the initiative, launched in 2016,

[35] Act on the Electronic Information Security of Central and Local Government Agencies (Act L of 2013/Information Security Act) (2013). Available at: https://nki.gov.hu/wp-content/uploads/2020/11/Cyber-Security-Act_2013_50.pdf
[36] '*Tools that take a black box view of the system under test; they do not rely on the availability of software source code or architecture, and in general try to explore the software's behavior from the outside.' – Cyber Security and Infrastructure Agency (2015), Black Box Security Testing Tools. Available at:* https://us-cert.cisa.gov/bsi/articles/tools/black-box-testing/black-box-security-testing-tools

has been to create a platform 'to share experiences and lessons learned in cybersecurity mechanisms for responsible disclosure or coordinated vulnerability disclosure policies and discussions on the broader topic of ethical hacking'[37].

Participants to the initiative have undersigned the CVD manifesto, committing to implement public reporting mechanisms on vulnerabilities in their ICT systems and calling upon other organisations to do the same. The manifesto aims to make all parties more aware of the importance of cooperation to improve cybersecurity. Furthermore, the program aims at developing a draft memorandum on CVD, at promoting the importance of CVD during conferences and high-level meetings and at strengthening a CVD network[38].

The initiative in the GFCE laid the groundwork for a joint project of four participating States (Czechia, Hungary, the Netherlands and Romania) aiming at operationalising the relevant confidence-building measure of the Organisation for Security Co-operation in Europe (OSCE) at a regional level. The project encourages responsible reporting of vulnerabilities affecting the security of / in the use of ICTs on a voluntary basis.

2.3.18 Malta

NOT IMPLEMENTED

Malta has not yet implemented a CVD policy. The *Malta Cyber Security Strategy 2016* mentions that 'the possibility of a national responsible disclosure policy framework may also be explored. The framework would need to establish the right parameters and conditions to ensure its effectiveness'. According to the report, the framework could be enabled through 'self-regulation, promotion and encouragement by the government, as well as through a proper framework to ensure responsible vulnerability disclosure'.

2.3.19 The Netherlands

IMPLEMENTED

The Netherlands has had a CVD policy in place since 2013. The Netherlands has led the EU's efforts in establishing CVD policies and heavily contributed to supporting other Member States in their efforts to address their own challenges and concerns. It is a formal policy although there is no reference to CVD in Dutch law. The closest to an official policy is the *beleidsbrief OM,* loosely translated, the 'policy letter of the public prosecutor on CVD'. The public prosecutor plays an autonomous role and has the discretion to decide when to prosecute. In this context, historical judicial cases have established the boundaries within which a security researcher can operate.

Since 2013 the **National Cyber Security Centre of the Netherlands (NCSC NL)** has received and processed hundreds of reports[39]. Many organisations in the country have actively adopted CVD and have been satisfied with the results. Even though there are vulnerability reports of minor or theoretical issues, there are some important reports that would not have been found otherwise and could, if abused, have had major adverse effects on the security of the infrastructure or customer data.

[37] Cybil, 'Coordinated Vulnerability Disclosure (GFCE Initiative)'. Available at: https://cybilportal.org/projects/coordinated-vulnerability-disclosure-gfce-initiative/
[38] GFCE (Global Forum on Cyber Expertise) (2017), *GFCE Global Good Practices – Coordinated Vulnerability Disclosure (CVD)*. Available at: https://thegfce.org/wp-content/uploads/2020/06/CoordinatedVulnerabilityDisclosure-1.pdf
[39] For detailed guidelines on CVD in the Netherlands access National Cyber Security Centre (2018), *Coordinated* Vulnerability Disclosure: The guideline, October. Available at: https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline

A detailed analysis of the Netherlands' CVD policy can be found in the Annex.

2.3.20 Austria

IN PROGRESS

Austria does not have a CVD policy in place at this time. CERT.AT provide on their website a section for incident reporting, both in the context of obligatory/voluntary reporting according to NIS law, and in the context of spontaneous reporting, while no section is dedicated to laying down a CVD mechanism.

During the NIS1 transposition process, establishing a CVD policy was regarded as unnecessary given that the national law already allowed for disclosure. Currently, Austria is considering whether to include a CVD policy in the national transposition of the NIS2 directive. According to the national CERT, there is a spectrum of vulnerabilities based on the type of data that are dealt with. For some vulnerabilities (e.g. those including personally identifiable data)[40] there might be the need for a CVD legal baseline, whereas with the majority of discovered vulnerabilities the national law would be sufficient. It also depends on whether the vulnerability is in common off-the-shelf software, bespoke software or reachable services on the Internet.

Some private companies are fostering the sharing of vulnerabilities according to established best practices. For example, A1 Telekom Austria runs a bug bounty program. Everyone is eligible to participate in the program, subject to the conditions and requirements of A1 Telekom Austria[41]. **Borealis**, an Austria-based international provider of advanced and circular polyolefin solutions, published on this website a guide for researchers on how to disclose vulnerabilities. The policy sets out steps and requirements for users, researchers and the company itself.

AUSTRIA – Borealis vulnerability disclosure policy ([42])

Borealis, an Austria-based international provider of advanced and circular polyolefin solutions, published on this website a guide for researchers on how to disclose vulnerabilities. The policy sets out steps and requirements for users, researchers and the company itself. Borealis is requiring that all users:

- make every effort to avoid privacy violations, degradation of user experience, disruption to production systems and destruction of data during security testing;
- perform research only within the scope set out below;
- use the identified communication channels to report vulnerability information to Borealis;
- keep information about any vulnerabilities you've discovered confidential between the user and Borealis for 90 days while it is used by Borealis to resolve the issue.

The steps for a responsible disclosure are:

- send your findings to infosecurity@borealisgroup.com and encrypt them to prevent this critical information from falling into the wrong hands;
- do not take advantage of the vulnerability or problem you have discovered, for example by downloading more data than necessary to demonstrate the vulnerability or deleting or modifying other people's data;

[40] The PI system collects, stores and manages data from your plant or process. You connect your data sources to one or more PI interface nodes. The interface nodes get the data from your data sources and send it to the PI Server.
[41] Open Bug Bounty (2021). Available at: https://www.openbugbounty.org/bugbounty/PaulMar23292621/
[42] Borealis (2021), ‚Responsible disclosure policy'. Available at: https://www.borealisgroup.com/legal/responsible-disclosure

- do not reveal the problem to others until it has been resolved;
- do not use attacks on physical security, social engineering, distributed denial of service (DDoS), spam or applications of third parties; and
- do provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as possible – usually, the IP address or the URL of the affected system and a description of the vulnerability will be sufficient, but complex vulnerabilities may require further explanation.

Borealis says:

- we will respond to your report within three business days with our evaluation of the report and an expected resolution date;
- if you have followed the instructions above, we will not take any legal action against you regarding the report;
- we will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission;
- we will keep you informed of the progress towards resolving the problem;
- in the public information concerning the problem reported, we will give your name as the discoverer of the problem (unless you desire otherwise).

Error! Bookmark not defined.

2.3.21 Poland

NOT IMPLEMENTED

Currently, there is no consistent policy for managing security vulnerabilities such as CVD in Poland. The 2018 cybersecurity strategy refers to the possibility for relevant CSIRTs to publish information on significant incidents, when it is necessary to prevent an incident from occurring, or when, for other reasons, disclosure of the incident is in the public interest[43].

The issue of reporting vulnerabilities has been partially covered by the National Cybersecurity System Act. In addition, in 2017, security breaches were partially decriminalised to improve researchers' protection (Articles 269b and 269c of the penal code)[44].

The **CSIRT NASK** (Research and Academic Computer Network) team receives reports of vulnerabilities regularly and finds them as part of software security research. CSIRT NASK approaches each case individually and does not strictly follow the Coordinated Vulnerability Disclosure process proposed by CERT/CC[45]. Sometimes, the centre cooperates with foreign institutions that can help in contacting software or devices' vendors.

2.3.22 Portugal

ON THE POINT OF IMPLEMENTING

[43] Law of 5 July 2018 on the National Cybersecurity System (2018), *Journal of Laws 2018* item 1560 (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa). Available at: http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/T/D20181560L.pdf

[44] *The Criminal Code of June 6 1997 (Journal of Laws 1997 transl. gb No 88, item 553) (The Criminal Code z dnia 6 czerwca 1997 r. (Dz.U. tłum. gb Nr 88, poz. 553). Available at:* https://supertrans2014.files.wordpress.com/2014/06/the-criminal-code.pdf

[45] Householder, A. (2019), *The CERT Guide to Coordinated Vulnerability Disclosure*, CERT, December. Available at: https://vuls.cert.org/confluence/display/CVD

Portugal does not have a CVD policy in place. However, a **task force** including the **Portuguese National Cybersecurity Centre (CNCS)**, **public authorities** and **stakeholders from the cybersecurity community** was convened to work on a proposal for establishing a policy at the national level which anticiptes the need to amend the criminal law. The task force presented a proposal with a comprehensive CVD policy and legislative amendments. The proposal is now being examined by decisionmakers.

In 2020, the CNCS also developed a National Cybersecurity Framework setting out a relatively long list of security measures and standards that organisations can use to perform a risk-based approach to tackle cyber threats. This framework includes information on setting processes to receive, analyse and respond to vulnerabilities disclosed from internal and external sources[46]. This allows willing organisations to implement their own process to receive, analyse and verify the submission of vulnerabilities. In terms of process implementation, the document states that organisations should do the following.

- 'Make available a process to report vulnerabilities, both internally and externally'.
- 'Provide a process to receive security alerts, recommendations, bulletins from vendors and suppliers, interest groups and others'.
- 'Consistently evaluate, treat and respond to each submission'.

The pieces of evidence that should be provided (by the organisation) are the following.

- 'Support document for vulnerability management process'.
- 'Records from past subscription to technical interest groups'.
- 'Records of receiving and treating reported vulnerabilities'[47].

Notably, it is in the view of the CNCS that each vendor should put in place its CVD policy and establish its own rules. The planned role of the national CERT would be to oversee the communication between the parties and check if the whole process is carried out consistently with the national guidelines. The CERT would, therefore, act as the mediator.

Finally, the National Cybersecurity Centre and the DNS.PT Association (referred to as '.PT') jointly launched Webcheck.pt[48], an initiative to promote the adoption of good practices and standards contributing to the security, integrity, and confidentiality of the internet. As promoters areresponsible for the maintenance of the Webcheck.pt platform, .PT and CNCS allow the interested communities to perform security tests and disclose results under the terms and conditions outlined in the website's policy[49].

2.3.23 Romania

NOT IMPLEMENTED

Romania initiated, together with the Netherlands and Hungary, the GFCE initiative for CVD with the objective to share experiences and lessons learned in CVD. According to ENISA, the National Cyber Security Directorate (NCSD) participates in the initiative on CVD, 'having

[46] Portuguese National Cybersecurity Centre (CNCS) (2020), National Cybersecurity Framework Version 1.0 EN, April. Available at: https://www.cncs.gov.pt/content/files/qnrcs_web_eng.pdf
[47] Access to Webchech.pt available at: https://webcheck.pt/pt/
[48] https://webcheck.pt/pt/
[49] Webcheck.pt, 'Responsible disclosure'. Available at: https://webcheck.pt/en/responsible-disclosure/

implemented a local program enabling security researchers to report vulnerabilities and acting as trusted 3rd party in coordinating the disclosure'[50].

The GFCE website mentions, among the expected outcomes of initiatives, the draft of a CVD policy at the national level in Romania[51]. No advancement in the GFCE initiative seems to be currently on the way.

2.3.24 Slovenia

IN PROGRESS

Slovenia has not yet implemented a CVD policy. The country is planning to include a CVD policy in the next cybersecurity strategy. A CVD policy will likely be included in an amendment to the Information Security Act, which transposed the NIS Directive into national legislation and was adopted in 2018, or even as a new act considering the NIS2 directive transposition into national legislation.

Most likely, the envisaged responsible body will be the national CERT. The Information Security Administration will also conduct awareness-raising campaigns aimed at tackling the entities that have been opposing the establishment of a CVD policy in the past.

Indeed as of 2018 the SI-CERT had proposed to add this topic to the upcoming law on information security, while no consensus for support was reached at that time. The highlighted challenges related in particular to the awareness of decision-makers at the political level on the current best practices in the information security community[52]. The 2018 Information Security Act did not make any reference to CVD, although providing that competent national authority 'may inform the public about individual incidents … when disclosure is in the public interest'[53]. The *2020 Digital Slovenia Strategy for the Information Society*[54] does not make any reference to CVD neither.

2.3.25 Slovakia

IN PROGRESS

Slovakia has not yet implemented a CVD policy. However, a CVD policy mechanism is available in Slovakia at the level of CERT. In 2019, the **SK-CERT** has published its 'Vulnerability Reporting Guideline' [55].

The National Cyber Security Centre SK-CERT published this guideline as a recommended procedure for vulnerability reporting. The guideline is also suitable for vulnerability reporting in products and services of the National Security Authority and SK-CERT.

On a legislative level, while there is no CVD policy in place, there are implicitly established processes regarding CVD. According to the national CSIRT, the current state of legal acts in

[50] ENISA, 'National Cyber Security Strategies' (interactive map). Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Romania
[51] Global Forum on Cyber Expertise (GFCE), 'Coordinated vulnerability disclosure'. Available at: https://thegfce.org/initiatives/coordinated-vulnerability-disclosure/
[52] Pupillo, L., Ferreira, A., & Varisco, G. (2018). Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges. Report of a CEPS Task Force. CEPS Task Force Reports 28 June 2018
[53] National Assembly of the Republic of Slovenia (2018), The Law on Information Security (Z A K O N O INFORMACIJSKI VARNOSTI (ZInfV), April. Available at: https://ccdcoe.org/uploads/2018/10/Slovenia_Information-Security-Act-2018_original.pdf
[54] Republic of Slovenia (2016), *Digital Slovenia* 2020 – Development strategy for the information society until 2020, March. Available at: https://www.gov.si/assets/ministrstva/MJU/DID/Digital-Slovenia-2020-Development-Strategy-for-the-Information-Society-until-2020.pdf
[55] SK-CERT National Cyber Security Centre (2019), Vulnerability Reporting Guideline, September. Available at: https://www.sk-cert.sk/wp-content/uploads/2019/10/Vulnerability_reporting.pdf

policy has two major shortcomings when it comes to CVD, namely that (i) there is no legal definition of 'vulnerability' and (ii) there is no binding CVD policy.

The Cybersecurity Act (CSA)[56] mentions 'vulnerability' only as part of *ex ante* security measures mandatory for essential services providers and the public sector. The delegated Act. no. 362/2018 then elaborates more on the importance of establishing the *ex ante* security measures on the known vulnerabilities and processes of revision. The delegated Act no. 436/2019 Coll. requires to check if the vulnerabilities and the vulnerability revision processes are present in the security measures and documentation. The delegated Act no. 166/2018 Coll. binds the CSIRT teams to safeguarding confidentiality once a vulnerability is discovered during their operations.

Thus, while a CVD policy is not present, it might be subsumed under Art. 8 of the CSA which constitutes the single point of contact regarding the cybersecurity issues for essential services operators and the public sector. The kind of cyber security information that the constituency should be reporting to the established single point of contact is broadly defined. Therefore, even vulnerability reports might be included. Although, they are not explicitly mentioned.

2.3.26 Finland

IN PROGRESS

Finland has no CVD policy in place at this time and there is no mention of vulnerabilities in the law. That said, they do appear to be making efforts in this direction.

In 2010, the **National Cyber Security Center Finland (NCSC FI)** had published a vulnerability coordination policy as an effort to spell out their position and to initiate a discussion on the topic. According to representatives from the Finnish Transport and Communications Agency (Traficom), the policy published in 2010 was not widely implemented across the country. However, the overall good situation with vulnerability management in the country could explain the limited application of this CVD policy.

Nevertheless, the policy has been used as a policy template to help vendors evaluate their own policies. It is envisaged that it will be updated and promoted at the level of decision-makers to form a national CVD policy, especially in the context of the new provisions that will stem from the NIS2 directive.

The role of CERT FI should also be mentioned. According to ENISA, there are three CSIRTs that have 'extensive experience with coordinating vulnerability disclosure. These are CERT FI in Finland, JP-CERT in Japan and CERT-CC in the United States. The work carried out by these coordination centres is widely recognised and it is recommended that since they already have the know-how they should continue to lead these activities'[57].

CERT FI acts as coordinator in the process of vulnerability disclosure. The aim of the centre is that the information about vulnerabilities, related patches and updates, reaches all involved parties, including the end users of products. CERT FI ensures that as many major vulnerabilities as possible are patched and that fixes are applied. As a vulnerability coordinator, it promotes

[56] European Commission (2019), Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) PE/86/2018/REV/1, Brussels, 7.6.2019

[57] ENISA (2015), *Good Practice Guide on Vulnerability Disclosure – From challenges to recommendations*. Available at: https://www.enisa.europa.eu/publications/vulnerability-disclosure

the responsible handling of vulnerability information during all stages of the vulnerability life cycle. CERT FI handles about 50 vulnerabilities every year.

Private organisations operating in Finland, such as the Cisco Product Security Incident Response Team[58], acknowledge the collaboration with third-party coordination centres such as CERT FI to manage a coordinated disclosure for vulnerabilities reported to them and impacting multiple vendors[59].

CERT FI sends information and news about vulnerabilities to customers on an almost daily basis and researches Finland's situation when a newly released vulnerability seems like it might affect Finland. The Microsoft Exchange Server vulnerability is a good example of this type of activity. CERT FI was mapping the situation in Finland when the vulnerability was released. The centre contacted every vulnerable organisation via email or direct phone calls. Over a month, all the vulnerable exchange servers (300) in Finland were patched.

Moreover, the 'white hat hacker'[60] ecosystem in Finland is quite active and CERT FI receives a handful of vulnerability notifications/reports from them every year. The bug bounty programs are also popular in Finland.

2.3.27 Sweden

NOT IMPLEMENTED

Sweden does not have a CVD policy in place at a national level and there is no plan to implement one at this stage. The 2017 national cybersecurity strategy[61] does not provide any indications for developing CVD mechanisms.

The Swedish national CSIRT, CERT-SE, gets involved in 5–10 cases per year, where CERT-SE preferably supports the resolution of vulnerabilities by helping reporters reach the manufacturers, guids reporters and manufacturers to business standard procedures and, if needed, acts as an intermediary between the two.

Sweden-based companies such as Swedbank, Northvolt or Klarna appreciate security researchers and encourage them to report potential vulnerabilities identified in any product, system or asset and offer responsible disclosure program guidelines[62]. Other companies use private initiatives like HackerOne or OpenBugBounty to be notified about vulnerabilities and interact with reporters.

2.4 CVD OUTSIDE THE EUROPEAN UNION

This Section provides an overview of the CVD-related practices outside the European Union, in particular, it explores the latest trends in the People's Republic of China, the United States of America and Japan.

2.4.1 People's Republic Of China[63]

[58] PSIRT – https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-psirt-infographic.pdf
59 *CISCO (2021), 'Security Vulnerability Policy'. Available at:* https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html
[60] *White hat hackers, also known as ethical hackers or reporters, are vulnerability researchers identifying, investigating and reporting vulnerabilities in good faith.*
[61] *Government Offices of Sweden Ministry of Justice (2017), A national cyber security strategy Skr. 2016/17:213.* Available at: https://www.government.se/4ada5d/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213
[62] See for example: Northvolt, Responsible Disclosure Program. Available at: https://static.northvolt.com/Responsible%20Disclosure%20Program.pdf
(63) This section of the report was contributed by Francesco Campoli, CEPS research asisstant intern

Introduction

According to the available literature, in China[64], the software vulnerability evaluation process is led by the intelligence services. China's process is one 'in which high threat vulnerabilities are likely evaluated for their utility in intelligence operations before they're published [on the Chinese National Vulnerability Database], and the publication is made or delayed for these high threat vulnerabilities based on whether they can be operationally useful to the [Ministry of State Security] whether for domestic surveillance or foreign intelligence operations'[65]. It is likely that the Chinese government holds on to high value vulnerabilities to be used for national security goals. One reason to believe that is the delay in publishing these vulnerabilities compared to the lower-threat ones: from 21 to even 156 days longer. For instance, the vulnerability CVE-2017-0199 of Microsoft Office was revealed by Chinese databases with a delay of nearly 2 months – sufficient time to exploit this software vulnerability and launch attacks against other countries or organisations. It is no coincidence that this same vulnerability is at the heart of both WannaCry and NotPetya attacks.

In 2020, the Chinese government was looking at introducing specific rules on how to disclose vulnerabilities, and to require researchers to report them to authorities before making them public. It is a crucial issue because media, in this manner, are limited from publishing any vulnerability details before they have been communicated to the competent authorities. This limitation weighs on companies and individuals who will receive information with a significant delay[66]. In 2019, there were various thefts of high-profile data in Chinal, such as internet café customers' information or sensitive medical data. Therefore, the official reason for the massive government presence was the need to not compromise national security and public interests. At the same time, it was required that Chinese nationals assisted the cyber efforts of the country[67]. Already in Article 7 of the cybersecurity law (2017) citizens are required to support and cooperate with national intelligence services. This assistance to the institutions becomes explicit in the regulations on the management of security vulnerabilities in network products (2021) which will be explained below.

