Software Vulnerability Disclosure in Europe

Technology, Policies and Legal Challenges

Report of a CEPS Task Force

Chair: Marietje Schaake

Rapporteurs: Lorenzo Pupillo
Afonso Ferreira
Gianluca Varisco

CEPS

Software Vulnerability Disclosure in Europe

Software Vulnerability Disclosure in Europe

Technology, Policies and Legal Challenges

Report of a CEPS Task Force

June 2018

Chair: **Marietje Schaake**

Rapporteurs: **Lorenzo Pupillo**
Afonso Ferreira
Gianluca Varisco

Centre for European Policy Studies (CEPS)
Brussels

CEPS is an independent think tank based in Brussels, whose mission is to produce sound analytical research leading to constructive solutions to the challenges facing Europe today. The views presented in this report do not necessarily represent the opinions of all the participants of the Task Force, nor do they explicitly represent the view of any individual participant (unless explicitly mentioned in this report).

The views expressed in this report are those of the authors writing in a personal capacity and do not necessarily reflect those of CEPS or any other institution with which they are associated.

ISBN 978-94-6138-687-8

CEPS
Place du Congrès 1, B-1000 Brussels
Tel: 32 (0) 2 229.39.11
e-mail: info@ceps.eu
internet: www.ceps.eu

Table of Contents

List of Figures and Tables

LIST OF ABBREVIATIONS

ANSSI	Agence nationale de la sécurité des systèmes d'information (France)
CERT	computer emergency response team
CFAA	Computer Fraud and Abuse Act (US)
CSAJ	Computer Software Association of Japan
CVD	coordinated vulnerability disclosure
DARPA	Defense Advanced Research Projects Agency (US)
DDoS attacks	Distributed Denial-of-Service attacks
DMCA	Digital Millennium Copyright Act (US)
DNS	Domain Name System
DoD	Department of Defence (US)
DoJ	Department of Justice (US)
DRM	digital rights management
ENISA	European Network and Information Security Agency (EU)
EPES	Electrical Power and Energy System
EULA	End User Licence Agreement
FDA	Food and Drug Administration (US)
FIRST	Forum of Incident Response and Security Teams
GCSCC	Global Cyber Security Capacity Center
GDDP	Government Disclosure Decision Processes
GDPR	General Data Protection Regulation (EU)
ICT	Information and communications technology
IEFT	Internet Engineering Task Force
IoT	Internet of Things
IPA	Information-technology Promotion Agency
ISO	International Standards Organisation
JEITA	Japan Electronics and Information Technology Industries Association
JISA	Japan Information Technology Service Industry Association
JNSA	Japan Network Security Association
JPCERT/CC	JPCERT Coordination Center (Japan)
JRC	Joint Research Centre (EU)

JVN	Japan Vulnerability Notes
METI	Ministry of Economy, Trade and Industry (Japan)
NCSC	Nationaal Cyber Security Centrum (NL)
NCSC-FI	National Cyber Security Centre (Finland)
NHTSA	National Highway Transportation and Safety Administration (US)
NIS	Network information systems (EU Directive on)
NTIA	National Telecommunications and Information Administration, Department of Commerce (US)
RDP	Responsible Disclosure Policy
SVD	Software vulnerability disclosure

FOREWORD

Cybersecurity is a hot topic of debate in today's policy circles. The abuse of software vulnerabilities is a growing concern that needs to be urgently addressed with better solutions, as increasing numbers of devices and people are connected to the internet every day. This CEPS Task Force report offers the first comprehensive account of the various measures EU member states are taking to counter these challenges. It also offers practical recommendations on how to improve the coordination and disclosure of software vulnerabilities by both private-sector and public actors.

Vulnerability disclosure has been the subject of a decades-long debate in the information security community. The American cryptographer Bruce Schneider said in the late 1990s that "full disclosure is a damn good idea". Today, the notion prevails that responsible disclosure should be done in a coordinated fashion, which takes into consideration that publicly releasing all vulnerability details can result in negative consequences for users. The private sector is responsible not only for developing the best possible software, but also for responsibly handling vulnerabilities whenever they are discovered.

We live in an age in which vulnerabilities are leaked by criminals, with potentially geopolitical motives, and when certain governments are stockpiling vulnerabilities to develop offensive cyber-weapons. This cannot be done in an accountability vacuum. Transparent decision-making processes are now needed in order to preserve the rule of law online and to hold government bodies accountable. Each EU member state needs to have an operational framework in place that guides their intelligence agencies in using and disclosing software vulnerabilities.

Thirteen EU member states are currently contemplating the creation of a national coordinated vulnerability disclosure policy (CVD). Two countries have already a CVD policy, and the remaining member states have no immediate plans in this area. Hopefully this report will contribute to the streamlining and rationalising of these existing efforts and encourage others to adopt their own CVD policy. Reaching agreement on a common, European approach is the key to avoiding a fragmented Digital Single Market and to preserving network and information security. To achieve that, it would be beneficial to agree on a single interpretation of what constitutes illegal access to a computer system and to develop a legal exception for security researchers in many areas of relevant EU law, including copyright law, e-evidence, cybercrime and the EU's export control regulation. Vulnerability disclosure is a horizontal policy issue, which deserves the attention of policy-makers dealing with a wide range of topics.

The CEPS Task Force on Software Vulnerabilities Disclosure has benefitted from the knowledge of experts representing EU governments, technology companies, civil society and academia. This multi-stakeholder approach reflects a recognition of the need to bring various people together and holistically assess how intended solutions are working out in practice. Our work aims to benefit Europeans by allowing them to connect without being fearful that any vulnerabilities in their devices will be abused by either companies or the very governments representing them.

Marietje Schaake, Chair of the Task Force
Member of the European Parliament
Brussels, June 2018

PREFACE

This report is based on discussions in the CEPS Task Force on Software Vulnerability Disclosure in Europe. The Task Force, chaired by Marietje Schaake, Member of the European Parliament, was composed of industry experts, representatives of EU and international institutions, academics, civil society organisations and practitioners (see a list of participants in Annex 1). The group met on four separate occasions in the period between September 2017 and February 2018.

As Coordinator of the Task Force, I would like to acknowledge the invaluable contributions of all the participants in the Task Force to this work. Particular thanks go to the members of the Advisory Board: Ross Anderson at the University of Cambridge, Andriani Ferti of Karatzas & Partners Law Firm, Allan Friedman at the US National Telecommunications and Information Administration and Tim Watson at the University of Warwick. I also wish to acknowledge the substantial work done by my fellow rapporteurs, Afonso Ferreira and Gianluca Varisco. As indicated in the text itself, other Task Force members directly contributed their expertise by personally drafting selected chapters of the report, namely Jochai Ben-Avie, Jeroen van der Ham, Baiba Kaskina and Uchiyama Takayuki. I am also grateful to members who kindly volunteered to review earlier versions of this report, especially Stefano Fantin of Katholieke Universiteit Leuven. Finally, I wish to thank Antonella Zarra for her valuable research assistance.

Lorenzo Pupillo, Rapporteur and Coordinator of the Task Force
Associate Senior Research Fellow, CEPS
Brussel, June 2018

EXECUTIVE SUMMARY

This report puts forward the analysis, policy implications and main recommendations for the design and implementation of a forward-looking policy on software vulnerability disclosure (SVD) in Europe. It is the result of a collective effort led by CEPS, which in September 2017 formed a Task Force on Software Vulnerability Disclosure in Europe, composed of industry experts, representatives of EU and international institutions, academics, civil society organisations and practitioners (see a list of participants in Annex 1). Meeting on four separate occasions in the period between September 2017 and February 2018, the group explored ways to formulate practical guidelines for governments and businesses to harmonise the process of handling SVD throughout Europe. These discussions led to policy recommendations addressed to member states and the EU institutions for the development of an effective policy framework for introducing coordinated vulnerability disclosure (CVD) and government disclosure decision processes (GDDP) in Europe.