To better understand the new law on vulnerability disclosure, it is helpful to briefly describe the current Chinese cybersecurity legal system. The Chinese cybersecurity legal system is organised in a pyramid with the national security law of 2005 at the top and the cybersecurity law of 2017 one step below it. The cybersecurity law, approved since 2016, aims to safeguard the Chinese 'cyberspace sovereignty' by strengthening existing regulations that concern cyber activities. For instance, companies that did not store their data in China at that time had to purchase cloud sharing services to avoid heavy fines[68]. The network security is the goal set to protect citizens' rights and interests, safeguard national security and promote economic development. To achieve network security, the law requires network owners and network operators to adopt security measures such as security incident recording or the establishment of security management bodies. In addition, companies supplying network products and services in China must comply with the mandatory national security maintenance requirements. Those that do not comply with the cybersecurity law may receive fines up to 1 000 000 RMB (132 719 EUR[69]), face an arrest of operations and even incur the revocation of business

[64] O'Neill, P. H. (2017), 'China hides homegrown hacks from its vulnerability disclosure process', Cyberscoop. Available at: https://www.cyberscoop.com/china-vulnerability-disclosure-mss-recorded-future/
[65] Udemans C. (2019), China working on rules to regulate vulnerability disclosures, TechNode. Available at: https://technode.com/2019/11/22/china-vulnerability-disclosures-risks/
[66] Udemans, C. (2019), 'China working on rules to regulate vulnerability disclosures', TechNode. Available at: https://technode.com/2019/11/22/china-vulnerability-disclosures-risks/
[67] Townsend, K. (2021), 'New law will help Chinese government stockpile zero-days', Security Week. Available at: https://www.securityweek.com/new-law-will-help-chinese-government-stockpile-zero-days
[68] National Law Review (2017), People's Republic of China Cybersecurity Law: A preliminary overview for western companies, Vol. 7, No 199. Available at: https://www.natlawreview.com/article/people-s-republic-china-cybersecurity-law-preliminary-overview-western-companies
[69] Exchange rate (InforEuro) of European Commission, October 2021

licenses. The cybersecurity law confirms and consolidates the passage from elective regimes toward obligatory standards and requirements in the cybersecurity field.

At the bottom of this legislative pyramid, stands the data security law and the abovementioned regulations on the management of security vulnerabilities in network products, both entered into force at the beginning of September 2021. The latter has many implications, which are explored below.

Regulations on the management of security vulnerabilities in network products

On 1 September 2021, new regulations on the management of security vulnerabilities in network products came into effect. They have been drafted and updated for two years, since 2019, before their official release.

In these 2 years there have been six rounds of updates and implementations, which indicates the great interest that the various ministries have in this area. The first three steps were necessary for the Chinese government to incorporate the various opinions of interested stakeholders. The regulations were introduced on 19 June 2019; the opinions of the community have been accepted since 10 August 2019; and in November the Ministry of Industry and Information Technology (MIIT) held a forum for enterprises, seeking advice, and to collect opinions from the industry. The fourth round, from December 2019 to December 2020, was the most important one because it involved a long negotiation between the MIIT, the Ministry of Public Security (MPS), the Cyberspace Administration of China (CAC) and the network operators. Following this negotiation, the articles of the regulations increased from 8 to 16. Finally, from December 2020 to May 2021, the final draft of the legislation has been submitted to the Central Cyberspace Affairs Commission for the final review and the regulation was officially issued simultaneously by the three ministries (MIIT, CAC and MPS) on 13 July 2021.

The regulations on the management of security vulnerabilities in network products is not the only law that came into force on 1 September, as the new regulations to protect the critical information infrastructure, were also released. They underline the importance of network threats and vulnerabilities along withcybersecurity monitoring, handling and emergency response. As already mentioned, the data security law also became effective, giving network operators a few directions on how to perform security protection obligations to protect networks from interference, damage or unauthorised access, and prevent network data from being disclosed, stolen or tampered with. The latest noteworthy act is the personal information protection law, the Chinese version of the general data protection regulation (GDPR), which focuses on the governance of Internet platforms and provides for an emergency plan in the event of personal information security incidents.

The management and security vulnerabilities law

The regulations on the management of security vulnerabilities in network products find their legislative basis in Article 22 of the cybersecurity law: ‘when a provider of network products or services discovers security defects or vulnerabilities in its network product or services, it shall take remedial measures immediately, inform users in time and report to the competent authorities in accordance with relevant regulations’.

The competent authority is subsequently indicated in the Ministry of Industry and Information Technology (MIIT). The law’s legislative intent is managing what they define ‘network products’, i.e. all devices that can be connected to the internet. Product vulnerabilities are key because they constitute one of the greatest threats to digital infrastructure security. In this view, the regulation shifts the emphasis on network product providers who are responsible for ensuring the cybersecurity of their products.

They are required to fix security vulnerabilities of their network products, eliminate security risk from the source of threats, prevent security incidents caused by malicious exploitations and effectively support the high-quality development of the digital economy, consolidating the security foundations of the rapidly developing digital society. More generally, four major objectives can be recognised in this regulation: maintain national cybersecurity; regulate vulnerability-related behaviours (standardise vulnerability discovery, reporting, patching and release); clarify the responsibilities and obligations of the network product providers, network operators and organisations or individuals engaged in vulnerability-related activities; encouraging various entities to make full use of their technical advantages to discover, collect and release vulnerabilities. There is a clear desire to standardise the behaviour of the various actors involved but above all to avoid that information on vulnerabilities is managed independently.

Another important aspect of the regulations is to define the role of the three Chinese ministries that participated in the consultations prior to the publication of the new package of laws. There is a clear division of supervision responsibilities that can be derived from Article 3 of the regulations. The CAC is responsible for overall coordination of network product security vulnerability management. MIIT, a strong ministry which can easily handle the product vendors (included cars and airplanes companies), is responsible both for the comprehensive management of network product security vulnerabilities and for the telecom and internet industry network product security vulnerability supervision. Finally, the MPS is the ministry in charge of combating illegal and criminal activities by exploiting loopholes according to the law. It is responsible for the supervision and management of network product security vulnerabilities. The collaboration between these three ministries is regulated by Articles 3 and 7 of the regulations and can be divided into three areas. The first one provides real-time vulnerabilities information sharing among three departments: the Network Security Threat Information Sharing Platform of the MIIT, the National Cybersecurity Notification Center of the MPS and the Chinese National Vulnerabilities Database (CNVD) of CN-CERT under the China Internet Network Information Center of the CAC. The second one states that the security vulnerabilities of major network products must be jointly evaluated and handled by the three departments. The last area concerns the vulnerability registration platform managed by MIIT, which subsequently informs the MPS and the China Internet Network Information Center.

As previously mentioned, one of the main purposes of the Chinese government is to use this new regulation to standardise the behaviour towards the discovery and disclosure of vulnerabilities. The goal is to ensure clear disclosure rules for the researchers, an almost immediate fix by the product providers and effective verification of the repair by network operators.

The law can be summarised as follows[70].

- Art. 4 lists the red lines that demarcate the boundary of what organisations and individuals shall not do. Three prohibitions should be mentioned. The first one is not to compromise cybersecurity, i.e. no organisation or individual may take advantage of the security vulnerabilities of network products to engage in activities that endanger cybersecurity. The second prohibition is not to illegally collect, sell or publish information about security vulnerabilities of network products. The third one regards more generally hazardous activities and the right behaviour to avoid them. Together

[70] Office of the Central Cyberspace Affairs Commission (2021), 'Notice of the Minitry of Industry and Information Technology and the States Internet Information Office of the Ministry of Public Security on Issuing the regulations on the management of network product security vulnerabilities'. Available at: http://www.cac.gov.cn/2021-07/13/c_1627761607640342.htm

with the red lines and the prohibitions, the punishments for the misconducts can be found in Articles 12, 13, 14 and 15.

- Art. 5 establishes a vulnerability reporting channel, which shall keep reception logs of the network product security vulnerability information for not less than 6 months.
- Art. 6 encourages people to report vulnerabilities to network product providers.
- The Articles 7, 8 and 9 regulate the responsibilities and obligations for three different entities, namely network product providers, network operators and reporters.
- Art. 7 concerns network product providers and the behaviours they must adopt. For instance, they are required to share all vulnerability reports with the MIIT within two days (7.2) and are encouraged to set up a reward mechanism for reported vulnerabilities (7.3) as a sort of bug bounty program.
- Art. 8 is dedicated to network operators and contains only one paragraph regarding the timely verification of communicated vulnerabilities and their repair in a short time. The requirements are higher for the reporters, so as to exercise a strict control over them, and they decrease with the network product providers, only to be minimized for network operators. The reason is that in China the latter are state-owned companies, hence, they are already directly regulated. Therefore, although the Article 8 is very short, the level of control is not lower than the one exercised on reporters and vendors.
- Art 9 is dedicated to organisations and individuals who discover a vulnerability. It prohibits researchers from disclosing vulnerabilities details before a vendor has had a reasonable chance to patch and prevent cybersecurity risks (9.1). It prohibits researchers from exaggerating risks associated with security flaws or using a vulnerability to extort vendors (9.3). It prohibits the publication of programs and tools to exploit vulnerabilities and put networks at risk (9.4). It prohibits disclosing vulnerability details to 'overseas organisations or individuals other than network product providers' (9.7)[71].
- Art. 10 regulates the procedure that network operators and product vendors must follow to report any vulnerability they face. It mandates that any organisation, or individual researcher, register their vulnerability reporting platforms with the MIIT (which has the duty to notify the MPS and the CAC). It is important to distinguish that the report is not anonymous for the companies but can be for the researcher when they inform the company. Furthermore, these actors are encouraged to submit vulnerability information to the relevant platforms of the MIIT and the CAC. Following the red lines set in Article 4, the penalties concern respectively the three main actors of the new regulations (product vendors, network operators and reporters) and the hazardous activities.
- Art. 12 is specific to product vendors. It punishes both failures to take measures to remedy or report network product security vulnerabilities and the circumstances specified in Art. 60 of the cybersecurity law.
- Art. 13 punishes network operators if no measures are taken to repair or prevent network product security vulnerabilities, also applying the situations specified in Art. 59 of the cybersecurity law.

[71] Cinpanu, C. (2021), 'Chinese government lays out new vulnerability disclosure rules', The Record. Available at: https://therecord.media/chinese-government-lays-out-new-vulnerability-disclosure-rules/

- Art. 14 addresses the penalties for reporters based on a misconduct collecting or publishing information about network product security vulnerabilities and in Art. 62 of the cybersecurity law.
- Art. 15 covers hazardous activities. It punishes those who use the security vulnerabilities of network products to engage in activities endangering network security or provide technical support for others to engage in activities endangering network security by taking advantage of the security vulnerabilities of network products (including the circumstances specified in Art. 63 of the cybersecurity law).

The new regulations aim on one hand to improve the working mechanism for vulnerability reporting, evaluation, patching and release. On the other hand, they aim to strengthen technical support with the construction of the Network Security Threat Information Sharing Platform of the MIIT which will collect, evaluate and process vulnerabilities (and share information with the other vulnerability platforms and ministries).

When it comes to data collection, the main one collects information from different platforms, each dedicated to a specific sector: the China Academy of Information and Communications Technology for common network product vulnerability; the China Software Testing Center for mobile internet app vulnerability; or the China Automotive Technology and Research Center for vulnerabilities regarding automobiles.

Implications of the new rules

According to some security analysts, the obligation to report all vulnerability details to the MIIT within 2 days after the discovery is the most troubling part of the law[72]. In particular, they notice that if other countries start imposing the same requirements on security researchers, it adds risk in aggregating unpatched vulnerability data, creating an unprecedented treasure trove of unpatched bugs for our adversaries to attack and steal. Another issue is represented by western bug bounty platforms that have been working with Chinese security researchers for the past years. The fear is that they will provide the Chinese government with a way to be aware of any vulnerability disclosure programme that includes Chinese researchers who report weaknesses (even from non-Chinese companies)[73].

Furthermore, according to other analysts, these new rules will reduce any prior flexibility security researchers had and will oblige them to share security research with the Chinese government. This probably will not imply a rise in the volume of attacks but an increase in sophistication. There will be repercussions on western organisations that are carrying out research and development activities in China, since the Chinese government will identify the vulnerabilities in their products before them[74]. Despite the fact that the provision allows the disclosure of cyber weaknesses to foreign manufacturers, there is no guarantee that this will happen.

2.4.2 Japan[75]

In Japan, the coordinated disclosure of vulnerabilities in products such as software is performed in accordance with the 'Information Security Early Warning Partnership Guideline' (hereafter 'Guideline'). This guideline is based on a 2004 notification from the Ministry of Economy, Trade and Industry (METI) entitled 'Standards for Handling Software Vulnerability Information and Others', which was amended in 2014 and 2017. The notification was renamed 'Standards for

[72] Balaji, N. (2021), 'Zero-day bugs must be reported to government within 2 days of discovery – New Chinese IT law', CyberSecurityNews. Available at: https://cybersecuritynews.com/all-the-zero-day-bugs-must-be-reported-to-government/
[73] Cinpanu C. (2021), Chinese government lays out new vulnerability disclosure rules, The Record. Available at: https://therecord.media/chinese-government-lays-out-new-vulnerability-disclosure-rules/
[74] Townsend K. (2021), New Law Will Help Chinese Government Stockpile Zero-Days, Security Week. Available at: https://www.securityweek.com/new-law-will-help-chinese-government-stockpile-zero-days
[75] This Section of the report was contributed by JPCERT/CC.

Handling Vulnerability-related Information of Software Products and Others' in 2017. The guideline was created and jointly announced in cooperation with several industry organisations, namely the Japan Electronics and Information Technology Industries Association (JEITA), the Japan Information Technology Service Industry Association (JISA), the Computer Software Association of Japan (CSAJ) and the Japan Network Security Association (JNSA). It serves as a recommendation to parties relevant to the coordinated vulnerability disclosure process. The recommended processes in the guideline are in alignment with ISO/IEC 29147:2014 'Vulnerability disclosure'. For the purposes of this document, vulnerabilities in products such as software and firmware will be considered.

In this guideline, vulnerability reports from researchers are sent to the Information-technology Promotion Agency (IPA), a policy implementation agency under the jurisdiction of METI handling initial analysis and triage. After this process, the reports are sent to the JPCERT Coordination Center (JPCERT/CC), an independent, non-profit organisation funded by METI for coordination with the vendor/developer of the product. Once the vulnerability has been addressed by the vendor/developer, an advisory will be published on Japan Vulnerability Notes (JVN), typically in conjunction with an advisory from the vendor/developer. Through this coordinated vulnerability disclosure process, a total of 1 875 advisories have been published on JVN as of March 2021.

While this coordinated vulnerability disclosure process has worked fairly well, the number of reports received has increased significantly over the past few years. Various factors have caused this increase, among them being an increase in the overall awareness of security vulnerabilities, in the number of researchers searching for vulnerabilities, in the number of products available and in the availability of easy-to-use tools for vulnerability discovery. The increase in reports has led to a process overflow where some reports are not being handled in a timely manner. The guideline initially stated that all reported vulnerabilities must be coordinated and subsequently disclosed on JVN after the vulnerability has been addressed. While it is probably best to coordinate and disclose all reported vulnerabilities, regardless of their severity or the number of users that a particular product has, this is not practical in practice. Also, since this guideline has been published, many vendors/developers have become receptive to the coordinated vulnerability disclosure process, but there remain vendors/developers that are not.

As a recommendation for creating a policy on coordinated vulnerability disclosure, the experiences in Japan lead to the following considerations.

- Incentive should be provided to researchers to report vulnerabilities to an organisation that can directly address the vulnerability or at least coordinate with an organisation that can address the vulnerability.
- Monetary incentive should also be provided (bug bounty).
- Recognition should also be provided (credit on an advisory).
- Incentives should be provided to vendors to support the coordinated disclosure of vulnerabilities.
- Vendors should be allowed to promote their own actions to address vulnerabilities as a good practice (market appeal).
- Third-party coordinators can also provide value in this process.
- Advisories should be published so that information can reach a wider audience.
- Support should be provided in the coordination process where multiple organisations need to be contacted with a vulnerability (multi-party coordination).
- The coordination process should be clarified so that researchers know how a reported vulnerability will be coordinated and disclosed.

- Vendors should be taught how to create a coordination process so that researchers know vendors will address reported vulnerabilities.

2.4.3 United States of America[76]

The US technical and security community has been concerned with vulnerability disclosure for decades. In 2002, in what was not the first attempt to standardise CVD behaviour, an IETF draft standard, prepared by research experts from the Internet Engineering Task Force (IEFT), which develops and promotes voluntary internet standards, noted that the issue had been 'a divisive topic for years'[77]. Security experts, industry leaders, and policymakers have sought to balance the need to protect users from those who seek to exploit vulnerabilities, the rights and roles of security researchers and those who make and maintain the systems that everyone uses. What was once a contentious area rife with conflict has seen an emerging consensus in the United States, with government policy and law supporting private-sector leadership. While there are no one-size-fits-all solutions, there can exist best practices and accepted ways of handling vulnerability information.

Early governament response to vulnerabilities: coordination and anti-hacking statutes

The initial approach to protect the public took two forms. First, the software and security communities realised that software vulnerabilities required organised coordination. Following the infamous Morris Worm that brought down much of the Internet in 1988 and demonstrated the risks of vulnerable systems, the Defense Advanced Research Projects Agency (DARPA) established the Computer Emergency Response Team, now known as the CERT Coordination Center or CERT/CC. This organisation plays a number of roles in securing the internet, including acting as a 'trusted third party' that could facilitate communication between the then small but burgeoning security research community, and the relatively small number of software vendors.

Early computer exploits in the 1980s also drove the government to punish bad actors in the new and poorly understood domain, in an attempt to discourage their activities. The legislature targeted malicious behaviour in the US anti-hacking statute, the Computer Fraud and Abuse Act (CFAA). Passed in 1986 and amended in 1994 and 1996, the law can apply to anyone who accesses a computer without authorisation, with criminal and civil penalties. This law is controversial among cyber law scholars, and many early judicial interpretations set a very broad scope that would include much potentially beneficial security research.

Software vendors could also use American copyright law to deter security research. The Digital Millennium Copyright Act (DMCA 1998) was a landmark attempt to balance copyright and the free flow of information in the internet age. Section 1201 of this law criminalises attempts to circumvent access control to a copyrighted work, regardless of the intent, although there are now recent exemptions to DMCA for security research. Since much software is copyrighted under US law, and basic technical protection measures are often included, this law has been used to threaten and prosecute hackers who have identified vulnerabilities in software. Some of these vulnerabilities were used maliciously to the detriment of companies and innocent users, but others may have been used more constructively. Both the Computer Fraud and Abuse Act (CFAA) and DMCA were used to threaten security research, and authorities ultimately had to clarify what they meant.

[76] This Section of the report was a contribution by Allan Friedman, Director of Cybersecurity Initiatives at the National Telecommunications and Information Administration (NTIA), US Department of Commerce, to the 2018 CEPS Task Force on Software Vulnerability Disclosure in Europe – see footnote (7).
[77] Christey, S. (2002), Memo 'Responsible vulnerability disclosure process', Internet Engineering Task Force, February. Available at: https://datatracker.ietf.org/doc/html/draft-christey-wysopal-vuln-disclosure-00

Chaos and contention

As the security community slowly grew in the early 2000s, the relationship between security researchers and vendors grew worse in the US. While some disclosures were successfully coordinated, often with little fanfare, there were enough high profile incidents to make trust a real issue. There was real concern among the security community that vendors simply were not taking software security as seriously as the researchers. For their part, vendors did not understand the motives or actions of the security research community, and often had real difficulty distinguishing between those who were attacking their software for malicious purposes and those who had no ill will. CERT/CC still played an important role in facilitating disclosure, but as an intermediary. They were criticised by both sides for being overly sympathetic and allied with the other side.

Absent clear guidance, some security researchers worked to create their own broad policies. Nomad Mobile Research Centre, a hacker collective, established their own policy in 1999 on disclosure with windows of one week or one month depending on the severity of each case[78]. A more famous one was posted to the BugTraq mailing list by respected hacker Rain Forest Puppy as a response to complaints that researchers never notified vendors or gave them a chance to respond. This policy gave a window of 2 (later 5) days for response from the vendor, demanding regular communication but not setting a specific timeline on fixing the vulnerability.

The underlying debate was between private disclosure and full disclosure. The former was criticised as ineffective, while the latter was condemned as socially irresponsible. This debate was even picked up by the nascent academic research community on the economics of information security, though they also failed to find an optimal response[79]. One low point in this period of distrust can be seen in 2009, with a presentation at the security conference CanSecWest preaching the mantra of 'no more free bugs', arguing that the legal and professional risks of working with vendors outweighed the benefits of selling them to any paying customer or simply disclosing them publicly[80].

Collaboration and CVD

By the early 2010s, it was clear to many in the community that the status quo was not sustainable. Security researchers were growing in number and wanted a safer ecosystem. Vendors were beginning to appreciate the role of external researchers. Cooperation began more explicitly as companies posted disclosure policies, and the idea of bug bounties spread from a revolutionary concept to an emerging business practice.

The American government followed suit to help shore up collaboration, through a variety of means. An early step was taken in 2013, when the Federal Trade Commission, the consumer protection agency, filed a complaint against mobile device manufacturer HTC for failing to employ ''reasonable security'[81]. While numerous lapses were alleged, the fifth of five charges was the failure 'to implement a process for receiving and addressing security vulnerability reports from third-party researchers'.