Based on its examination of current best practices throughout Europe, the US and Japan, the Task Force recommends implementation of various policies related to SVD. Part I of this report concentrates on CVD and Part II focuses on GDDP.

CVD policy

The Task Force calls upon the European Commission and the member states to collectively draft a European-level framework complemented by national legislation in accordance with the guidelines and recommendations defined in ISO/IEC 29147:2014 and ISO/IEC 30111 in order to provide legal clarity for software vulnerability discovery and disclosure. The Nationaal Cyber Security Centrum (NCSC) in the Netherlands has published a general guideline for responsible disclosure, which can serve as a useful model that EU member states can follow in drafting their own responsible disclosure policy. In addition, it gives security researchers guidance on how to act in finding and reporting a vulnerability.[1]

[1] See https://www.ncsc.nl/english/current-topics/news/responsible-disclosure-guideline.html.

The Coordinated Vulnerability Disclosure Template from the National Telecommunications and Information Administration (NTIA) of the US Department of Commerce could also offer helpful suggestions.[2]

It is also worth mentioning that the US Department of Justice (Cybersecurity Unit, Computer Crime and Intellectual Property Section of the Criminal Division) released in July 2017 the first version of a framework for a Vulnerability Disclosure Program for Online Systems.[3] This framework could serve as a possible model for EU member states to consider adopting. Recognising that different organisations may have different goals and priorities for their vulnerability disclosure programs, the US framework does not dictate the form of or the objectives for vulnerability disclosure. Instead, it outlines a process for designing a vulnerability disclosure program that will clearly describe authorised vulnerability disclosure and discovery behaviour, thereby substantially reducing the likelihood that such described activities will result in a civil or criminal prosecution.

The Task Force recommends that national computer emergency response teams (CERTs) should put in place frameworks that are similar to the ones adopted in the Netherlands and the US. Moreover, such frameworks should be prominently announced on the websites of organisations that establish a CVD, which researchers can consult and rely on for legal certainty.

Policy recommendations from the Task Force

Implementation of CVD in Europe

EU legislation

1. **Amending Directive 2013/40/EU on attacks against information systems (the EU cybercrime Directive) to support CVD**.
2. **Protection of security researchers.** Researchers involved in vulnerability discovery are often exposed to criminal or civil liability.[4] The legal liability and responsibilities of security researchers should be fully clarified to enable them to continue their work without fear of prosecution.
3. **Incentives for security researchers**. Appropriate policies should be adopted with the aim of encouraging 'white-hat hackers' to actively participate in coordinated vulnerability disclosure programmes.

---

[2] See https://www.ntia.doc.gov/files/ntia/publications/ntia_vuln_disclosure_early_stage_template.pdf

[3] See https://www.justice.gov/criminal-ccips/page/file/983996/download.

[4] See https://techcrunch.com/2017/07/25/hungarian-hacker-arrested-for-pressing-f12/.

4. **Directive on security of network information systems (NIS).** In transposing the NIS Directive, particularly its Article 14, member states may explicitly consider including CVD as one of the technical and organisational measures.
5. **General Data Protection Regulation (GDPR**). According to the GDPR, software owners and tech firms become data controllers when they exercise overall control over the purpose for which, and the manner in which personal data are processed. Assuming that irresponsible handling of vulnerabilities could lead to personal data breaches falling within the scope of GDPR, CVD should be viewed as one of the necessary tools to mitigate the relevant risks.
6. **Cybersecurity Act.** According to the proposed Regulation submitted in October 2017 by the European Commission concerning the European Network and Information Security Agency (ENISA) and cybersecurity certification, in its coordination and capacity-building roles, ENISA can contribute to the harmonised development of CVD in the EU by having its mandate amended, thereby allowing it to engage in the following activities:
    - Writing EU-wide guidelines for the reporting process, addressing the issues it raised in its January 2017 "Good Practice Guide on Vulnerability Disclosure" report;[5]
    - Installing and operating a web portal where disclosure of software and hardware vulnerabilities can be coordinated at the European level and contributed to anonymously;
    - Building a team of 'white-hat hackers' who would conduct campaigns in coordination with EU member States to assist EU member states and operators of essential services to mitigate software vulnerabilities, with the objective of increasing the security of critical infrastructure;
    - Implementing training in all issues that may arise in the context of CVD, e.g. technical, legal, etc., to build capacity on CVD in the EU; and
    - Liaising formally with other key international actors on CVD in order to enhance cooperation, collaboration and the sharing of best practices.