As the issue became more common, it became clear that the private sector could benefit from clarity. In 2015, the National Telecommunication and Information Administration (NTIA) in the

[78] Nomad Mobile Research Centre (1999), Announcement Simple Nomad, September. Available at: https://www.nmrc.org/pub/advise/policy.txt
[79] For example, five different papers on the economics vulnerability discovery and disclosure were presented at 2004's Workshop on the Economics of Information Security at Harvard University. See Information Security Economics (2005), 'Schedule'. Available at: http://infosecon.net/workshop/schedule.php
[80] Fisher, D. (2009), 'No more free bugs for software vendors', Threat Post, March. Available at: https://threatpost.com/no-more-free-bugs-software-vendors-032309/72484/
[81] United States of America Federal Trade Commission (2013), DOCKET NO. C-4406 In the Matter of HTC AMERICA Inc., a corporation, June. Available at: https://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htccmpt.pdf

US Department of Commerce announced that it would convene a multi-stakeholder process 'to bring together security researchers, software vendors, and those interested in a more secure digital ecosystem to create common principles and best practices'[82]. This process brought together very diverse viewpoints, while emphasising that there was no one-size-fits-all solution. Participants in this process developed a template disclosure policy to make it easier for organisations to begin a CVD process; conducted research to understand researcher and vendor motivations and concerns; and developed a framework for multiparty disclosure involving vulnerabilities that affect multiple vendors.

Other government agencies followed in quick order. In 2015, the FTC included vulnerability disclosure in the cybersecurity guide for businesses[83]. By the end of 2016, regulators like the Food and Drug Administration (FDA) and the National Highway Transportation and Safety Administration highlighted CVD as an important part of cybersecurity guidance and best practices for medical devices and modern vehicles. The FDA's programme is particularly noteworthy, as it establishes incentives for medical device manufacturers to learn about and deal with vulnerabilities quickly, rather than avoid knowing about them.

Even the often-conservative Department of Defence (DoD) joined the CVD throng. In 2016, in addition to their targeted bug bounty programme for the Pentagon's website, the DoD announced a CVD policy for all public-facing systems. Then Secretary of Defence Ash Carter described it in common terms as a 'see something, say something' policy for the digital domain'[84].

As CVD practices spread across the American economy, the law had to catch up as well. In October 2015, the United States Copyright Office recommended exemptions under the DMCA for 'good faith security research' on the computer systems that are built into voting machines, motorised land vehicles and implantable medical devices[85]. Researchers looking for vulnerabilities in these categories of systems could no longer be targeted for criminal or civil penalties under the DMCA – vulnerabilities in voting machines have since attracted strong attention in the United States. The Copyright Office agreed with NTIA that copyright law may be a poor vehicle for cybersecurity policy, and many anticipate that further calls will be made for the Copyright Office to exempt other categories of systems for security research.

The US anti-hacking law (Computer Fraud and Abuse Act (CFAA)) still remains in force to protect American computer systems, but the Department of Justice has acknowledged the importance of securing the role of security research. In 2014, the Department issued guidance for federal prosecutors contemplating charges under the CFAA. While there is no carve-out or even any explicit reference to security research or disclosure, the guidance lists factors to consider to 'ensure that charges are brought only in cases that serve a substantial federal interest'. The Cybersecurity Unit of the DoJ went further in 2017 by offering a Framework for Vulnerability Disclosure Programs. The goal of this guidance was to assist in the development of CVD programs to clarify 'authorised vulnerability disclosure and discovery conduct, thereby substantially reducing the likelihood that such described activities will result in a civil or criminal violation of law.'

One common theme across the different legal and policy approaches to CVD is that they acknowledge the inherent diversity in CVD programs, based on an organisation's systems, capacity and preferences. The DoJ guidance makes it clear that 'different organisations may

[82] Simpson, A. (2015), 'Enhancing the digital economy through collaboration on vulnerability research disclosure', National Telecommunications and Information Administration (NTIA), July. Available at: https://www.ntia.doc.gov/blog/2015/enhancing-digital-economy-through-collaboration-vulnerability-research-disclosure
[83] Federal Trade Commission (2015), 'Start With Security – A guide for business', June. Available at: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf
[84] United States Department of Defence (2016), 'DOD announces digital vulnerability disclosure policy and "Hack the Army" kick-off', November. Available at: https://www.defense.gov/Newsroom/Releases/Release/Article/1009956/
[85] United States Copyright Office (2015), Section 1201 Rulemaking: Sixth triennial proceeding to determine exemptions to the prohibition on circumvention, October. Available at: https://www.copyright.gov/1201/2015/introduction-analysis.pdf

have differing goals and priorities'. CERT/CC still plays a role as a coordinator, but acting as a single neutral party has not scaled as the digital world has grown and they now offer expertise while supporting others in their efforts. CERT/CC joined a group of security experts to advocate CVD's inclusion in the NIST Cybersecurity Framework, a key security strategy and standards document for the US economy. It is acknowledged in the 2017 2nd draft of the Cybersecurity Framework Version 1.1, which notes the importance of 'processes … established to receive, analyse and respond to vulnerabilities disclosed to the organisation from internal and external sources (e.g., internal testing, security bulletins or security researchers)'[86].

Vulnerability disclosure policy (VDP) platform[87]

In autumn 2020, the Cybersecurity and Infrastructure Security Agency (CISA) released the binding operational directive (BOD 20-01) in support of better management and resolution of software vulnerabilities. The purpose was to strengthen the cybersecurity of federal civilian agencies by requiring them to establish policies that would allow external researchers to report vulnerabilities. On July 30 2021, to consolidate this goal, CISA released a new service for the disclosure of vulnerabilities: the vulnerability disclosure policy (VDP) platform. This service provides a website suitable for receiving vulnerability reports from both security researchers and private citizens. The Platform is offered by CISA's Cyber Quality Services Management Office (QSMO) and provided by BugCrowd and EnDyna.

Along these lines, federal civilian agencies can benefit from QSMO shared services with consequent savings on a development of independent systems. CISA has calculated savings on government-wide costs of more than 10 million USD. Furthermore, thanks to the platform, agencies can receive more information on their possible vulnerabilities that will help in maintaining cybersecurity.

The service providers, BugCrowd and EnDyna, will be responsible for an initial estimate of the reports received. Agencies can then devote their time to vulnerabilities that could have a real impact. With this project, CISA wants to help the Federal Civilian Executive Branch (FCEB) agencies manage vulnerabilities in their informatic systems. The VDP platform makes it easier for the FCEB to coordinate with reporters, helping secure information exchange and increasing collaboration between the public and private sectors.

The process that led to the VDP included a comment period on the draft. Given the relevance of the topic, for the first time CISA allowed a binding operational directive to be subject to public comments before it was issued. Consequently, since November 2019, CISA has received many suggestions for improvements, such as introducing legal parameters for the protection of researchers or defining a mandatory timeline for vulnerabilities' remediation. Jeannette Manfra, assistant director of cybersecurity at CISA at the time, was clearly on the side of the research community: 'A VDP allows people who have "seen something" to "say something" to those who can fix it. It makes it clear that an agency welcomes and authorizes good faith security research on specific, internet-accessible systems'[88]. Finding and reporting a vulnerability for the common good shouldn't involve the risk of a legal action.

Currently, CISA coordinated vulnerability disclosure process consists of five steps[89].

[86] NIST (2017), Framework for Improving Critical Infrastructure Cybersecurity – Version 1.1 (Draft 2), December. Available at: https://csrc.nist.gov/publications/detail/white-paper/2017/12/05/cybersecurity-framework-v11/draft
[87] This final section of the overview of the CVD policies in the USA was contributed by Francesco Campoli, CEPS research assistant intern.
[88] Manfra, J. (2019), 'Improving vulnerability disclosure together', CISA. Available at: https://www.cisa.gov/blog/2019/11/27/improving-vulnerability-disclosure-together
[89] This final section of the overview of the CVD policies in the USA was contributed by Francesco Campoli, CEPS research assistant intern

- Collection. When receiving a report, CISA has the task of carrying out an initial screening to ensure the presence of the vulnerability and that it has not already been reported. After the first check, CISA can collect the report with all the relevant information. A vulnerability report can be collected through CISA vulnerability analysis; checking public information on software vulnerabilities; or through a researcher who submits it.
- Analysis. In this part, CISA works together with the vendor(s) to study the vulnerability by examining both the technical problems and the risks it could pose.
- Mitigation coordination. Continuing closely with the vendor(s), CISA will work to find a way to fix the issue by developing a mitigation (for instance a patch or an update).
- Application of mitigation. Affected end users must test and apply the mitigation prior to public disclosure. This happens at this stage.
- Disclosure. As a last step, CISA will notify affected users about the vulnerability through its channels. It is important to underline that this phase is characterized by the coordination between CISA, the affected vendor(s) and the source of the vulnerability report.

After examining the behaviour that CISA intends to implement, it is necessary to assume the case that a vendor is not responsive or does not establish a reasonable timeline for the mitigation. In this scenario, CISA can disclose a vulnerability 45 days after the first attempt to contact the vendor, regardless of the availability of a mitigation.

With the continuous increase and evolution of cyber threats, it is necessary for vendors to become aware of their role and the support that security researchers can offer them. CISA is at the forefront to help identify and implement the best practices in this process[90].

[90] Goldstein, E. (2021), 'CISA announces new vulnerability disclosure policy (VDP) platform'. Available at: https://www.cisa.gov/blog/2021/07/29/cisa-announces-new-vulnerability-disclosure-policy-vdp-platform; this final section of the overview of the CVD policies in the USA was contributed by Francesco Campoli, CEPS research assistant intern.

3. CVD POLICY PRACTICES

3.1 DESIRED ELEMENTS OF CVD PROCESSES

The next Section provides more detailed information, gathered through the consultation with Member States, on the different elements of the CVD processes and procedures established, or soon to be established, in the different EU countries.

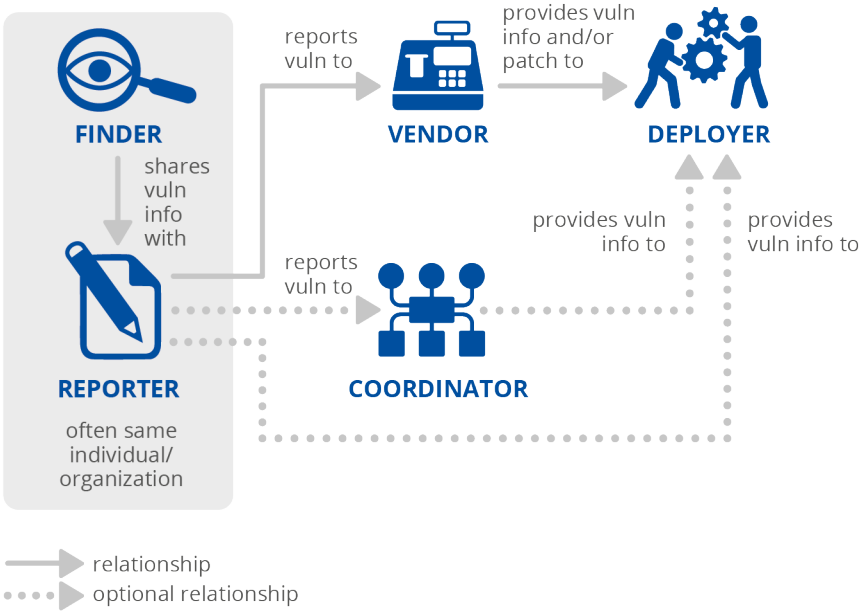
3.1.1 Entities Involved

As mentioned in the Carnegie-Mellon's 'CERT Guide to Coordinated Vulnerability Disclosure', certain roles are critical to the CVD process[91].

- Finder – the individual or organisation that identifies the vulnerability.
- Reporter – the individual or organisation that notifies the vendor of the vulnerability.
- Vendor – the individual or organisation that created or maintains the product that is vulnerable.
- Deployer – the individual or organisation that must deploy a patch or take other remediation action.
- Coordinator – an individual or organisation that facilitates the coordinated response process.

Interactions among these actors are illustrated in Figure 3.

Figure 1 – Visualisation of the Entities Involved in the CVD process



Source: Householder, Allen D., et al. The CERT guide to coordinated vulnerability disclosure. Carnegie-Mellon University Pittsburgh, Pittsburgh, United States, 2017, p. 15

[91] Householder, A. D., et al. (2017), The CERT Guide to Coordinated Vulnerability Disclosure, Carnegie-Mellon University, Pittsburgh PA, United States, p. 15

Most of the Member States anticipate the involvement of the national CERT and/or the national cybersecurity authority in the CVD process with a coordination role. As already mentioned in the previous Section, the mediation role is important for managing parties' expectations in terms of disclosure. The CERT can mediate the conversation between the parties to meet the needs of the vendors and help to decide the appropriate time to disclose the vulnerability. Besides, the involvement of the national CERT is considered central in all the cases in which the researcher wishes to keep its anonymity, and in the cases in which the vulnerability is found in the CERT's constituency.

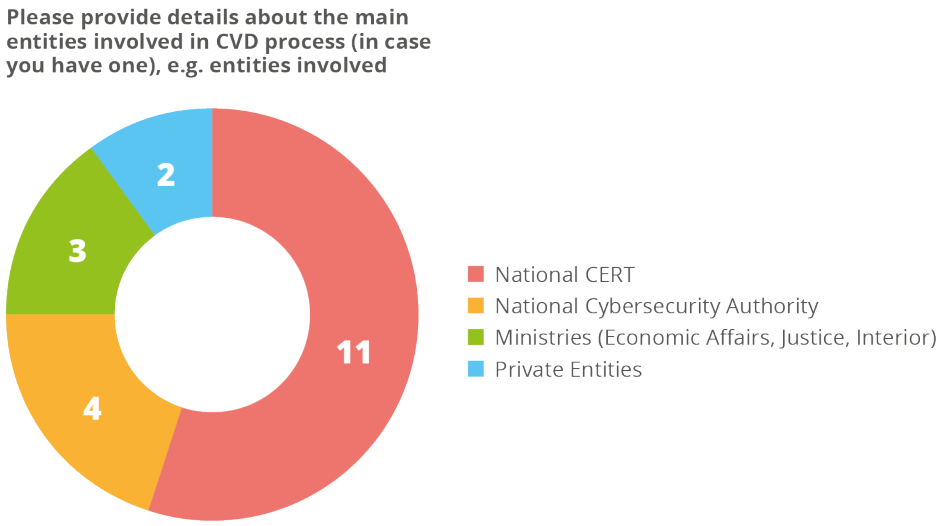
Among the tasks of the coordinator according to stakeholders consulted are: the identification of stakeholders to involve in the process (e.g. when a researcher does not know whom to report the vulnerability to); the management of information flows from reporting to the full disclosure (e.g. when the vulnerability owner might hold a threatening or untrustworthy attitude towards the researcher or when they decides not to address the matter and thus reject the treatment of a vulnerability); providing security researchers with a protection and/or legal shield; setting up cooperation rules in vulnerability management processes; ensuring an objective risk assessment (e.g. by filtering low-quality reports from researchers not meeting expectations set out in the CVD policy).

In some cases, the national CERT together with the community of security researchers will be / is also responsible for the discovery process. For example, the Tallinn University of Technology and the University of Tartu are very renowned in terms of cryptographic skills and have been responsible, together with the national CERT, for the discovery of the abovementioned ROCA vulnerability in the Estonian eID system.

In terms of communication and coordination, the parties involved can vary according to the vulnerability discovered. In case a vulnerability is found in a specific database, the relevant sectoral authorities usually participate in the CVD process. For public disclosure, private companies can also be integrated into the process.

Finally, as shown in Figure 4, the entities involved vary among the Member States according to whether the focus of the CVD policy is / will be on the public sector only. In this case, the implementation of the policy is usually handled by the national CERT and the public sector institutions that are willing to participate. For example, it could be up to the public institutions to identify which resources can/should be tested (e.g. their website or their portal). However, it should be noted that, even in the cases in which a national CVD policy does not focus on private entities as such, private companies are usually allowed and encouraged to publish their own CVD policy.

Figure 2 – Entities Involved in the CVD process



Source: Interviews with EU Member States

Role of CERTs

Stemming from the consultations, two approaches can be identified concerning what role the Member States envisage for the national CERT:

In some cases, the **national CERT only acts as an observer.** The entities involved in these cases are simply the researcher and vulnerability owner. Only in cases where the vulnerability owner does not respond to the researcher requests for contact will the CERTs come into play. If needed, the national CERT can be present in the different steps of the process but, ideally, just as an observer. In the case of multiparty CVD, the role of the CERT as a coordinator is more relevant.

In other cases, **the CERT rather plays a central role**. The CERT is indeed in charge of the implementation of the law and provides guidance and procedures allowing researchers to benefit from the safe harbour.

3.1.2 Tools

The tool that most countries are planning to adopt or have already adopted is **a dedicated website** for receiving requests for coordination/intervention, and to provide a template for notification reports.

The implementation of a **ticketing system** has also been mentioned by several countries as an established good practice. Every mail is sent to the ticketing system, as such, in case the personnel is unavailable, all information will be logged. This pipeline should have permanent support.

Custom tools with enhanced security have also been mentioned by several countries as useful systems to be adopted in the context of a CVD process. The Estonian national CERT for example uses and publicly provides on its website the Cuckoo Sandbox for automated malware analysis, which has proved to be a useful tool in finding vulnerabilities.

On the assessment side, **validation tools** can be used (e.g. Burp suite) to verify the material that is sent out. Burp is generally used for the reproduction and assessment of the severity of the vulnerability.

Besides, in a CVD process **communication tools** are needed, especially in multiparty processes where there are requirements for ensuring the confidentiality of communications. In this respect, communication systems that are pluggable, decentralised and exchangeable are needed.

Mechanisms can also be established to find vulnerabilities through **open-source intelligence software**. ShadowServer or Abuse scan the IP address and disseminate to the national CSIRT the vulnerabilities found on the public IPs – those of Critical Operators for example – that are shared with the national CERT.

In more general terms, the tools that are needed depend on the tasks to be performed. For example, to analyse and exploit vulnerabilities, there is a need for a lab network where vulnerable systems can be tested (e.g. testing whether the received report is trustworthy before addressing the vendor).

3.1.2.1 Common Security Advisory Framework

In Germany, the BSI has in place a warning and information service system. This is a decade-old website where advisories are published daily. It can be regarded as an advisory database accessible to the BSI constituency. More detailed information is instead sent to government entities and critical infrastructures operators. This is one of the most important services that the BSI provides to help its constituency with patch management. In this context, the drafting of the advisories is crucial. The BSI has been very keen on fostering automation in vulnerability management. Each advisory information should hence be machine-readable. Together with national and international partners, the BSI is therefore working on a solution to make it easier for users to find, evaluate and implement security advisories. The machine-processable format for security advisories, the **Common Security Advisory Framework** (CSAF) 2.0, will make a decisive contribution to ensuring that companies can supervise and secure their systems. Two tools, in particular, have been introduced in the context of the CSAF.

- CSAF Aggregator. It allows interested parties to get the relevant information in one single repository, identify the advisory that should be prioritised in their specific case, etc.
- CSAF Advisory Editing System. The tool has been developed by the BSI and is made available to vendors to ensure that they can create and upload advisories on CSAF in the future.

The BSI also strongly advocates for the establishment of a software bill of materials, at least for the most critical vendors.

GERMANY – Advisories and bulletins[92]

According to the German Federal Office for Information Security, an advisory (short bulk of information concerning the vulnerability) shall contain the following information.

- Title or identifier of the advisory (e.g. systematically and consecutively numbered).
- Date of publication.
- Affected products, versions and configurations.

[92] Federal Office for Information Security (2012), Recommendation: IT-producers – Vulnerability Handling – Recommendations for software vendors, October. Available at: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_019E.pdf?__blob=publicationFile&v=1

- Affected platforms and operating systems (and where appropriate their configuration).
- Criticality (categorisation low/medium/high) and estimation according to the Common Vulnerability Scoring System.
- Implications (denial of service, remote code execution, local privilege escalation, etc.).
- Short description of the vulnerability (management summary).
- Detailed description (for technical staff).
- Estimated availability of patch/update.
- History/timeline regarding events relevant to this vulnerability.
- Workarounds.
- Appreciation of the discoverers.
- Information on the way the vulnerability was reported/published (e.g. coordinated disclosure).
- Information on whether exploit or proof-of-concept code is publicly available.
- Authors of the advisory.
- CVE number or CVE candidate reference number.
- Supplemental information.
- URL to the up-to-date version of the advisory.

If an advisory is updated, the additional or modified sections should be clearly marked as an update. An advisory should not include any information that allows technically skilled experts to exploit the vulnerability.

3.1.3 Awareness-Raising Campaigns

All consulted Member States expressed the intention of carrying out awareness-raising campaigns on CVD, especially if the implementation of a national CVD policy will be mandated. In terms of specific activities, the Member States mostly mentioned the following.

Publish guidelines to assist the involved entities on their respective roles, and guide the code owners and researchers on how to handle the CVD process (e.g. guide companies that are reluctant in accepting vulnerability reports or guide researchers on how to act if the vendors do not replay);

Organise discussion fora to involve representatives of the cybersecurity community, relevant state institutions, or Critical Entities Operators. In these communities, experts (programmers, researchers, etc.) can gather and exchange relevant information or good practices. This helps foster a favourable ecosystem for CVD. These communities are also used to train and manage the expectations of partners during the CVD process;

Participate in international communities (e.g. the CERT network or the NIS Cooperation Group), considered particularly valuable to discuss, among others, good practices, present draft policies or analyse the criticality of specific vulnerabilities with a cross-border impact.

Acquire broad media coverage to raise awareness on particularly disruptive vulnerability cases.

Examples of awareness-raising campaigns

In **Hungary**, cybersecurity awareness campaigns are carried out mainly using social media and participation in awareness-raising campaigns at university educational fairs, and through e-learning courses for the NCSC HU sectoral constituency.

The National Cybersecurity Centre of **Lithuania** holds quarterly events – the Cybersec Breakfast – where presentations and discussions on different matters are carried out for about 200 representatives of public sector institutions. Some presentations on the CVD process have been organised in this context. Similar presentations have been held in the context of the 'Safer Internet' event.

In the **Netherlands**, there are several good practices in place in terms of awareness-raising campaigns. **Hack right** is an awareness programme that addresses specifically young first offenders (below 23 years old) and helps them understand their rights and duties. The programme was established in 2019 after it was noticed that most cases arriving in court involved young researchers. NCSC NL published a guideline on CVD policies, which has been helpful for organisations implementing CVD. Besides, researchers in the Netherlands have created the DIVD.NL a platform to report vulnerabilities, supported by volunteers, where they established their code of conduct. DIVD.NL had, for example, an active role in the Kaseya case: DIVD has been in a CVD process with Kaseya, who was working on a patch. Some of these vulnerabilities were used during an attack performed by REvil. Kaseya and DIVD collaborated to limit the damage wherever possible.

3.1.4 Operational and Crisis Management Activities

For most countries, there are no dedicated practices for dealing with CVD, and the same procedures that the CERT adopts in the event of crisis management are applied.

In terms of operational or crisis management activities practices, most Member States referred to the establishment of channels to share information about cybersecurity (incidents, vulnerabilities, etc.). These channels usually include **early warning systems** where the contact details of people operating in critical infrastructures are collected so that they can be contacted in case of an emergency. For reporting from third parties that are not critical operators, the Member States argued that due diligence should be guaranteed in contacting the relevant person in the organisation (security officers, technical team, etc.). In any case, technical details should never be sent to a generic email address. In some cases, specific sectoral information groups are established.

For a limited number of countries (2), **voluntary information sharing** is also promoted at the level of CERTs. According to some Member States, limited voluntary information sharing is due, among others, to the sensitivity of vulnerability information. To foster voluntary information sharing, the level of trust of critical operators should be enhanced (e.g. by ensuring anonymisation of the information).

Some **challenges** have also been underlined by the Member States in terms of operational and crisis management activities. According to consulted countries, from a crisis management point of view, it is unlikely that the national CERT will receive a long-term heads-up about these vulnerabilities, nor will it receive all the relevant information ahead of time. In this respect, the problem with information sharing is that, on a global scale, it is very challenging to ensure that every critical operator using a certain software gets the patch without any information being leaked. In this context, what can be done is to inform the whole supply chain through a heads-up notice stating that something will be happening soon, so that all relevant parties are aware that a process has started, without sharing all the details of the process.

Additionally, small countries have highlighted that the process of building capabilities in the field of information security, incident handling and crisis management is still ongoing. As such, the CERT's capacities are in some cases still limited.

Examples of operational and crisis management activities

The **Estonian** national CERT is in contact with the service providers who are alerted each time a vulnerability is found. The information on the vulnerability is also shared by the CERT with the

Analysis and Prevention Department which is responsible for establishing the connection between the technical and the strategic levels. The Analysis and Prevention Department is in charge of drafting a memo on the discovered vulnerabilities and circulating it within the Ministry. Based on the level of criticality of the vulnerability, the Ministry decides whether to inform the Cabinet. The Analysis and Prevention Department, hence, helps in the interpretation of the technical details to make them understandable at the policy level. This mechanism is regarded as an established best practice.

3.2 CVD POLICY – GOOD PRACTICES

After having assessed the status of implementation of CVD policies across the Member States, good practices were collected in terms of national policies related to the processes they have employed.

Firstly, internationally there are two ISO/IEC standards on CVDP: ISO/IEC 2914741 and ISO/IEC 3011142. The first describes the procedure for disclosing a vulnerability, while the second deals with the processing procedures for the reported vulnerability. The ISO/IEC 3011142 also distinguishes between the different stages of the CVD process (discovery, reporting, validation and triage, remediation, public awareness, deployment). These two standards describe a complete model with the different aspects of a CVDP[93]. Besides, the standard ISO/IEC 27005 on security risk management is also linked with the CVD process insofar as, according to Clause 11 on 'Information security risk communication and consultation', information security risks need to be communicated between responsible individuals and stakeholders. A risk communication plan should be developed by the organisation for both normal operations and emergency situations. The outcome of all this should be a continual understanding of the organisation's information security risk management process and results.

3.2.1 Content of a CVD Policy

A series of good practices can be implemented when drafting a CVD policy. This Section reports the most relevant.

Firstly, the policy must be implemented by individuals or bodies that can validly represent the responsible organisation and should be adequately advertised. Its content should be easily accessible to potential participants, preferably from the website of the responsible organisation.

A disclosure policy helps to define how the vendor will deal with the reported vulnerabilities. As such, the scope of the policy – which sites, products, devices, services, systems or networks are concerned – should be clearly defined. The CVD policy should be applicable to the vendors' various IT systems and to their contractual commitments (suppliers, clients, subcontractors, staff, etc.). If this is not the case, the policy must explicitly list third parties' systems that are excluded from the scope.

The policy should also contain a description of the mutual obligations of the involved parties.

Authorisation to access the computer system

The very existence of a CVD policy or a bug bounty program should imply that authorisation to access the computer system has been granted to the participant. The coordinated vulnerability disclosure policy will include provisions which, depending on their exact wording, may be considered as explicit or tacit authorisations. As such, the vendor should point out that researchers will not be sued if they stick to the ground rules laid out by the vendor.

[93] Centre for Cyber Security Belgium (2020), Guide to Coordinated Vulnerability Disclosure Policies Part I – Good practices. Available at: https://ccb.belgium.be/sites/default/files/Guide20CVDP20part20I20Good20practices.pdf

According to the German Federal Office for Information Security, in order not to scare researchers, the vendor should not demand formal or legal agreements such as contracts, a formal memorandum of understanding or a non-disclosure agreement. Vendors must, however, state in the policy the **conditions** under which participants may or may not access the computer system. The authorisation to modify or delete IT data depends on the way in which the coordinated vulnerability disclosure policy has been drawn up.

According to the CCB, it is good practice to prohibit participants from using DDoS attacks or social engineering attacks, compromising the system, and persistently maintaining access to it, installing malware or viruses, stealing passwords, using brute force to gain access to systems, sharing the vulnerability with third parties, etc. The policy should also explicitly exclude any deliberate attempt to intercept, record or become aware of communications that are not accessible to the public.

More generally, participants must commit to complying with the principle of **proportionality**, i.e. not to exploit vulnerabilities beyond what is strictly necessary to demonstrate the security problem. Participants should also commit not to keep the collected data of the responsible organisation, including any personal data, longer than necessary.

Whenever these conditions are met and participants are complying with the terms of the policy, the vendor should pledge to carry out its coordinated disclosure policy in **good faith** and not pursue civil or criminal action against them.

Information required to report a vulnerability

A CVD policy must clearly state what information the participant must provide when reporting a vulnerability. A clear and detailed description of the vulnerability shall be provided by the security researcher together with clear and detailed information of how the vulnerability has been discovered (actions taken, tools used). The objective is to be able to reproduce it. If applicable, the participant should also report any relevant information such as proof of the existence of the vulnerability (screenshot, link, etc.) and information about the moment the vulnerability was discovered.

Confidentiality

'Coordinated' means that a vulnerability is reported confidentially. As such, one of the essential elements of a coordinated disclosure policy is respect for **confidentiality**: participants should not share the information collected with third parties or disseminate it without the express consent of the responsible organisation.

Procedural deadlines

Clear deadlines shall be set in the policy for each stage of the procedure. As soon as the report has been received, vendors should send acknowledgements of receipt. During the process, the participant should be kept informed with follow-up on the stage of the handling and management processes.

To the extent possible, a deadline for fixing the vulnerability should be established. Ideally, the solution should be developed within **90 days** at the latest. However, such deadlines should remain relatively flexible, depending on the complexity of the vulnerability, the number of systems affected, the urgency or the seriousness of the situation.

Communication channels

Another pivotal aspect of a CVD policy relates to the **point of contact** to which the information should be sent. A specific email address – such as vulnerabilitypolicy@organisation.com – can be used for this purpose. Notably, common addresses such as info@company.com should not be used for security-related issues.

According to the CCB, the use of an online form is a practical way to receive information about discovered vulnerabilities. This method has the advantage that the input and processing of data and the sending of an acknowledgement of receipt can be done automatically.

According to the German Federal Office for Information Security, the **vendor's website** shall offer security-related information at a central position. Such security-related information should contain the following.

- Vulnerability information (advisories on vulnerabilities not fixed yet, information regarding possible workarounds and bulletins on vulnerabilities for which security updates are available).
- Contact information specific for the security of products (email, phone including services hours, public PGP keys and 'IdenTrust Secure Email' certificates of the company to enable confidential communication on security issues).
- The company's disclosure policy.
- Patches and updates.
- Supplemental documents (white papers, FAQ, etc.) regarding the secure usage of products.
- A contact form allows the vendor to structure the information flow and to make certain information mandatory. In addition, such a form supports the alternative to report vulnerabilities anonymously. The company should decide if such a form is relatively simple or more complex.

These webpages shall be protected using valid and verifiable Secure Sockets Layer (SSL) certificates to guarantee the authenticity and confidentiality of the information provided.

Reward to the security researchers

Offering a reward or public recognition could make the CVD policy more attractive for the participants. Rewards could account for monetary compensation in case a bug bounty program is in place. Bug bounty platforms operate as a marketplace intermediary. Vulnerability owners can use a web interface to rapidly design a public or private bug bounty policy and publish it on the platform. The rewards may even be purely symbolic.

Non-monetary rewards, credits and acknowledgements can be particularly appreciated and act as an incentive for the security researchers. For example, the Netherlands rewards researchers with a humorous T-shirt marked 'I hacked the Dutch government and all I got was this lousy T-shirt'. Similarly, many organisations include researchers in a 'hall of fame' published on the organisation website.

Possible public disclosure

Any disclosure of a vulnerability should be coordinated and synchronised between the parties to allow the responsible organisation to resolve the vulnerability and to inform affected parties in advance. Indeed, when a vulnerability is identified in a program, component, protocol, etc. provided by a third-party, the responsible organisation shall notify them directly before any public disclosure.

The same applies when the vulnerability threatens to affect other organisations using similar technology, or in the cases in which the responsible organisation has provided other organisations with the vulnerable component/components. In these cases, it is essential that a report on the vulnerability and its resolution is provided to the parties concerned. In the case of

public disclosure, **the vulnerability report and the solution should be published at the same time**.

The responsible organisation must envisage various means to inform its users, for example, automatic system updates, the publication of security notices on its website or mailings with a link to a specific internet page.

3.2.2 Established Good Practices in Member States CVD Procedures

Besides the content of a CVD policy, the disclosure of vulnerabilities entails a series of procedures that should be implemented for the policy to be effective. This Section provides a brief overview of the procedures that should be envisaged in a CVD policy. Besides, it provides an outline of the procedures in place in three Member States – Belgium, Lithuania, and the Netherlands – considered among the most virtuous examples across the EU.

Overall, the objective of the disclosure policy is to enable the development and deployment of a solution to remove the vulnerability from the IT system. After the researcher finds and reports the vulnerability, unless legally or contractually obliged to do so, the responsible organisation remains free to choose to develop and implement a solution. As mentioned, ideally, the solution should be developed within 90 calendar days. While such deadlines should remain relatively flexible, it is important to keep them to the strict minimum, especially if users of the affected systems are at risk or if there are risks to the protection of personal data. If the organisation is unable to solve the problem immediately, the IT system concerned should be taken completely out of service temporarily. The supply chain and the multiple interdependencies between information systems can complicate the time needed to develop a solution and deploy it.

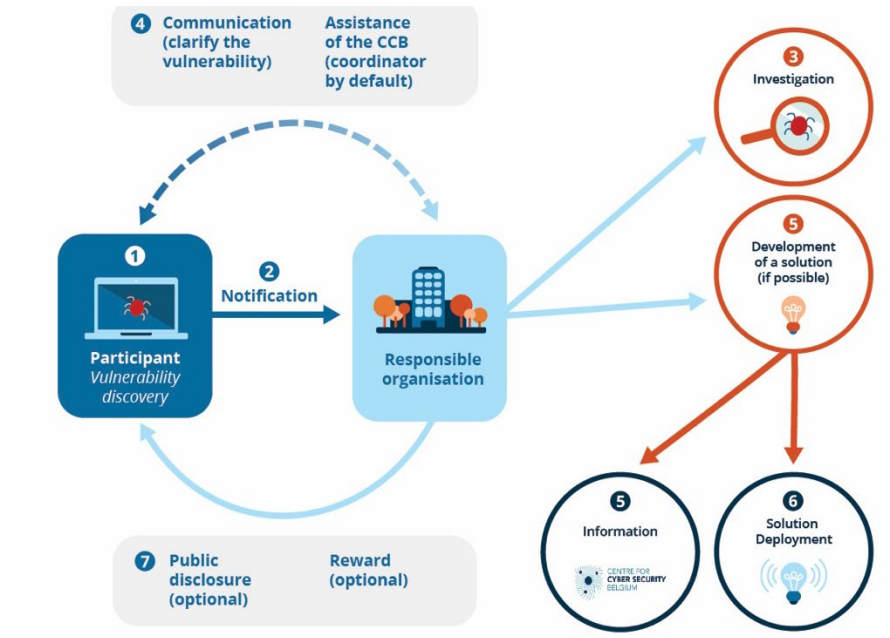
During this phase, the responsible organisation must, on one hand, perform positive tests to verify that the solution is working properly and, on the other hand, negative tests to ensure that the solution does not disrupt the proper functioning of other existing functionalities ([94]). If the solution is ready and the vulnerability would affect other organisations, it should be communicated to the CVD coordinator as a matter of priority and before any public disclosure. The responsible organisation should respect a reasonable period from this transmission before a possible general disclosure to users, to allow operators of vital interest to implement the solution as a priority. If one of the parties does not respond, the parties can always call upon the designated coordinator, in general, the national CERT or the National Cybersecurity Centre.

Belgium

The procedures established by the **CCB** can be regarded as a good practice in the EU. Figure 5 and Figure 6 provide a detailed description of the different phases of the CVD process under the CCB.

[94] Centre for Cybersecurity Belgium (2020), Guide to Coordinated Vulnerability Disclosure Policies Part I: Good Practices. Available at: https://ccb.belgium.be/sites/default/files/Guide%20CVDP%20part%20I%20Good%20pratices.pdf

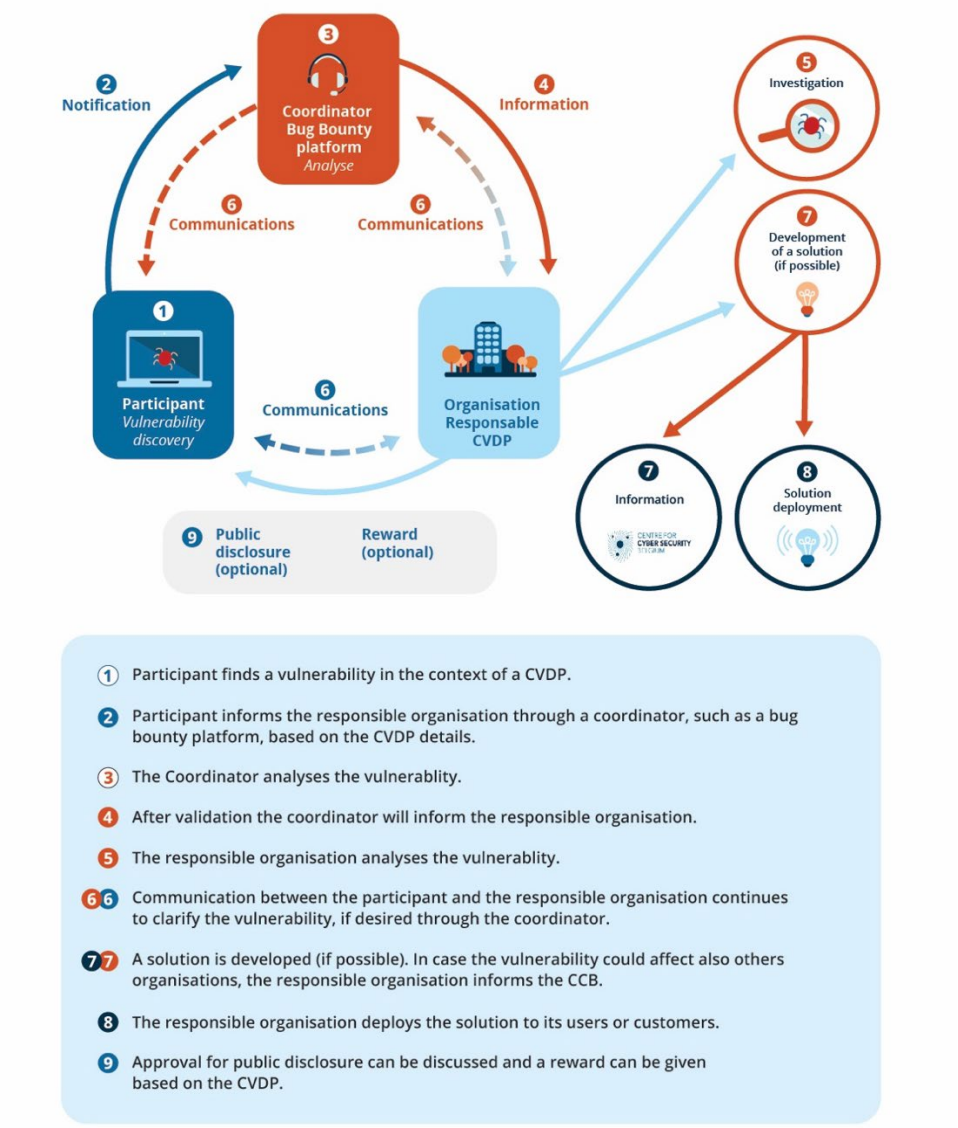
Figure 3 – CCB CVD process (I)



1. Participant finds a vulnerability in the context of a CVDP.
2. Participant informs the responsible organisation based on the CVDP details.
3. The responsible organisation analyses the vulnerablity.
4. Communication between the participant and the responsible organisation continues to clarify the vulnerability. assistance from the CCB (as coordinator by default) can be asked if there is a lack of communication in this process.
5 5. A solution is developed (if possible). In case the vulnerability could affect also others organisations, the responsible organisation informs the CCB.
6. The responsible organisation deploys the solution to its users or customers.
7. Approval for public disclosure can be discussed and a reward can be given based on the CVDP.

Source: Centre for Cyber Security Belgium

Figure 4 – CCB CVD process (II)



Source: Centre for Cyber Security Belgium

Lithuania

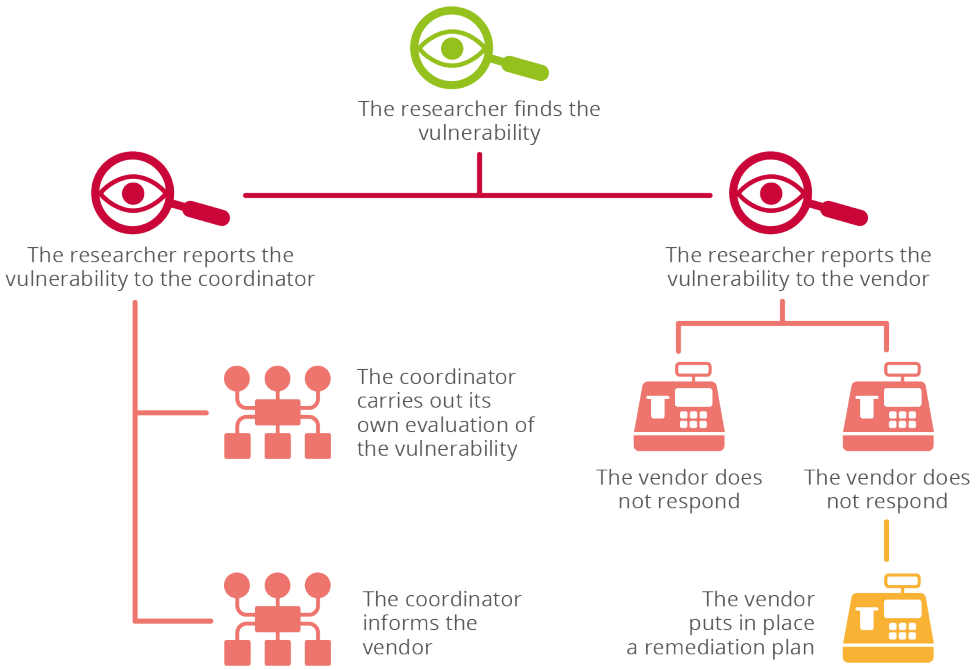
The **National Cyber Security Centre of Lithuania** has also put in place procedures that could serve as a basis for the drafting of best practices at the EU level.

According to the centre's policy, if the researcher decides to report the vulnerability to the National Cybersecurity Centre – or the vulnerability owner does not reply to the researcher – the cybersecurity centre carries out its evaluation of the vulnerability, informs the vulnerability owner, and obliges the vulnerability owner to evaluate the vulnerability and prepare a vulnerability remediation plan. If the researcher decides to report directly to the vulnerability owner, there is no coordination involved (unless the vendor fails in responding to the researcher's request). In both cases, the researcher needs to act according to the rules established in the law and share information about the research process he has conducted. Private entities' policies can envisage less severe requirements than those established in the national law (even no requirements at all). Notably, private entities cannot establish stricter

requirements than those envisaged at the national level. In the case of multiparty disclosure, the National Cybersecurity Centre is in charge of contacting all the interested parties that are affected by the same vulnerabilities.