Furthermore, **Article 47 (1)j of the Cybersecurity Act** states that a European cybersecurity certification scheme is expected to include *inter alia* "rules

[5] See https://www.enisa.europa.eu/publications/vulnerability-disclosure.

concerning how previously undetected cybersecurity vulnerabilities in ICT products and services are to be reported and dealt with." This provision of the Cybersecurity Act provides the possibility to introduce CVD in a European Cybersecurity Certification Scheme, which in fact may encourage CVD as a standard practice.

7. **Software vulnerabilities in durable goods such as cars and medical devices**
    - The European Commission should amend the radio equipment Directive so that Article 3 paragraph 3 provides that "radio equipment is cybersecure by design, by default and by implementation".
    - The Commission should incorporate the standards for vulnerability management (ISO 29174, 30111) directly into the CE mark system.

National legislation

8. **Amending national legislation to support CVD.** As a medium-to-long-term solution and given that the revision of the EU cybercrime Directive (from 2013) may take several years, the Task Force advises member states to consider amending their national legislation bearing on CVD, using the framework on CVD introduced in the Netherlands as a model.

EU research funding

9. **Framework Programmes for Research and Innovation**. The various European Framework Programmes for Research and Innovation offer several ways to leverage funding to promote CVD among public and private researchers in Europe. For instance, the following H2020 calls described in the Work Programme 2018-2020 could be used to finance research and innovation in this area:
    - SU-ICT-03-2018: Establishing and operating a pilot project to create a Cybersecurity Competence Network
    - SU-DS02-2020: Management of cyber-attacks and other risks
    - SU-DS03-2019-2020: Digital security and privacy for citizens and small and medium enterprises and micro enterprises
    - SU-DS04-2018-2020: Cybersecurity in the Electrical Power and Energy System (EPES)
    - SU-DS05-2018-2019: Digital security, privacy, data protection and accountability in critical sectors

    The next Framework Programme for Research and Innovation, FP9, should also provide explicit funding for CVD across Europe.

Recommendations to implement government disclosure decision processes (GDDP) in Europe

In the course of their day-to-day functioning, governments often acquire insights into vulnerabilities. Thus, ensuring that governments and their agencies have strong policies for reviewing and coordinating the disclosure of vulnerabilities is a critical norm that should be advanced within the EU. It appears, however, that most member states have not yet implemented a government disclosure decision process (GDDP).

GDDP characteristics. The Task Force recommends that all member states adopt the following policies and practices to inform the GDDP activities of their government institutions and agencies:

10. All security vulnerabilities should be subject to a government vulnerability disclosure review process.[6]
11. All relevant ministries, including those with missions for user, business and government security, should participate in the GDDP and participants should work together using a standard set of criteria to ensure that all risks and interests are considered.
12. The policies, practices and findings of the GDDP should be subject to independent oversight and transparency. Regular public reporting should be viewed as a critical part of this.
13. The executive secretariat of the GDDP should be housed within a civilian agency with expertise in existing coordinated vulnerability disclosure.
14. The GDDP should be codified in law or other legally binding policy to ensure compliance and permanence.
15. Any non-disclosure agreement with contractors, resellers or security researchers should be prohibited, and any other exceptions should be limited (e.g. for ultra-sensitive issues).
16. Any decision to delay disclosure of a vulnerability should be reviewed at least every six months.
17. The default policy should be to disclose vulnerabilities immediately to the affected vendor(s) so they can be patched.
18. Where the vulnerability potentially affects the safety of regulated products (such as cars, medical devices or railway signals), the relevant EU safety and standards bodies should be involved in the GDDP.