According to the National Cyber Security Centre of Lithuania, given the reluctance of vulnerability owners to respond to researchers, the involvement of the National Cybersecurity Centre as a mediator in the process is particularly helpful, although as a more mature CVD ecosystem will unfold, the involvement of the National Cybersecurity Centre in the process could be reduced (see Figure 7).

Figure 5 – National Cyber Security Centre of Lithuania CVD process – Role of the coordinator



The Netherlands

The Netherlands is perceived as having established one of the most effective CVD processes in the EU.

According to them, the most important success factor for the Netherlands has been the **bottom-up approach** that was followed to set up the current CVD process. The process started with major banks and Internet Service Providers (ISPs) in the country feeling the urgency to accommodate ethical hackers in finding vulnerabilities. The country noticed that if companies, institutions or organisations are not faithful to individuals reporting vulnerabilities, it is difficult to force them to implement/adopt a CVD system. Hence, rather than requiring companies to establish a CVD policy (top-down approach), it is much more fruitful to stimulate an ecosystem in which researchers/hackers know they are safeguarded judicially and that they are acknowledged by society. At the same time, companies and organisations know that the rights and duties of researchers have borders, as they are not allowed to abuse vulnerabilities for whatever reason.

Other countries have highlighted a series of procedures that they have implemented that should be regarded as best practices.

- Talk to the vendor. Normally, vendors need to have processes in place for rolling out the patches for the discovered vulnerabilities following the normal software update cycle. Cooperating extensively with internal and external product experts also helps to understand the product's vulnerabilities or vulnerabilities details.
- Become familiar with the ethical hackers' community and properly value its work, for example by establishing bug bounty programs. In this respect, it has been argued by some Member States that the informal CVD recognition program does not provide the right incentives to be effective. Overall, it is important to manage the researchers' expectations by clarifying which type of incentives/rewards they can receive.
- Isolate the information that is received by the researcher and the information that is sent to the companies. Once an agreement between the two parties is established the communication can occur independently from the coordinator.
- Implement the OECD's good practices within the national strategy.
- Adopt the CSAF[95] to reduce the time between patch release and patch application.
- Base the CVD policy on international standards such as ISO 29147 and 30111.
- Provide CVD stakeholders with a 'Vulnerability Disclosure Toolkit'[96] as operated by NCSC UK since September 2021. This guide is dedicated to all organisations willing to set in place a vulnerability disclosure process and governance. The document refers to three main CVD aspects: Communication, Policy and Security.

3.3 CHALLENGES AND ISSUES

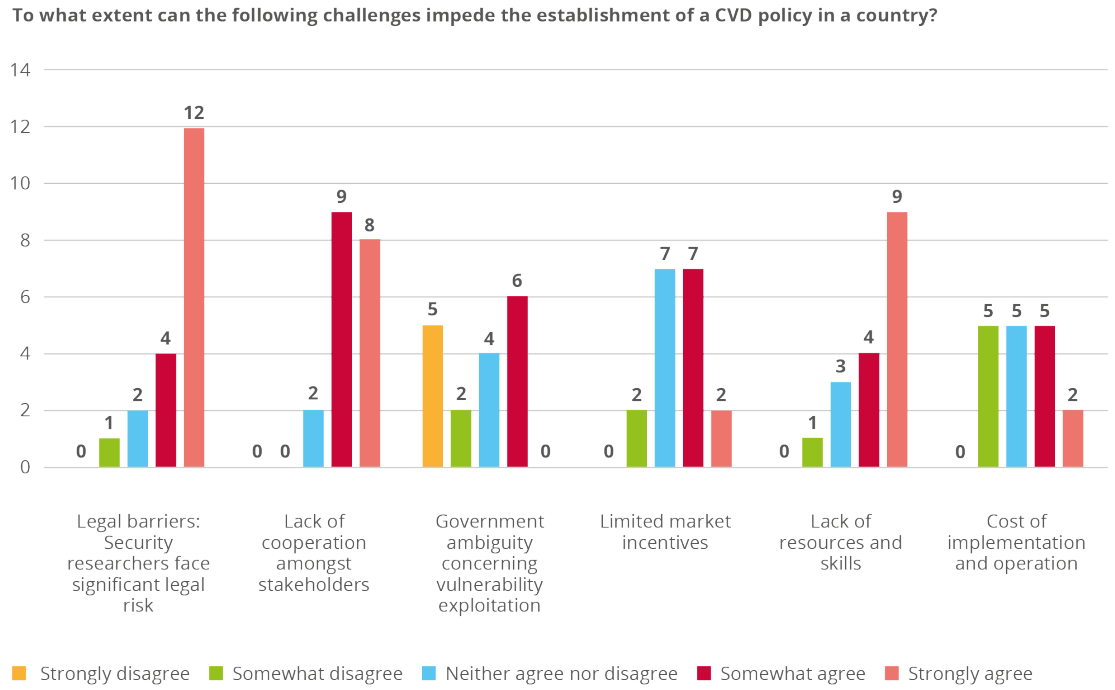
This Section presents an overview of challenges and issues related to the definition of coordinated vulnerability disclosure policies in the EU. Legal, economic, policy and technical challenges are addressed. During the interviews with Member States, to assess the challenges that Member States face in setting out a CVD policy, they were asked to comparatively evaluate to what extent the following challenges impede the establishment of a CVD policy in their countries.

- Legal barriers. Security researchers face significant legal risk.
- Lack of cooperation amongst stakeholders.
- Government ambiguity concerning vulnerability exploitation. Government looking for / stockpiling vulnerabilities to exploit as part of their law enforcement, intelligence and national security activities.
- Limited market incentives. Incentives for security researchers to participate in coordinated vulnerability disclosure programmes.
- Financial and human resources challenges. Lack of resources and skills, and costs of implementation and operation.

Figure 8 shows that legal barriers and the lack of cooperation amongst stakeholders represent the greatest challenges. 84 % of Member States (16) believe that legal barriers have a strong or at least some impact in the process. Similarly, 89 % of Member States (17) consider the lack of cooperation among stakeholders to either strongly or somewhat impede the establishment of a CVD policy.

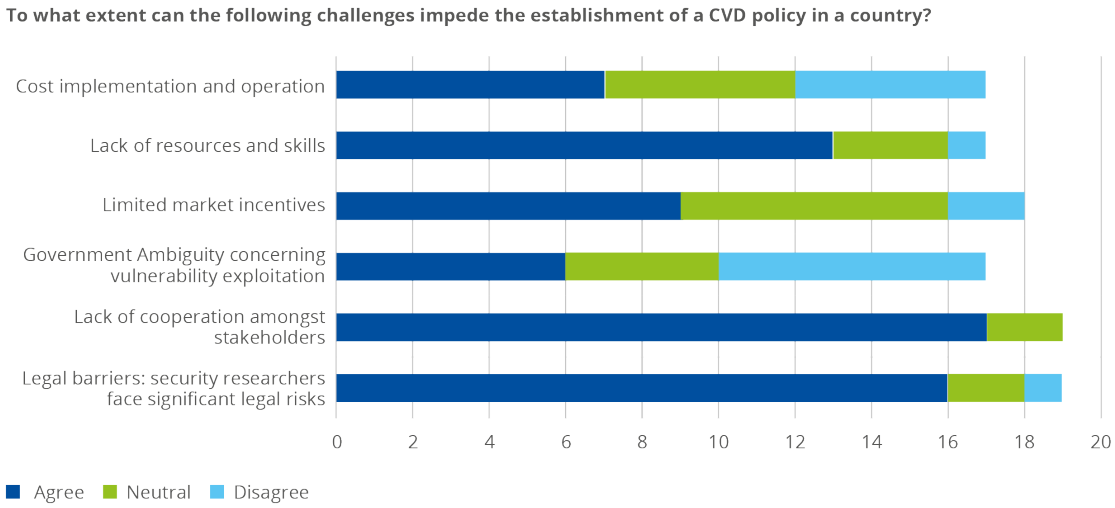
[95] *OASIS (2017), CSAF Common Vulnerability Reporting Framework (CVRF) Version 1.2. Available* at: http://docs.oasis-open.org/csaf/csaf-cvrf/v1.2/csaf-cvrf-v1.2.html
[96] NCSC UK (2020), *Vulnerability Disclosure Toolkit.* Available at: https://www.ncsc.gov.uk/information/vulnerability-disclosure-toolkit

Figure 6 – Evaluation of the different barriers to the establishment of a CVD policy



Source: Interviews with EU Member States

Figure 7 – Aggregated evaluation of the different barriers to the establishment of a CVD policy



Source: Interviews with EU Member States

3.3.1 Legal challenges

The legal challenges faced by researchers when they report a vulnerability to a vulnerability owner is considered one of the most significant obstacles to adopting CVD policies[97]. According to the OECD, legal challenges 'are enabled by an overall legal environment that does not sufficiently protect security researchers and by the behaviour of many vulnerability owners threatening security researchers with legal proceedings when receiving reports'[98].

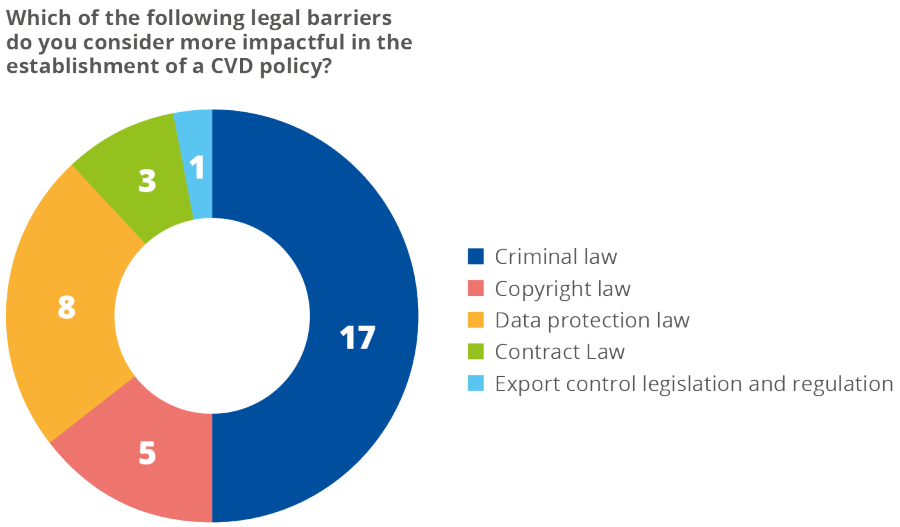
There are several areas of legal challenges researchers can face.

- Criminal law. According to the Cybercrime Convention, intentionally accessing a computer system without rights is a criminal offence. Since the cybercrime directive (2013/49/EU) sets minimum protections, the Member States can adopt stricter rules.
- Copyright law. Researchers can breach copyright law when the information disclosed entails portions of copyrighted code. The vulnerability owners can establish exemptions, enabling the possibility of safe harbours.
- Data protection law. Researchers discovering vulnerabilities may access personal data which could be interpreted as a breach of data protection law. Most vulnerability deals with personal data, interest in reporting versus interest in data protection can clash.
- Contract Law. Bug bounty policies and in some cases vulnerability disclosure policies represent the terms of a contract between the vulnerability owner and the researcher. Breaching the terms of the contract entails legal liability and risks for the researcher,
- Export control legislation and regulation are often cited as a legal risk for researchers as they may apply to tools and knowledge used to discover vulnerabilities.

As shown in Figure 10, the great majority (17) of Member States consulted consider criminal law to be the most pressing legal challenge, followed by data protection law.

[97] *ENISA (2016),* ENISA *Threat Landscape Report* 2016 – 15 top cyber threats and trends. *Available at* https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016; See footnote (7).
[98] *OECD (2021), 'Encouraging Vulnerability Treatement – Overview for policy makers', OECD Digital Economy Papers, No 307, OECD Publishing, Paris, France, February, p.°27. Available at*: https://www.oecd.org/sti/encouraging-vulnerability-treatment-0e2615ba-en.htm;

Figure 8 – Impact of the legal barriers in establishing a CVD policy



Source: Interviews with EU Member States

Criminal law

In most EU countries, the legal framework has not been updated to provide for researchers' legal protections. According to the existing legal provisions in place in most cases, anyone who finds and discloses a vulnerability by scanning a system without prior authorisation is bound by criminal law and other legislative clauses.

Both in the cases in which the researchers were actively searching for vulnerabilities and in the cases in which vulnerabilities are found by accident during the normal use of a system, the researcher might inadvertently gain access to critical data he was not supposed to gain access to. In this context, disclosing vulnerabilities without prior authorisation is, hence, not allowed. Notably, these are distinct cases from accesses where consent is granted in the form of pen testing arrangements between parties.

But what is the link between finding vulnerabilities and criminal law? According to CEPS (2018), from a criminal law perspective there are two questions relevant for the process of finding vulnerabilities as opposed to reporting them. The first one is 'a substantive one and concerns the circumstances under which finding vulnerabilities may be associated with a criminal offence, that of illegal access to information system';the second one is 'procedural and relates to the conditions that need to be met for any crimes associated with finding vulnerabilities to be prosecuted'[99].

Regarding the first question, Article 2 of the 2001 Council of Europe Convention on Cybercrime (**the Budapest Convention**) mentions what should be meant by illegal access to an information system when it states 'Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right'. According to CEPS (2018), this means that there are four conditions that need to be met for illegal access to apply under the cybercrime convention: the person should have accessed the system intentionally; that person should have actually had access to the computer system; that access

[99] Pupillo, L., Ferreira, A. and Varisco, G. (2018) 'Software Vulnerability Disclosure in Europe: Technology, policies and legal challenges – Report of a CEPS Task Force', CEPS Task Force Reports, 28 June 2018, p. 42. Available at: https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges/

should concern either the whole or part of the computer system; and that person should have no right to access the system'[100].

Directive 2013/40/EU of 12 August 2013 (**the cybercrime directive**) reflects the Budapest Convention and states that 'when committed intentionally, the access without right, to the whole or to any part of an information system, is punishable as a criminal offense were committed by infringing a security measure'.

Therefore, as stated also by the OECD (2021), according to the **Budapest Convention only the unauthorised access should be considered as criminal offence**. It follows that computer system owners can authorise access through the publication of a vulnerability disclosure policy, allowing for the protection of security researchers (a limited liability waiver).

When it comes to the second question – the procedural one – related to the conditions that need to be met for any crimes associated with finding vulnerabilities to be prosecuted, several countries mentioned during the interview that the interpretation of the intentions of the researchers by the prosecutor should make it possible to adequately guarantee a level of legal protection for the researchers.

The Netherlands is the most renowned case in Europe, where researchers are protected based on a formalised prosecutorial discretion within defined boundaries. The prosecutor in a case examines three aspects/questions: is the researcher acting in the interest of society? Are the means used by the researcher proportional? Is the subsidiarity principle fulfilled (were there other means to accomplish the same goal)? For example, brute-force attacks or entering a system and waiting a long time to report the vulnerability are deemed criminal. If one of these three aspects is not fulfilled, then it is expected that the judicial system will prosecute the researcher.

Similarly, according to the **Hungarian** case-law, there is judicial discretion to decide whether the 'ethical' hacking (in the lack of contractual basis) is dangerous to society or not. If it turns out that the committed activity was not dangerous to society – therefore not a crime – the perpetrator cannot be punished. Of course, in these cases, the court also takes further conditions into consideration (e.g. the intent of the suspect and other factors).

Furthermore, the **CCB** has played an important role in clarifying in its CVD policy the interpretation of how the current criminal law can be applied in a way that would allow for the CVD process to take place and, similar to the Netherlands, the public prosecutor has clarified the interpretation of the law.

Likewise, according to the **BSI**, a CVD policy can be drafted and published based on the legal foundation already in place in a country. Criminal law only mandates the researcher to behave in a certain way ('to play by the rules'). The BSI's CVD policy incorporates this principle by establishing boundaries to the researcher's behaviour. Aspects related to the level of detail of the reporting could be critical (e.g. a researcher is required to not disclose some information that might be useful for the public), nonetheless, legal challenges do not overall impede the establishment of a CVD policy. Once the vulnerability is processed, there are no legal hindrances to the process. To incentivise reporting without the fear of legal proceedings, the BSI enables the possibility of anonymity via an ad hoc form on its website. Overall, even if reporting to the BSI is not free of any legal consequence, the court always takes into consideration the good intent of the vulnerability finder. Following a published CVD policy could be considered as an indicator of good intent.

[100] Pupillo, L., Ferreira, A. and Varisco, G. (2018) 'Software Vulnerability Disclosure in Europe: Technology, policies and legal challenges – Report of a CEPS Task Force', CEPS Task Force Reports, 28 June 2018, p. 43

The **Ministry of Justice of Denmark** has made a similar evaluation. According to this evaluation, publishing a CVD policy is regarded as a statement from the vulnerability owner that it will not pursue a legal proceeding if the security researcher acts within the framework of the published policy. **It is a limited liability waiver.** In the event that there is a disagreement among the parties, the decision is ultimately made by the court.

Therefore, considering the answers to both questions, the approach followed by some countries in the EU of establishing a CVD policy without the amendment of the penal dode is coherent with the Budapest Convention and could be considered sufficient to offer a safe harbour to security researchers.

However, it is important to mention that since criminal law is a prerogative of Member States and the cybercrime directive, as a piece of EU legislation, it affords only a minimum level of protection. The interpretation of what constitutes illegal access varies among Member States. Therefore, as mentioned by **some other Member States**, although the Budapest Convention establishes that only unauthorised access to systems is prohibited – and as such, having in place a CVD policy might be sufficient to guarantee some level of protection for the researchers even without amending the legal framework – **establishing a CVD mechanism needs to be grounded on more specific criminal law rules concerning the discovery of vulnerabilities.** In particular, the legal framework needs to specify which cases would count as unauthorised access. Hence, while organisations might authorise researchers to access their system and prevent researchers from being legally prosecuted, to ensure trust in the CVD process, guarantees at the institutional level should be established. As such, to promote a national CVD policy the government must proceed with the necessary legal fundamentals.

Furthermore, there are also several Member States (8) that strongly advocate for an amendment of the penal code in place in their countries or have already proceeded with amending the criminal code.

In **Lithuania**, for example, before the implementation of the law on cybersecurity, the researchers' activities were considered a violation of criminal law. As such, the main purpose of the law has been precisely to create a safe harbour for the ethical hackers to operate whenever they act in line with the established obligations. The principles for the establishment of this safe harbour and the rules of behaviour that the researchers have to respect have been taken up also by the Prosecutor General's Office and police department.

Analogously, while the **French** law does not provide immunity to criminal law or such in this context for researchers, it envisages two protective legal frameworks that can account for partial protection of the security researcher:

Article L 2321-5 of the French defence code provides a protected alert framework to the French national cybersecurity authority when discovering a vulnerability. This authority does not have to refer such alerts to Justice if some conditions are respected.

A whistleblower framework also exists (art 6 à 16 de la Loi No 2016-1691) but it is more about 'incidents' than vulnerabilities.

Greece does not have the type of judicial exemptions described but means to establish one. The country does have a constitutional provision (Article 16 Constitution of Greece) which deals with the freedom of academic expression. This provision, while it cannot be interpreted as granting a right to violate the existing criminal law, it is a basis upon which academics and scientists are currently being protected in the execution of their duties. As mentioned, however, Article 16 does not preclude the application of criminal law. There are also legal clauses related to intellectual property rights that allow for a degree of flexibility when, for example, a protected document is copied for academic or scientific research. The Greek system has, thus,

recognised the importance of academic expression, although the parameters for allowing unauthorised access to systems for research purposes are yet to be defined.

According to **Portugal,** one of the main ideas when adopting a CVD policy will be to establish a safe harbour for researchers (non-criminalisation of the researchers' activities) when they demonstrate good intentions. The national policy itself will be a framework that can be used to check on the intentions of the researchers as it provides a series of indications on the steps that researchers should follow to properly report a vulnerability. Besides, the researchers' intentions can be assessed by looking at the logs in the system where the vulnerability is found (e.g. which kind of tools and techniques the researcher used to find the vulnerability).

In the context of the discussion on the impact of criminal law challenges, the Member States have been asked whether national or EU jurisdictions address the protection of security researchers and if they plan on establishing or have established legal immunity (through criminal law exemptions, for instance) or judicial or prosecutorial discretion, based on an *ex post*, case-by-case assessment.

Most of the consulted Member States (11) do not plan on establishing legal immunity by amending the criminal code, hence the introduction of criminal law exemptions. In some cases (6), as mentioned, Member States do not consider it necessary to amend the criminal code because the protection of the researchers is / will be based on judicial discretion.

In some other cases, the Member States do not plan on amending the criminal law due to the opposition that was faced in the past from the national governments and the state police. Given that this represented one of the main stumbling blocks, countries are proceeding with the implementation of a voluntary policy or including CVD in the cybersecurity strategy and raising awareness on the topic. Very likely, they will move forward with amending the criminal law if the provision of the NIS2 directive, which suggests that Member States adopt cybersecurity strategies that include CVD policies, will create the right context to do so.

Data protection law

According to several responding countries, the data protection law is also relevant, as it requires the balancing of the rights for the protection of personal data when somebody identifies a vulnerability in a system's database with the effectiveness of the research activities.

However, under some legal frameworks, such as the Belgian one, if you have a clear privacy statement and the data protection law is respected, establishing a CVD policy would not be challenging. Notably, the relationship between the vulnerability owner and the researcher could be seen as a subcontract: the ethical hacker could be seen as the processor of the personal data in the event that personal data is found during its activities according to the GDPR aspects of the CVD policy. If the policy is not clear enough on the privacy aspects, the researcher could be seen as a data controller. Overall, the researcher is dealing with any sort of data and the most important aspect is the confidentiality of the process [101].

Other legal challenges

According to some countries, if you have a traditional kind of product (running on a user's computer), **contract law is also an impactful legal challenge.** Very often, researchers must contact cross-border vendors (usually in the United States). These products include licensing rules stating that all the disputes concerning the product are handled according to US law. However, United States contract law might contain provisions stipulating that all reverse engineering is prohibited (including the type of testing employed for finding vulnerabilities). Similarly, the DMCA could lead to legal liabilities and risks for the researcher. Researchers

[101] According to some experts, this idea should be further evaluated since the controller-processor relationship must be bilaterally agreed and put in writing. Therefore, a policy would not be enough of a waiver for data protection law.

testing products under the EU's customer protection law have different legal obligations, and this leaves room for interpretation and uncertainty. This is one of the reasons why CERTs intervene in these cases and report the vulnerability on the behalf of the researcher so that the researcher will not have to face the legal burden. Additionally, national software companies might include in the contractual obligations with the third party purchasing their product the prohibition to perform CVD.

Cross-border dependencies also create additional legal barriers. While in recent years there has been a greater degree of cooperation between the Member States, this could be handled more efficiently. Establishing contacts in different universities and private companies around EU have been proven to be useful, but the most effective way to enhance the cooperation between the Member States in case of cross-border dependencies would be to improve the single-point-of-contact system established with the NIS directive.

3.3.2 Economic challenges

As acknowledged in the *Economics of Vulnerability Disclosure* report by ENISA[102], economic factors play an important role in the development of vulnerability disclosure policies. While quite often information security is regarded only as a technical issue, the underlying factors that characterise the persistency of vulnerabilities in hardware and software are only partially related to the nature of vulnerabilities themselves, since to a great extent come from the economic aspects of information security and its market dynamics.

Today, many ICT products are embedded with software and hardware and can connect to networks. Besides the very recent attention from policymakers directed towards these products, it is important to mention that while in some sectors, such as aeronautics, manufacturers have been ahead of regulation in considering cybersecurity in their production processes[103], the software industry has, for instance, strongly opposed assuming liability for its products over the last 50 years, as the car industry did for the first 70 years of its existence. This approach is generated by economic incentives that, according to some researchers, can be as detrimental for security as bad technical design[104]. This approach from the software industry has its own rationality. In a market in which network economics apply, exploiting the 'first-mover' advantage requires being first to market even if the product is not perfect ('we'll ship it on Tuesday and get it right by version 3.0')[105]. However, it is clear that this approach values cost-effectiveness, usability and time to market over security. Indeed, using security-by-design guidelines and updating software rise costs increase time to market and make products less user friendly with negative effects on the product demand. Therefore, a rational behaviour from a company conflicts with the optimal level of security. This misalignment of incentives while in a competitive market in general does not exist, in a market with network economics[106] it is becoming the norm.

Furthermore, even if the alignment of incentives is correct, the market could fail to deliver optimal levels of security given to information asymmetries and negative externalities. Examining the ICT products market, market failures are generated from one side by information asymmetries – the customer does not have a clear and neutral idea of the level of security of

[102] *ENISA (2018), Economics of Vulnerability Disclosure, December 2018. Available at:* https://www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure
[103] *OECD (2019), 'Role and Responsibility of Actors for Digital Security',* OECD Digital Economy Papers, *No 286, OECD Publishing, Paris, France. Available at:* https://www.oecd-ilibrary.org/science-and-technology/roles-and-responsibilities-of-actors-for-digital-security_3206c421-en
[104] *Anderson, R. and Moore, T. (2006), Information Security Economics – and Beyond. Available at*: https://www.researchgate.net/publication/221355448_Information_Security_Economics_-_and_Beyond
[105] Anderson, R. (2001), 'Why information Security is Hard – An Economic Perspective', paper prepared for 17th Annual Computer Security Applications Conference (ACSAC01), EEE Computer Society, December. Available at: https://www.researchgate.net/publication/3941712_Why_Information_Security_is_Hard-An_Economic_Perspective
[106] Market with network economics is characterized by: high fixed costs and low marginal costs; network externalities on the demand side; path dependency; and customers lock-in. Therefore, the outcome of these markets is quite often that 'the winner takes all' (see Varian, R. and Shapiro, C. (1999), Information Rules – A strategic guide to the network economy, Harvard Business School Press, Boston MA, United States).

the product – and from the other side by negative externalities – software producers are not accountable for the damages created by the exploitation of vulnerabilities in their products.

There is also an additional factor that needs to be considered: the changing nature of the information security market. The information security market of today is very different from yesterday's market. Today, with software and hardware embedded everywhere and always being used by almost everybody, the vulnerability surface is increasingly dramatically. At the same time, many companies that have not traditionally had a relevant presence in the ICT sector, such as automotive or white goods producers, are starting to develop products with integrated software and hardware components and, therefore, need to familiarise themselves with secure development and information security and understand how to implement vulnerability disclosure policies – a complete new domain that requires a technical and organisational maturity unknown to them until very recently[107].

Therefore, according to ENISA (2018), 'the changing nature of the information security market also has consequences for the economics of vulnerability disclosure, how vulnerability disclosure is carried out, and how actors behave in the vulnerability disclosure process'[108]. It will increase vulnerability complexity and the number of vulnerabilities that will require multi-vendor coordination. Since the vulnerability disclosure process is characterised by the action of multiple economic agents, quite often with conflicting interests, **it will become increasingly important to use regulations or incentive mechanisms to mitigate or eliminate the aforementioned negative market outcomes.**

Incentives can take a financial or a not financial form. Monetary rewards for finders from bug bounty programmes are the most common financial incentives. Non-financial incentives have ad hoc characteristics that inspire a behaviour not directly connected to monetary rewards. This is the case of finding vulnerabilities for the technical challenge it offers, for the prestige that this action entails (some companies create a 'hall of fame' for security researchers that find vulnerabilities) or for ethical or ideological reasons.

During the interviews with Member States, (as shown in 53Figure 9), several (9) suggested that **limited market incentives** for security researchers to participate in coordinated vulnerability disclosure programmes **have a strong impact on the establishment of a CVD policy in the EU.**

Furthermore, vendors do not have incentives to offer secure products. Indeed, while consumers can understand the usability and price of a product, they are unable to assess its level of security. This can generate adverse selection: since customers are unable to distinguish more secure products from less secure products, developers offering more secure products will not be rewarded since customers will not be willing to pay for it.

It should also be noted that most security researchers are activists, not professionals since professional researchers usually would rather work for private companies. This is due, among other reasons, to the limited market incentives that are in place now in terms of (economic) rewards that are provided to researchers, for example through bug bounty programmes.

Furthermore, most Member States (13) regard the lack of resources and skills to implement coordinated vulnerability disclosure policy as being particularly impactful. This challenge impacts vendors, as they might not be able to build secure products, but also makes it harder to find the vulnerabilities as researchers are not numerous. The adoption of CVD processes can be challenging for coordinators as well (i.e. national CERTs or national cybersecurity

[107] *ENISA (2018), Economics of Vulnerability Disclosure, December 2018, p. 24. Available at:* https://www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure
[108] *ENISA (2018), Economics of Vulnerability Disclosure, December 2018, p. 24. Available at:* https://www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure

authorities) if there are no resources to help handle and understand the criticality of the vulnerability. Indeed, in the case of a highly technical vulnerability found in a specific sector (e.g. aviation sector), the national CERT might lack the required skills and capabilities. As such, the trust of the parties in the ability of the national CERT to handle the vulnerability is undermined. Hence, the lack of resources and skills applies to and affects all stakeholders.

On the other hand, the **costs of implementation and operation** have been regarded as relatively less impactful. According to the CCB 'setting up costs of a coordinated vulnerability disclosure policy are more budget-friendly than having external companies perform audits. After all, the reward for a bug bounty programme is the result of a commitment on the part of the participant to achieve a certain result, whereas an external auditor is usually only bound by a commitment of means. The latter must therefore be compensated for all their activities, even if they have not found any vulnerabilities or only minor vulnerabilities at the end of their investigation.'[109]

An additional economic challenge to effective vulnerability treatment is the lack of cooperation among stakeholders. Most of the **Member States interviewed (17) consider that the lack of cooperation among stakeholders either strongly or somewhat impedes the establishment of a CVD policy. All consulted Member States consider addressing the lack of coordination between vulnerability owners and researchers as more challenging than addressing the lack of coordination at the level of CSIRTs.**

In this context, the most critical issue is that researchers see the vulnerabilities as more severe than the vulnerability owner, and the timeline for disclosure set by the owners as too lax. Additionally, challenges in the coordination exist due to the lack of preparation of the vulnerability owners on how to handle vulnerability reports. To give an example, one Member State mentioned that some years ago several researchers were using an open bug bounty platform to contact vulnerability owners. However, the contacts that were on the platform were often incorrect or the reports would end up in the spam folder of the vendors' email inboxes. This problem has been overcome thanks to the intermediation of the national CERT. As time went by, indeed, researchers started to include the CERT as an email recipient when contacting the vendors.

On the other hand, it has been argued that at the level of national CSIRTs, vulnerability disclosure mostly stays within the perimeter of the CSIRT itself. Besides, even when a non-EU country is involved and coordination would be needed, the level of coordination among CSIRTs is already quite well established via communication channels for incident response.

Finally, considering the role of the government in taking action to address the grey market for code vulnerabilities as an economic chalenge, it is interesting to notice that no consulted Member States consider addressing the grey market as a priority. Indeed, it has been argued that the government could outlaw the selling of vulnerabilities to foreign agencies, but it might be very challenging to address researchers' selling of vulnerabilities on the grey market.

3.3.3 Political challenges

In this Section the challenges related to the development of the vulnerability disclosure process and the roles and dynamics of the different stakeholders will be assessed.

Top down or bottom-up approach?

One of the issues raised during the analysis of the status of play of the EU experience on CVD policies and the interviews with Member States is the different dynamics followed in developing CVD policies, namely a bottom-up v a top-down approach. The Netherlands consider having

[109] Centre for Cybersecurity Belgium (2020), Guide to Coordinated Vulnerability Disclosure Policies Part I: Good Practices. Available at: https://ccb.belgium.be/sites/default/files/Guide%20CVDP%20part%20I%20Good%20pratices.pdf

followed a bottom-up approach as the most important success factor for their CVD policy. The process started with the major banks and ISPs in the country feeling the urgency to accommodate ethical hackers in finding vulnerabilities. The country noticed that if companies, institutions or organisations are not faithful to individuals reporting vulnerabilities, it is difficult to force them to implement/adopt a CVD system. Hence, rather than imposing companies to establish a CVD policy (top-down approach), it is much more fruitful to stimulate an ecosystem in which researchers/hackers know that they are safeguarded judicially and that they are acknowledged by society. At the same time, companies and organisations know that the rights and duties of researchers have limits, as they are not allowed to abuse vulnerabilities for whatever reason. Some other Member States, such as France, are instead in favour of developing a more centralised approach.

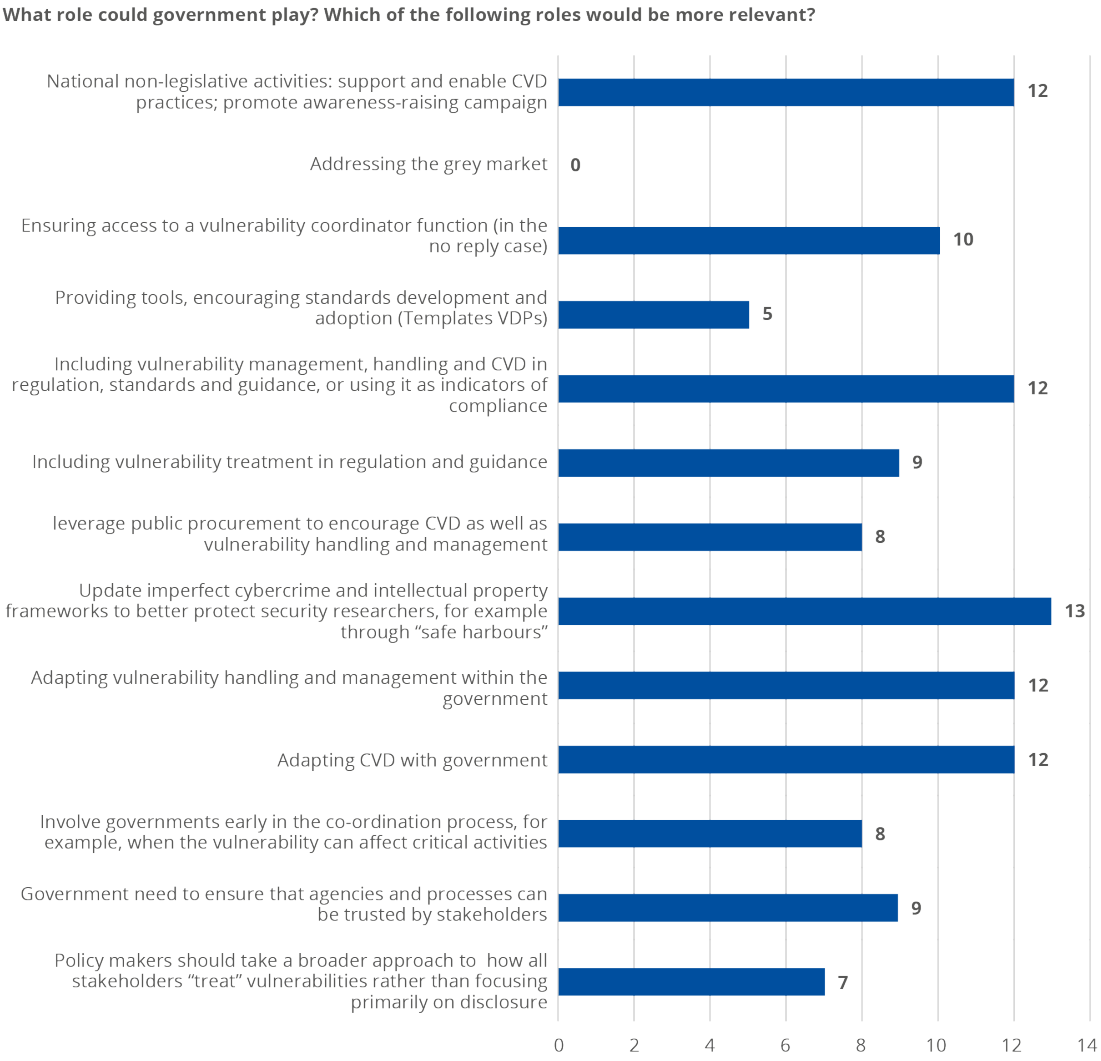
The role of government

The Member States have been consulted concerning the role that government can/should play to ease the establishment of a national CVD policy. As shown in Figure 11, **among the proposed actions, most of the Member States (13) consider updating imperfect cybercrime and intellectual property frameworks to better protect security researchers, for example through 'safe harbours', as the most important action governments could carry out**. Changing criminal law will be, however, only one step in the process. Indeed, a safe harbour could be established for well-intentioned researchers accessing a system without authorisation, but this will not cover all the different offences/violations that could occur in the process. As such, this action should be accompanied by other actions aimed at fostering an overall trusted environment for CVD.

More generally, all actions that government could carry out to lead by example in the establishment of a CVD policy (i.e. adapting CVD within the government; adapting vulnerability handling and management within the government; including vulnerability management and handling and CVD in regulation, standards and guidance, or using them as indicators of compliance) are regarded as essential. Governments should lead by example, especially in economies where there are numerous vendors and a great variety in the level of acceptance of the vulnerability reports and in the value attributed to secure products. In this context, first convincing public entities to adopt CVD and reassuring them that the reports will be handled is considered as important.

National non-legislative activities (e.g. supporting and enabling CVD practices and promoting awareness-raising campaigns) have also been particularly appreciated by several Member States (12).

Figure 9 – Role of government



Source: Interviews with EU Member States

The role of the private sector

Different approaches can be distinguished when a CVD policy is established at the level of private companies or at the governmental level. Companies enjoy a degree of flexibility when adopting a CVD policy, and they can do so irrespective of a CVD policy being adopted at the governmental level.

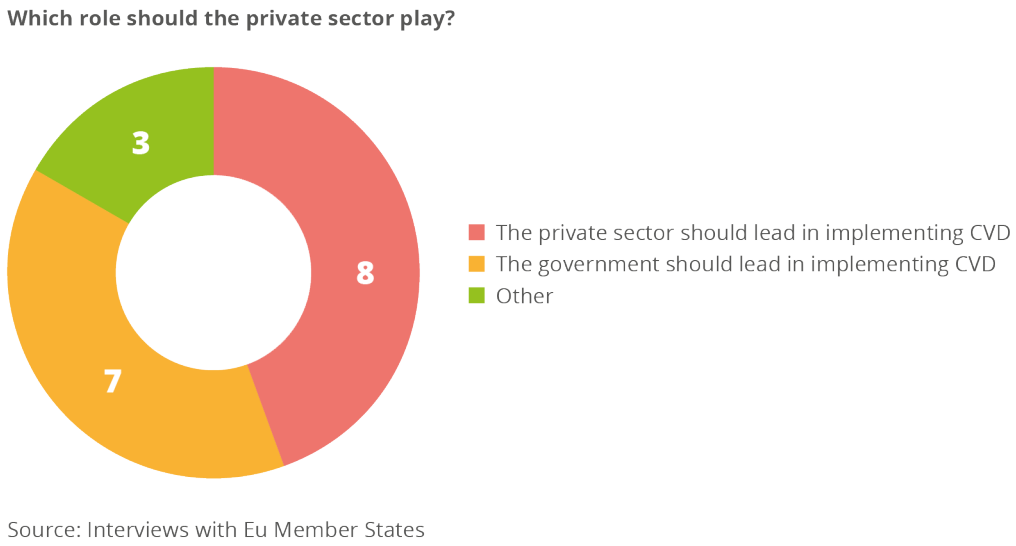
For their part, companies need mainly to use existing documents and apply them in a flexible manner to implement the necessary processes, develop a policy and publish it on the company's website. Establishing a policy at the governmental level entails instead fostering an overall ecosystem in which vulnerabilities are accepted and acknowledged. As such, CVD policy at the governmental level may introduce or enhance a third-party coordinator (e.g. CSIRT), should foster awareness-raising activities, support the legal sector in identifying possibilities and mitigate the legal challenges (e.g. prosecution or liability of the security researchers) with regard to coordinated responsible disclosure.

These two processes are clearly related since establishing a policy at the governmental level might increase the chances of private companies implementing policies at their individual level

and security researchers engaging in finding vulnerabilities. This, as mentioned above, should not necessarily take the form of an obligation from the government to private entities but can entail stimulating a societal environment in which security researchers are safeguarded judicially and are acknowledged by society.

This being said, when it comes to the role of the private sector in developing vulnerability disclosure policies, there are different views among the Member States. As illustrated the Figure 12, consulted Member States are divided on whether the private sector or the government should lead the process or not.

Figure 10 – Role of the private sector



Source: Interviews with Eu Member States

According to some Member States, companies should not wait for a government legislative/policy intervention, especially because establishing a CVD policy at the company level is already possible within some of the existing national legal frameworks. Therefore, the private sector could take the lead in implementing coordinated vulnerability disclosure by defining and publishing on the companies' website public reporting mechanisms on vulnerabilities disclosure according to the ISO standards and best practices. Furthermore, some Member States mentioned that one of the most important aspects for the private sector to take the lead in is the establishment of bug bounty programmes, as they help in fighting the vulnerability taboo.

Besides, according to a consulted Member State, in many cases researchers have found that the private sector is more appropriately positioned for dealing with vulnerability disclosure rather than state-sector entities. Indeed, in some cases state entities have limited resources and capabilities to deal with CVD, especially because the resources allocated for national security can be scarce. On the other hand, there are large companies that have well-established policies and disclose them publicly. In this context, it should be noted that CVD should be considered necessary only insofar there is insufficient trust between the finder and the industry. As such, direct disclosure should be promoted.

Moreover, irrespective of a CVD policy being established at the national level, companies will still have to carry out their verification of the data the researcher has provided them with. In this context, the role of the coordinator can be questioned. If the role of the CERT in the CVD process is intended only as a facilitator of the communication between the parties, it could be beneficial. However, in a CVD process, CERTs can also be empowered with the verification of the information, and there might be cases in which CERTs are badly equipped to carry out these activities, further undermining the trust in the process. This is usually the case with highly

technical vulnerabilities in specialised sectors. As such, mandating national CERTs to undertake a coordinator role in the CVD process might not be the most appropriate way to go for all Member States. In some cases, CERTs will be not equipped with adequate resources, nor would they have the required links with the industries and the researchers' community. In this context, the EU should promote industries to take the lead and disclose their vulnerability management policies along with promoting direct disclosure.

Notably, the process for the establishment of a CVD policy in **the Netherlands** has been initiated by the private sector, specifically by banks and ISPs. These companies led by example and started establishing CVD policies. This allowed for the creation of an ecosystem in the country in which there is a societal awareness of the usefulness of the CVD process.

In other countries, the private sector also seems willing to take the lead in the CVD process. For example, **Belgium** mentioned that while the private sector must increase its overall level of maturity, the Cybersecurity Coalition[110] is considering implementing its cybersecurity policy, and leads by example. Similarly, in **Finland,** some vendors such as ICASI are already taking the lead in establishing CVD policies and industry consortiums, and trying to deal with CVD and play a role in the development of standards. Notably, Finland considers thatinitiatives at the level of industry consortium can have a greater impact than initiatives at the company level.

On the other hand, several Member States believe that the example should be given by the government. Among the arguments that have been provided, the Member States mentioned that the private sector is constrained by economic considerations. Hence, the example should be given by the government which can foster a favourable ecosystem for IT security. The private sector should participate in the discussions with governments and understand that the final goal of the government is not to regulate private entities but to create a more secure ecosystem. This can also be fostered by creating communication groups with representatives of vendors, or communication groups with sector-specific stakeholders. Establishing safe and reliable communication channels could indeed allow more information concerning vulnerabilities to be shared between parties.

Besides, in some cases, the capabilities of the private sector are too limited (especially for SMEs). Implementing a CVD policy without a well-established security researcher network and a government coordination network could be risky as the companies would not have the resources and skills to handle the inflow of information, the patching and the disclosure. Furthermore, if the government takes the lead in the establishment of a national CVD policy, greater harmonisation of the processes can be assured. As such, having a patchwork of different incoherent policies can be avoided.

Finally, for some of the smaller countries, the private sector is not expected to take the lead given the size of the internal market.

In most of these countries' views, the private sector is in a leading position in establishing bug bounty programmes. The private sector can also help to develop standards and codes of conduct defining the practical aspects of a CVD policy. Following a harmonised approach towards CVD among private organisations also allows benefits to be disseminated more effectively and market imbalances to be reduced.

[110] Partnership between players from the academic world, the public authorities and the private sector with currently more than 100 key players from across these three sectors as active members

4. RECOMMENDATIONS

According to CEPS (2018), in May 2018 only two countries had CVD policies in place: the Netherlands and France. Section 2 of this report shows that there are two other countries that have recently implemented CVD policies (Belgium and Lithuania), four additional countries are close to releasing their policies and there are ten other countries where this process is in progress. These data show that, although the situation on CVD policies in the EU is still fragmented, the awareness of the need to develop them is growing and that, amid a lack of legal certainty for security researchers, some countries are still using the current legal framework or are amending national criminal laws to promote CVD policies in the EU.

In this Section, the challenges previously mentioned will be addressed focusing on the current best practices in the EU.

4.1 RECOMMENDATIONS ON LEGAL CHALLENGES

It has been mentioned that legal risks faced by security researchers represent a major obstacle to the development of vulnerability disclosure policies. However, the current practices among Member States can suggest a modular approach to overcome these challenges.

First, as suggested by the CVD policy implemented by Belgium, since according to the Budapest Convention only unauthorised access is unlawful, **EU countries could implement CVD policies that will offer a limited liability waiver to security researchers** if they comply with ad hoc requirements such as those of the CVD policy described in the Belgian or also in the Dutch model of disclosure. According to the CCB, Belgium is a civil-law country and all the countries that have signed the Budapest Convention could follow their example. A boost in this direction could be offered by the adoption and transposition of the NIS2 directive, which requires Member States to design cybersecurity strategies that include 'policies to promote and facilitate coordinated vulnerability disclosure …' [111]. Furthermore, according to some Member States such as the Netherlands, Hungary, Denmark, Germany and Austria, the interpretation of the intentions of the researchers by the prosecutor should adequately guarantee a level of legal protection for the researchers.

Second, if national criminal laws put ad hoc limitations on the possibility of offering a liability waiver to security researchers, **Member States could amend their criminal laws** to create the legal certainty and the necessary 'safe harbour' for researchers involved in vulnerability discovery, also recognising ethical hacking. Countries like Lithuania have recently amended their penal code, countries like Portugal, Greece, Slovenia and Spain are in the process of doing so.

Third, the **EU could amend the cybercrime directive** to offer legal certainty to security researchers involved in vulnerability discovery and to allow for the definition of common rules and procedures across Member States to allow for a common process of software coordinated vulnerability disclosure in Europe. Article 3 of the directive could be amended so that Member States consider the specific case of well-intentioned security researchers in their national legislation. Such minimal harmonisation could offer security researchers increased protection, particularly in cross-border situations[112].

[111] European Commission (2020), NIS2 proposal, p. 35. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN
[112] YesWeHack (2020), 'Coordinated vulnerability disclosure policy for a safer cyberspace', August. Available at: https://blog.yeswehack.com/advocacy-policy/coordinated-vulnerability-disclosure-policy-for-a-safer-cyberspace/

Furthermore, in terms of European legislation, **the protection of security researchers could also be achieved by recognising the status of the whistleblower** (in the sense of the Directive 2019/1937). This directive applies to reporting persons working in the private or public sector who acquired information through breaches of EU law in a work-related context. This directive only protects internal researchers and not external ethical hackers. It is applied to breaches of the NIS directive or the GDPR and not to all vulnerabilities on an IT system. However, a general EU approach on this could be limited by the principle of subsidiarity.

An additional action could be **for Member States to define the role of ethical hackers**. According to some consulted Member States, an aspect that should be defined before the establishment of any legal protection for the security researchers is how to distinguish/identify 'ethical hackers' from 'black hats' (i.e. researchers aiming at finding vulnerabilities for an illicit use or bad intentions). In this context, a law could be drafted defining the criteria according to which a researcher could be considered a professional ethical hacker (education/publications/experiences, etc.). For instance, the NIS directive transposition in the Hungarian information security law defines who could be responsible for information security, as well as what education a security professional must have. This definition might be a useful example of possible criteria that can be envisaged for establishing a shared definition of ethical hackers.

Moreover, there is the need **to align the EU approach to coordinated vulnerability disclosure** with the existing EU regimes and regulations such as the intellectual property regime and the GDPR, thus ensuring the protection of intellectual property rights or the protection of data of stakeholders involved in vulnerability management processes. Nevertheless, it is recommended to also be mindful about the limitations and blind spots of the existing frameworks.

Finally, the development of CVD policies could also play an important role in the implementation of various regulations such as the NIS2 directive and the GDPR. As mentioned previously, the NIS2 directive proposal mentions in Article 6 the need for Member States to design cybersecurity strategies that promote the development of CVD policies. Many Members States mentioned during the interviews the catalyst role that the transposition of the NIS2 directive could have for the development of CVD policies in the EU and in particular for the impetus that could provide for amending the national criminal law, offering legal certainty to security researchers involved in the discovery of vulnerabilities. Furthermore, according to CEPS (2018), since the GDPR entails that software owners, vendors and tech firms become data controllers insofar as they process personal data within their systems, if it is assumed that that irresponsible handling of vulnerabilities could lead to personal data breaches falling within the scope of GDPR, CVD can be an effective tool to mitigate relevant risks.

To be more precise, 'When an unpatched vulnerability leads to the breach of personal data under Article 33 of the GDPR, a data controller may be subject to administrative fines and potentially other sanctions. In assessing the level of the fines, the authorities will take into account a number of factors as stipulated in Article 83(2), including the measures taken by controllers to avoid personal data breaches (e.g. how carefully the vulnerability was handled). Therefore, if a controller implements a CVD allowing vulnerabilities to be dealt with in a timely manner, then it may reduce the risk of incurring fines arising from possible personal data breaches' ([113]).

4.2 RECOMMENDATIONS ON ECONOMIC CHALLENGES

During the interviews, several Member States suggested that limited market incentives for security researchers to participate in coordinated vulnerability disclosure programmes have a

[113] Pupillo, L., Ferreira, A. and Varisco, G. (2018) 'Software Vulnerability Disclosure in Europe: Technology, policies and legal challenges – Report of a CEPS Task Force', CEPS Task Force Reports, 28 June 2018, p.55

strong impact on the establishment of a CVD policy in the EU. Therefore, **appropriate initiatives aimed at encouraging security researchers to actively participate in CVD programmes need to be promoted by Member States, but also at the EU level** – such as the European Commission's free and open source software auditing (FOSSA) project[114].

In this context, a specific role could be played by **bug bounty programmes.** Bug bounty programmes are **crowdsourcing initiatives** that reward security researchers for finding and reporting vulnerabilities and represent a more proactive approach to vulnerability discovery by companies. They **operate as a marketplace intermediary** between vulnerability owners and researchers[115]. Bug bounty programmes can either be public or private. **Public programmes** are open to everyone but may nevertheless ban some researchers from taking part based on their track records. Private programmes are invite-only programmes for selected highly skilled security researchers.

Many companies have created their own programmes: Microsoft, Mozilla, Kaspersky Lab and Google run their own bug bounty programmes. In other cases, these programmes are managed by other companies that use their own platforms and teams of experts, connecting organisations to a global crowd of trusted security researchers to identify vulnerabilities. This is the case for companies such as Bug Crowd, Hacker One or YesWeHack in Europe[116].

Bug bounty programmes have been discussed during the interviews. Some stakeholders have engaged in reflections on whether it would make sense for the EU to have its own bug bounty programme in place. The general feeling is that **the EU should not set up a bug bounty programme**. The risk is to face individual governments' reluctance and requests for justifications of such initiative, potentially seen as excessively intrusive. Interviewees have expressed scepticism regarding the entity owning and managing the programme, and the availability of financial resources to cover for the bounties. Indeed, organisations often underestimate the cost of launching a bug bounty programme. In addition, some industries and companies are currently not in favour of bug bounty programmes, as data treated in their activities may be too sensitive to be handled by external parties, or there is too great a risk of trade secrets being stolen. These are seen as significant obstacles to the creation of an EU bug bounty programme. In conclusion, bug bounty programmes work well in some circumstances, for example, for large companies who have an interest in outsourcing a part of their security (often because external researchers are less costly than internal employees). Nevertheless, at this stage **the EU should harmonise regulation and practices across the EU Member States on bug bounty programmes** rather than attempting to set up one of their own.

However, incentives to promote CVD policies could also take the form of support to research programmes to foster CVD policies among public and private researchers in Europe. like the Framework Programme for Research and Technology Development and in particular the figital Europe programme and Horizon Europe. Furthermore, the European Cybersecurity Competence Centre could also finance projects focused on enhancing coordinated vulnerability disclosure practices in Europe.

Furthermore, since many Member States (13) regard the insufficient resources and skills to implement coordinated vulnerability disclosure policy as being particularly impactful**, it is**

[114] European Commission (2021), EU-FOSSA2. Available at: https://ec.europa.eu/info/departments/informatics/eu-fossa-2_en
[115] OECD (2021), 'Encouraging Vulnerability Treatement – Overview for policy makers', OECD Digital Economy Papers, No 307, OECD Publishing, Paris, France, February. Available at: https://www.oecd.org/sti/encouraging-vulnerability-treatment-0e2615ba-en.htm
[116] CEPS (2018) Software Vulnerability Disclosure in Europe – Technology, Policies and Legal Challenges. Report of a CEPS Task Force, June. Available at: https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges/

necessary that the EU makes available appropriate funding and programmes to train people and make viable the development of CVD policies in the EU.

When it comes to addressing the lack of coordination between vulnerability owners and researchers, the **role of a trusted third party as a coordinator to facilitate coordination becomes particularly relevant**. This role could be played by CERTs or CSIRTs or other entities able to facilitate the coordination process. This role could be very helpful in facilitating the relationship between researchers and vulnerability owners and in managing complex multi-party disclosure when the CVD involves more than two actors[117]. Furthermore, the coordination role could be very effective in facilitating relationships among stakeholders across borders. According to some experts, to approach cross border coordination an international not-for-profit and well-resourced entity should be created[118].

4.3 RECOMMENDATIONS ON POLITICAL CHALLENGES

This Section provides possible guidance on how to approach the political challenges related to the development of the vulnerability disclosure process, and the roles and dynamics among the different stakeholders will be assessed.

Top down or bottom-up approach?

One of the issues raised during the analysis of the status of play of the EU experience on CVD policies and the interview with Member States is the different dynamics followed in developing CVD policies, namely a bottom-up v a top-down approach. The development of decentralised or centralised approaches has both pros and cons. For instance, countries such as France, the United States and China, follow a top-down approach where researchers need to report vulnerabilities through a government agency. As mentioned in some interviews with the research community or private sector, researchers may be reluctant to share information with government agencies in the first place. Furthermore, countries like the Netherlands consider having followed a bottom-up approach as the most important success factor for their CVD policy. However, while national policies reflect the different views towards vulnerability disclosure policies, it is **likely that a top-down approach in which the EU suggests a common model of coordinated vulnerability disclosure at the EU level could work better and promote coordination at the EU and international levels.**

The role of government

Governments can play a key role in the development of CVD policies. According to the Member States, governments should promote the following actions.

- Updating cybercrime and intellectual property frameworks to better protect security researchers, for example through ‘safe harbours’.
- Leading by example in the establishment of a CVD policy:
    - adapting CVD within the government;
    - adapting vulnerability handling and management within the government;
    - including vulnerability management and handling and CVD in regulation, standards and guidance, or using them as indicators of compliance.

Governments should lead by example, especially in economies where there are numerous vendors, a great variety in the willingness of the vulnerability owner to accept and handle the vulnerability report and in the value attributed to secure products. In this context, first convincing

[117] FIRST (2017), ‘Guidelines and practices for multi-party vulnerability coordination and disclosure’. Available at: https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.0
[118] OECD (2021), ‘Encouraging Vulnerability Treatement – Overview for policy makers’, OECD Digital Economy Papers, No 307, OECD Publishing, Paris, France, February, p. 25. Available at: https://www.oecd.org/sti/encouraging-vulnerability-treatment-0e2615ba-en.htm

public entities to adopt CVD and reassuring them that the reports will be handled is considered as important.

Furthermore, governments should also promote national non-legislative activities such as supporting and enabling CVD practices and/or promoting awareness-raising campaigns.

Finally, governments could promote cooperation across borders and standards by facilitating the exchange of information on vulnerabilities across borders between vulnerability owners and security researchers, and encouraging all stakeholders to take part in the development and enhancement of international standards on CVD policies[119].

The role of the private sector

According to some Member States, companies should not wait for a government legislative/policy intervention, especially because establishing a CVD policy at the company level is already possible within some of the existing national legal frameworks. Therefore, the private sector could take the lead in implementing coordinated vulnerability disclosure by defining and publishing on the companies' website public reporting mechanisms on vulnerabilities disclosure according to standards and best practices, such as the ISO/IEC 29147:2018[120] or the European Telecommunications Standards Institute's guide to coordinated vulnerability disclosure[121].

The private sector could also take the lead in putting in place **bug bounty programmes** as they help in fighting the vulnerability taboo.

Besides, according to a consulted Member State, in many cases, researchers have found that the private sector is more appropriately positioned for dealing with vulnerability disclosure than state sector entities.

4.4 RECOMMENDATIONS ON CHALLENGES FROM OPERATIONAL AND CRISIS MANAGEMENT ACTIVITIES

Some challenges in terms of operational and crisis management activities have also been underlined by the Member States. These challenges could be better managed with stronger **private-public partnerships (PPPs) and better information sharing** among companies and between companies and public authorities. PPPs are very helpful to start building trust among stakeholders and, with their flexibility in terms of spectrum of mandate and type of participants, can be very effective for sharing information on vulnerabilities. The presence of public authorithies in the PPS can further encourage information sharing of vulnerabilities and actionable intelligence.

4.5 THE ROLE OF ENISA AND OF THE EUROPEAN COMMISSION

Consulted Member States have proposed several actions that ENISA and the Commission can adopt to facilitate and support the establishment of CVD policies. Specific measures that would ease the adoption of CVD in EU include the following.

According to several Member States (8), providing clear guidance to countries on how to establish a CVD policy, publishing countries' best practices and challenges, and publishing templates upon which countries can draft their policies. Publishing best practices would be very

[119] OECD (2021), 'Encouraging Vulnerability Treatement – Overview for policy makers', OECD Digital Economy Papers, No 307, OECD Publishing, Paris, France, February'. Available at: https://www.oecd.org/sti/encouraging-vulnerability-treatment-0e2615ba-en.htm
[120] ISO (2014), 'ISO/IEC 29147:2014 Information Technology – Security techniques – Vulnerability disclosure'. Available at: https://www.iso.org/standard/45170.html
[121] ETSI (2022), 'Cyber Security; Guide to Coordinated Vulnerability Disclosure', ETSI Technical Reports, January. Available at: https://www.etsi.org/newsroom/press-releases/2029-2022-02-etsi-releases-report-on-coordinated-vulnerability-disclosure

useful especially for countries that are still in the process of implementing a policy, to understand the challenges that other countries have faced, and for countries where the government is opposing the establishment of a CVD policy, to understand different approaches that can be followed. The CSIRT Network has been suggested by few countries as a very useful forum to share best practices.

Promoting awareness-raising campaigns on CVD at the EU level to persuade vendors across the EU to work on preparing the required interface to be able to handle the researchers' report.

Foster cooperation and trust. Identifying and supporting initiatives meant to increase trust between public and private stakeholders are fundamental to improving the vulnerability management process. Establishing safe and reliable communication channels, for example, could allow more information concerning vulnerabilities to be shared between parties. Publishing a webpage where all the regulations in place in the different countries are collected (a repository of Member States' CVD initiatives) allows researchers to be more informed on the level of protection they can receive in the different countries.

Harmonising the CVD initiatives in the different countries and promoting the use of international standards, such as the MITRE standard for publishing vulnerabilities. Currently, each Member State will have to establish a CVD policy upon a different national framework. Once every country has a CVD policy in place, EU institutions can work on the harmonisation of the different frameworks.

Encourage the establishment of bug bounty programmes at the EU level for open software or core modules of critical infrastructures. Notably, in 2017 the EU had already established a bug bounty programme to 15 open source software used by the European institutions, giving awards of up to 25 000 EUR. The programme was a component of the EU-founded EU-FOSSA2[122] project. The EU could built on this experience and encourage the establishment of bug bounty programmes at the EU level.

Addressing Member States' resource constraints that hamper the implementation of CVD policies by fostering an ecosystem where it is economically rewarding to make secure IT systems. This can be achieved, for example, by implementing a regulation to establish mandatory ICT security, which could create a business case for companies to revive the ICT market.

Including procurement rules for ICT products. Procurement policies at the EU level could be a great market driver for vendors to produce more secure products.

Establish an easy-to-use interface for entities to report vulnerabilities, similar to **the CERT/CC** web-based platform VINCE. This will encourage and enable fast vulnerability reporting and remove potential delays from the chain of reporting.

Suggesting or mandating to Member States to define a clear separation between what should be considered a breach of criminal law and what should not before the transposition of

[122] European Commission (2021), EU-FOSSA2. Available at: https://joinup.ec.europa.eu/collection/eu-fossa-2

the NIS2. This is particularly pivotal for countries where the criminal code is more difficult to change[123].

Establishing a CVD policy at the EU level. The CERT EU or other EU bodies/agencies could undertake the role of CVD coordinator, easing the communications between researchers and companies involved without them having to engage with multiple national CERTs. Establishing a CVD policy at the EU level could also help to address some fundamental questions about liability implications (e.g. on the gathering of personal data or infringement of copyright rules).

Initiating and promoting a broader dialogue on vulnerability handling and management at the EU level, not just on CVD. The NIS Cooperation Group could more significantly foster the conversation on these topics. Indeed, it is not apparent that such discussions have taken place between the Member States.

[123] Italy is proposing an amendment to the NIS2 directive text, aiming at facilitating the definition of this separation. Italy is proposing to add the following statements to Article 6 (1.a) NIS2: 'Member States may provide for specific requirements to make the Coordinated Vulnerability Disclosure mechanism consistent and compliant with their national legal frameworks. In particular, they may define the conditions according to which the identification and disclosure of vulnerabilities would not entail a breach of Criminal Law.'

5. REFERENCES

Act on the Electronic Information Security of Central and Local Government Agencies (Act L of 2013/Information Security Act) (2013). Available at: https://nki.gov.hu/wp-content/uploads/2020/11/Cyber-Security-Act_2013_50.pdf

Anderson, R and Moore, T (2006), *Information Security Economics – and Beyond*. Available at: https://www.researchgate.net/publication/221355448_Information_Security_Economics_-_and_Beyond

Anderson, R. (2001), 'Why information Security is Hard – An Economic Perspective', paper prepared for 17th Annual Computer Security Applications Conference (ACSAC01), EEE Computer Society, December. Available at: https://www.researchgate.net/publication/3941712_Why_Information_Security_is_Hard-An_Economic_Perspective

Authors' translation in English from the original text, Ministry of Research, Innovation and Digital Politics (2020), *Government Security Strategy of the Republic of Cyprus Cybersecurity Strategy of the Republic of Cyprus 2020* (ΥΦΥΠΟΥΡΓΕΙΟ ΕΡΕΥΝΑΣ, ΚΑΙΝΟΤΟΜΙΑΣ ΚΑΙ ΨΗΦΙΑΚΗΣ ΠΟΛΙΤΙΚΗΣ ΑΡΧΗ ΨΗΦΙΑΚΗΣ ΑΣΦΑΛΕΙΑΣ έγγραφο Πολιτικής Στρατηγική Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας 2020).

Balaji, N. (2021), 'Zero-day bugs must be reported to government within 2 days of discovery – New Chinese IT law', CyberSecurityNews. Available at: https://cybersecuritynews.com/all-the-zero-day-bugs-must-be-reported-to-government/

Bannister, A. (2020), 'German armed forces launch security vulnerability disclosure program', The Daily Swig, 27 October. Available at: https://portswigger.net/daily-swig/german-armed-forces-launch-security-vulnerability-disclosure-programv

Borealis (2021), 'Responsible disclosure policy'. Available at: https://www.borealisgroup.com/legal/responsible-disclosure

Bundeswehr (2021), 'Vulnerability disclosure policy der Bundeswehr (VDPBw)'. Available at: https://www.bundeswehr.de/de/security-policy

Centre for Cyber Security Belgium, 'CCB coordinated vulnerability disclosure policy'. Available at: https://ccb.belgium.be/en/vulnerability-policy

Centre for Cyber Security Belgium, 'Coordinated vulnerability disclosure policy and vulnerability detection reward program (bug bounty)'. Available at: https://ccb.belgium.be/fr/politique-de-divulgation-coordonnée-de-vulnérabilités-et-programme-de-récompense-pour-la-découverte

CERT.LV, 'Responsible disclosure policy'. Available at: https://cert.lv/en/about-us/responsible-disclosure-policy

CERT-FR, 'InterCERT-FR definition'. Available at: https://www.cert.ssi.gouv.fr/csirt/intercert-fr/

Christey, S. (2002), Memo 'Responsible vulnerability disclosure process', Internet Engineering Task Force, February. Available at: https://datatracker.ietf.org/doc/html/draft-christey-wysopal-vuln-disclosure-00

Cinpanu, C. (2021), 'Chinese government lays out new vulnerability disclosure rules', The Record. Available at: https://therecord.media/chinese-government-lays-out-new-vulnerability-disclosure-rules/

CISCO (2021), 'Security vulnerability policy'. Available at: https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html

CVE MITRE, 'Request CVE IDs'. Available at: https://cve.mitre.org/cve/request_id.html

Cyber Security and Infrastructure Agency (2015), Black Box Security Testing Tools. Available at: https://us-cert.cisa.gov/bsi/articles/tools/black-box-testing/black-box-security-testing-tools

Cybil, 'Coordinated vulnerability disclosure (GFCE initiative)'. Available at: https://cybilportal.org/projects/coordinated-vulnerability-disclosure-gfce-initiative/

Dodd, J. C., Li, J. J., Luo, D. and Campbell, R. (2017), 'People's Republic of China Cybersecurity Law: A preliminary overview for western companies', *The National Law Review*, Vol. 7, No 199, Hunton Andrews Kurth, Richmond VA, United States. Available at: https://www.natlawreview.com/article/people-s-republic-china-cybersecurity-law-preliminary-overview-western-companies

ENISA (2015), *Good Practice Guide on Vulnerability Disclosure – From challenges to recommendations*. Available at: https://www.enisa.europa.eu/publications/vulnerability-disclosure

ENISA (2016), *ENISA Threat Landscape Report 2016 – 15 top cyber-threats and trends*. Available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

ENISA (2021), *PSIRT Expertise and Capabilities Development – Health and energy PSIRT study and recommendations*, June. Available at: https://www.enisa.europa.eu/publications/csirt-expertise-and-capabilities-development

ENISA, 'National cyber security strategies' (interactive map). Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Romania

European Commission (2019), Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) PE/86/2018/REV/1, Brussels, 7.6.2019. Available at: https://eur-lex.europa.eu/eli/reg/2019/881/oj

European Commission (2020), NIS2 proposal, p. 35. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN

European Commission (2021), EU-FOSSA2. Available at: https://joinup.ec.europa.eu/collection/eu-fossa-2

Federal Office for Information Security (2012), Recommendation: IT-producers – Vulnerability Handling – Recommendations for software vendors, October. Available at: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_019E.pdf?__blob=publicationFile&v=1

Federal Trade Commission (2015), *Start With Security – A guide for business*, June. Available at: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

FIRST (2017), 'Guidelines and practices for multi-party vulnerability coordination and disclosure'. Available at: https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.0

Falot, N. (2013), *Criminal Liability for Ethical Hackers in the EU*, Considerati. Available at: https://cert.lv/uploads/pasakumi/Nathalie_Falot.pdf

Fisher, D. (2009), 'No more free bugs for software vendors', Threat Post, March. Available at: https://threatpost.com/no-more-free-bugs-software-vendors-032309/72484/

GFCE (Global Forum on Cyber Expertise) (2017), '*GFCE Global Good Practices – Coordinated Vulnerability Disclosure (CVD)*'. Available at: https://thegfce.org/wp-content/uploads/2020/06/CoordinatedVulnerabilityDisclosure-1.pdf

Global Cyber Security Capacity Center (GCSCC) (2017), *Cybersecurity Capacity Review – Republic of Lithuania*, August. Available at: https://www.nrdcs.lt/file/repository/resources/Lithuania_Report_10_8_2017_FINAL.pdf

GFCE, 'Coordinated vulnerability disclosure'. Available at: https://thegfce.org/initiatives/coordinated-vulnerability-disclosure/

Gobierno de España Ministerio de la Presidencia, Relaciones con las cortes y memoria democrática, (2010), Royal Decree 3/2010, of 8 January, regulating the National Security Framework in the area of e-Government, Agencia Estatal Boletín Oficial del Estado. Available at: https://www.boe.es/eli/es/rd/2010/01/08/3/con

Gobierno de España Ministerio de la Presidencia, Relaciones con las cortes y memoria democrática, (2018), Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, Agencia Estatal Boletín Oficial del Estado. Available at: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-12257

Goldstein, E. (2021), 'CISA announces new vulnerability disclosure policy (VDP) platform'. Available at: https://www.cisa.gov/blog/2021/07/29/cisa-announces-new-vulnerability-disclosure-policy-vdp-platform

GOVCERT.LU (2019), Responsible Disclosure Policy (Public) – Version 1.0 – 2019-12-02 (Final), December. Available at: http://www.govcert.lu/docs/POL226_Responsible_Disclosure_Policy_(Public)_1.0.pdf

GOVCERT.LU (2020), 'Hall of Fame'. Available at: http://www.govcert.lu/en/hall_of_fame/

Government of Ireland (2019), *National Cyber Security Strategy*, December. Available at: https://www.gov.ie/en/publication/8994a-national-cyber-security-strategy/

Government of Luxembourg (2015), *National Cybersecurity Strategy II – Approved and made enforceable by the Government Council on 27.03.2015*. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf

Government of Luxembourg (2019), *National Cybersecurity Strategy III – Approved and made enforceable by the Government Council on 26.01.2018*. Available at: https://hcpn.gouvernement.lu/dam-assets/fr/publications/brochure-livre/national-cybersecurity-strategy-3/national-cybersecurity-strategy-iii-en-.pdf

Government Offices of Sweden Ministry of Justice (2017), *A national cyber security strategy – Skr. 2016/17:213*. Available at: https://www.government.se/4ada5d/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213

Householder, A. D. (2019), *The CERT Guide to Coordinated Vulnerability Disclosure*, CERT, December. Available at: https://vuls.cert.org/confluence/display/CVD

INCIBE-CERT, 'Vulnerability disclosure policy'. Available at: https://www.incibe-cert.es/en/what-is-incibe-cert/vulnerability-disclosure-policy

ISO (2014), 'ISO/IEC 29147:2014 Information Technology – Security techniques – Vulnerability disclosure'. Available at: https://www.iso.org/standard/45170.html

JVN iPedia website. Available at: https://jvndb.jvn.jp/en/

Latvian Defence Ministry (2019), Informative report 'Latvian cyber security strategy for 2019–2022', (Informatīvais ziņojums'Latvijas kiberdrošības stratēģija 2019.–2022. gadam'). Available at: https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf

Law of 5 July 2018 on the National Cybersecurity System (2018), *Journal of Laws 2018* item 1560 (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa). Available at: http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/T/D20181560L.pdf

Ministry for Competitiveness and Digital Maritime and Services Economy (2016), *Malta Cyber Security Strategy 2016*. Available at: https://mita.gov.mt/wp-content/uploads/2020/07/Mita-_Malta-Cyber-Security-Strategy-Book.pdf

National Assembly of the Republic of Slovenia (2018), The Law on Information Security (Z A K O N O INFORMACIJSKI VARNOSTI (ZInfV), April. Available at: https://ccdcoe.org/uploads/2018/10/Slovenia_Information-Security-Act-2018_original.pdf

National Cyber Security Authority (2018), *National Cyber Security Strategy – Version 3.0*. Available at: https://ccdcoe.org/uploads/2018/10/Greece_National-Cyber-Security-Strategy-ver.3.0_EN.pdf

National Cyber Security Centrum, 'Report vulnerability (CVD)'. Available at: https://www.ncsc.nl/contact/kwetsbaarheid-melden

National Telecommunciations and Information Administration, 'Software bill of materials'. Available at: https://www.ntia.gov/SBOM

NCSC NL scoring matrix details. Available at: https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2019/juli/02/inschalingsmatrix/Inschalingsmatrix.pdf

NIST (2017), Framework for Improving Critical Infrastructure Cybersecurity – Version 1.1 (Draft 2), December. Available at: https://csrc.nist.gov/publications/detail/white-paper/2017/12/05/cybersecurity-framework-v11/draft

Nomad Mobile Research Centre (1999), Announcement Simple Nomad, September. Available at: https://www.nmrc.org/pub/advise/policy.txt

OASIS (2017), CSAF Common Vulnerability Reporting Framework (CVRF) Version 1.2. Available at: http://docs.oasis-open.org/csaf/csaf-cvrf/v1.2/csaf-cvrf-v1.2.html

OECD (2019), 'Roles and Responsibilities of Actors for Digital Security', *OECD Digital Economy Papers*, No 286, OECD Publishing, Paris, France. Available at: https://www.oecd-ilibrary.org/science-and-technology/roles-and-responsibilities-of-actors-for-digital-security_3206c421-en

OECD (2021), Encouraging Vulnerability Treatment – Overview for policy makers, *OECD Digital Economy Papers*, No 307, OECD Publishing, Paris, France, February, p. 13. Available at: https://www.oecd.org/sti/encouraging-vulnerability-treatment-0e2615ba-en.htm

Office of the Central Cyberspace Affairs Commission (2021), 'Notice of the Minitry of Industry and Information Technology and the State Internet Information Office of the Ministry of Public Security on issuing the regulations on the management of network product security Vulnerabilities'. Available at: http://www.cac.gov.cn/2021-07/13/c_1627761607640342.htm

O'Neill, P. H. (2017), 'China hides homegrown hacks from its vulnerability disclosure process', Cyberscoop. Available at: https://www.cyberscoop.com/china-vulnerability-disclosure-mss-recorded-future/

Open Bug Bounty (2021), Available at: https://www.openbugbounty.org/bugbounty/PaulMar23292621/

Portuguese National Cybersecurity Centre (CNCS) (2020), National Cybersecurity Framework Version 1.0 EN, April. Available at: https://www.cncs.gov.pt/content/files/qnrcs_web_eng.pdf

Pupillo, L., Ferreira, A. and Varisco, G. (2018), 'Software Vulnerability Disclosure in Europe: Technology, policies and legal challenges – Report of a CEPS Task Force', *CEPS Task Force Reports*, 28 June 2018. Available at: https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges/

Republic of Bulgaria Council of Ministers (2016), *National Cyber Security Strategy 'Cyber Sustainable Bulgaria 2020'* (Национална стратегия за киберсигурност 'Киберустойчива България 2020'). Available at: https://www.strategy.bg/StrategicDocuments/View.aspx?lang=bg-BG&Id=1120

Republic of Croatia Ministers of Interior (2015), 'The National Cyber Security Strategy of the Republic of Croatia', *Official Gazette*, No 108/2015. Available at: https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf

Republic of Estonia Information System Authority (2018), 'Estonia offers recommendations in the light of eID vulnerability', May. Available at: https://www.ria.ee/en/news/estonia-offers-recommendations-light-eid-vulnerability.html

Republic of Estonia Ministry of Economic Affairs and Communications (2019), *2019–2022 Cybersecurity Strategy – Republic of Estonia*. Available at: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Republic of Slovenia (2016), *Digital Slovenia 2020 – Development strategy for the information society until 2020*, March. Available at: https://www.gov.si/assets/ministrstva/MJU/DID/Digital-Slovenia-2020-Development-Strategy-for-the-Information-Society-until-2020.pdf

Simpson, A. (2015), 'Enhancing the digital economy through collaboration on vulnerability research disclosure', National Telecommunications and Information Administration, July. Available at: https://www.ntia.doc.gov/blog/2015/enhancing-digital-economy-through-collaboration-vulnerability-research-disclosure

SK-CERT National Cyber Security Centre (2019), Vulnerability Reporting Guideline, September. Available at: https://www.sk-cert.sk/wp-content/uploads/2019/10/Vulnerability_reporting.pdf

The Criminal Code of 6 June 1997 (*Journal of Laws 1997* transl. gb No 88, item 553) (The Criminal Code z dnia 6 czerwca 1997 r. (Dz.U. tłum. gb Nr 88, poz. 553)). Available at: https://supertrans2014.files.wordpress.com/2014/06/the-criminal-code.pdf

The Danish Government Ministry of Finance (2018), *Danish Cyber and Information Security Strategy*, May. Available at: https://digst.dk/media/16943/danish_cyber_and_information_security_strategy_pdfa.pdf

The Network Law on Security of Networks and Information Systems of 2018 Third Annex (Part II) of the *Official Journal of the European Union* (2019), June 7th. Available at: https://dsa.cy/wp-content/uploads/Decision-218-2019.pdf

Townsend, K. (2021), 'New law will help Chinese government stockpile zero-days', Security Week. Available at: https://www.securityweek.com/new-law-will-help-chinese-government-stockpile-zero-days

Udemans, C. (2019), 'China working on rules to regulate vulnerability disclosures', TechNode. Available at: https://technode.com/2019/11/22/china-vulnerability-disclosures-risks/

United States Copyright Office (2015), Section 1201 Rulemaking: Sixth triennial proceeding to determine exemptions to the prohibition on circumvention, October. Available at: https://www.copyright.gov/1201/2015/introduction-analysis.pdf

United States Department of Defence (2016), 'DOD announces digital vulnerability disclosure policy and "Hack the Army" kick-off', November. Available at: https://www.defense.gov/Newsroom/Releases/Release/Article/1009956/

United States of America Federal Trade Commission (2013), DOCKET NO. C-4406 In the Matter of HTC AMERICA Inc., a corporation, June. Available at: https://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htccmpt.pdf

Washington University in St. Louis, School of Law (2014), 'What is the difference between common law and civil law?', 28 January. Available at: https://onlinelaw.wustl.edu/blog/common-law-vs-civil-law/#:~:text=The20main20difference20between20the,law20systems2C20codified20statutes20predominate

Webcheck, 'Responsible Disclosure'. Available at: https://webcheck.pt/en/responsible-disclosure/

YesWeHack (2020), 'Coordinated vulnerability disclosure policy for a safer cyberspace', August. Available at: https://blog.yeswehack.com/advocacy-policy/coordinated-vulnerability-disclosure-policy-for-a-safer-cyberspace/

6. BIBLIOGRAPHY

Ablon, L. and Bogart, A. (2017), *Zero Days, Thousands of Nights – The life and times of zero-Day Vulnerabilities and Their Exploits*, Rand Corporation, Santa Monica, CA. Available at: https://www.rand.org/pubs/research_reports/RR1751.html

Anderson, R. (2017), 'Disclosing vulnerabilities and breaches in the internet of things', Presentation at the first meeting of the CEPS Task Force on SW Vulnerability Disclosure in Europe, Brussels, September. Available at: https://www.ceps.eu/sites/default/files/Ross20Anderson2C20Cambridge.pdf

Australian Government Department of Health (2021), 'Vulnerability disclosure policy', February. Available at: https://www.health.gov.au/using-our-websites/vulnerability-disclosure-policy

Bada, M. and Weisser Harris, C. (2017), *Cybersecurity Capacity Review Republic of Lithuania*, August Available at: https://www.nrdcs.lt/file/repository/resources/Lithuania_Report_10_8_2017_FINAL.pdf

Biggs, J. (2017), 'Hungarian hacker arrested for pressing F12', Techcrunch, July. Available at: https://techcrunch.com/2017/07/25/hungarian-hacker-arrested-for-pressing-f12/

Ellis, J. (2015), 'New DMCA exemption is a positive step for security researchers', Rapid1, October. Available at: https://blog.rapid7.com/2015/10/28/new-dmca-exemption-is-a-positive-step-for-security-researchers/

European Commission (2017), Joint Communication from the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy on 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU', September.

European Commission (2020), Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, December.

Goodin, D. (2012), 'Rise of "forever day" bugs in industrial systems threatens critical infrastructure – When Microsoft, Adobe, and Apple learn of critical flaws in their products …', Ars Technica, April, Available at: https://arstechnica.com/information-technology/2012/04/rise-of-ics-forever-day-vulnerabiliities-threaten-critical-infrastructure/

Herr, T. and Schneier, B. (2017), 'What You See Is What You Get: Revisions to our paper on estimating vulnerability rediscovery', Lawfare. Available at: https://www.lawfareblog.com/what-you-see-what-you-get-revisions-our-paper-estimating-vulnerability-rediscovery

Herr T., Schneier, B. and Morris, C. (2017), Working paper 'Taking Stock: Estimating vulnerability rediscovery', Cyber Security Project, Belfer Center, Harvard Kennedy School, Cambridge, MA, July. Available at: https://www.belfercenter.org/node/96161

IOT Security Foundation (2020), *Consumer IoT: Understanding the contemporary use of vulnerability disclosure – 2020 progress report*. Available at: https://www.iotsecurityfoundation.org/wp-content/uploads/2020/03/IoTSF-2020-Progress-Report-Consumer-IoT-and-Vulnerability-Disclosure.pdf

ISO (2018), 'ISO/IEC 29147:2018 Information Technology – Security techniques – Vulnerability disclosure'. Available at: https://www.iso.org/standard/72311.html

ISO (2019), 'ISO/IEC 30111:2019 Information Technology – Security techniques – Vulnerability handling processes'. Available at: https://www.iso.org/standard/69725.html

Khanji, A. (2019), 'New Vulnerability Disclosure Policy Requirement: Australian government releases draft code of practice for IoT security', Gridware, November. Available at: https://www.gridware.com.au/new-vulnerability-disclosure-policy-requirement-australian-government-releases-draft-code-of-practice-for-iot-security/

Leverett, E., Clayton R. and Anderson R. (2017), 'Standardization and Certification of the "Internet of Things"', May. Available at: http://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/05/WEIS_2017_paper_23.pdf

Mayer, J. (2016), 'The "Narrow" Interpretation of the Computer Fraud and Abuse Act: A user guide for applying United States v. Nosal', *The George Washington Law Review*, Vol. 84:1644, No 6, December. Available at: http://www.gwlr.org/wp-content/uploads/2016/11/84-Geo.-Wash.-L.-Rev.-1644.pdf

NIST (2018), *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (2nd Draft), December. Available at: https://csrc.nist.gov/publications/detail/white-paper/2018/04/16/cybersecurity-framework-v11/final

NTIA Multistakeholder Process on Software Component Transparency Framing Working Group (2021), Software Identification Challenges and Guidance. Available at: https://www.ntia.gov/files/ntia/publications/ntia_sbom_software_identity-2021mar30.pdf

NTIA Safety Working Group (2016), 'Early Stage' Coordinated Vulnerability Disclosure Template, December. Available at: https://www.ntia.doc.gov/files/ntia/publications/ntia_vuln_disclosure_early_stage_template.pdf

Posey, B. (2020), 'Definition of "zero-day (computer)"', TechTarget, August. Available at: https://searchsecurity.techtarget.com/definition/zero-day-vulnerability

RFPolicy, 'Full Disclosure Policy, v2.0'. Available at: https://docu.ilias.de/goto_docu_wiki_1357_RFPolicy.html#ilPageTocA214

Sanchez, I. and Beslay, L. (2017), 'EU zero-day vulnerability management', presentation at the CEPS Workshop on SW Vulnerability Disclosure: The European Landscape, Brussels, June. Available at: https://www.ceps.eu/sites/default/files/JRC_presentation_ceps_final2028Sanchez29

Spring, J. M., Hatleback, E., Householder, A., Manion, A. and Shick, D. (2019), Prioritizing Vulnerability Response: A stakeholder-specific vulnerability categorization, Software Engineering Institute,

Carnegie-Mellon University, Pittsburgh, PA, United States. Available at: https://resources.sei.cmu.edu/asset_files/WhitePaper/2019_019_001_636391.pdf

U.S. Department of Justice Cybersecurity Unit Computer Crime & Intellectual Property Section Criminal Division (2017), A framework for a vulnerability disclosure program for online systems, July. Available at: https://www.justice.gov/criminal-ccips/page/file/983996/download

U.S. Food and Drugs Administration (2016), Guidance document 'Postmarket Management of Cybersecurity in Medical Devices – Guidance for industry and food and drug administration staff', December. Available at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices

Udemans, C. (2019), 'China working on rules to regulate vulnerability disclosures', TechNode, November. Available at: https://technode.com/2019/11/22/china-vulnerability-disclosures-risks/

Weise, E. (2017), 'Hackers at DefCon conference exploit vulnerabilities in voting machines', USA Today Tech. Available at: https://eu.usatoday.com/story/tech/2017/07/30/hackers-defcon-conference-exploit-vulnerabilities-voting-machines/523639001/

TP-05-22-071-EN-C

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the agency works together with its key stakeholders to strengthen trust in the connected economy, to boost the resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: https://www.enisa.europa.eu/

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-574-6
doi:10.2824/42129