---

[6] Vulnerabilities identified through security researcher activity and incident response that are intended to be disclosed in a rapid fashion should not be subject to adjudication by GDDP review.

ENISA can play a vital role in sharing best practices in GDDP and assisting and advising member states in their implementation.

Survey of member states' GDDP. It might also be useful for the European Commission or ENISA to conduct a study of member states' efforts to implement GDDP. A better understanding of how member states are handling vulnerabilities will contribute to a more robust and informed debate about cybersecurity in Europe and the types of measures that are needed to improve coordination and cooperation vis-á-vis cybersecurity incidents in the EU.

PART I
COORDINATED VULNERABILITY DISCLOSURE IN EUROPE

1. INTRODUCTION

1.1. Background

The year 2018 kicked off with two of the worst computer security flaws ever experienced – Meltdown and Spectre – which affect nearly every computer chip manufactured in the last 20 years. And last year, people all over the world became familiar with the names of malicious ransomware, such as Wannacry and Petya, which block access to a computer system until a sum of money is paid. We also learned that the personal information of nearly 146 million Americans was compromised by a hacker who took advantage of a security flaw in software used by Equifax that had not been patched.

Today, software is embedded everywhere: in our smartphones, our cars, our offices and our homes. This fact of 21st century life means that most software and software-based products are susceptible to vulnerabilities (see definitions of key terms in section 1.3). It has been estimated that the average programme has at least 14 separate points of vulnerability.[7] Each of those weaknesses could permit an attacker to compromise the integrity of the product and exploit it for personal gain. Therefore, software vulnerabilities and their timely patching pose a serious concern for everyone. What can we do to protect ourselves? Who should look for vulnerabilities and should the vendors or the users be informed about them?

The debate on how to handle the disclosure of insecurities pre-dates software security. It can be traced back to the locksmiths and lock-picking in England in the 1850s. In his book, *The Rudimentary Treatise on the Construction of Locks*, locksmith Alfred Hobbes argued that "it is to the interest of honest persons to know about [insecurities], because the dishonest are tolerably certain to be the first to apply the knowledge practically". And for several decades now, this issue has been the subject of broad debate in the information security arena.

But the extraordinary events of early this year have created a heightened sense of anxiety and urgency on this issue. Moreover, with the development of the "Internet of Things" (IoT) and billions of devices connected to the internet, software plays an ever-greater role in our daily lives. Indeed, as industries and

[7] "The myth of cyber-security", *The Economist,* 8 April 2017, p. 9.

infrastructure become more digitalised and connected, the attack surface becomes broader, which greatly increases the potential impact of vulnerabilities on the ecosystem. Large attacks, such as Wannacry, have shown that vulnerabilities can be used to construct exploits that can put unprecedented pressure on critical infrastructure and more broadly to threaten the integrity, availability and confidentiality of data and the smooth provision of essential services. As the saying goes: "Phones and laptops don't kill many people directly: cars and medical devices do."[8]

Many of these smart systems and devices (refrigerators, medical devices and cars) are expected to be operational for many years or even decades with a minimum of intervention. They also make extensive use of third-party libraries in integrated products, which act as a black box whose security is difficult to analyse. Therefore, industry, government and researchers should start thinking of how to effectively merge safety with security to ensure sustainability in software and in the supporting tool-chains.[9] This process presents numerous challenges, including vulnerabilities research and disclosure.

Where does Europe stand on the debate and practices on vulnerability research and disclosure?

In 2016, the European Union Agency for Network and Information Security (ENISA) published a report,[10] presenting the current situation on vulnerability disclosure, the challenges related to this process and some recommendations to address the challenges and increase adoption of good practices.

The Joint Research Centre (JRC) of the European Commission, and in particular the Cyber and Digital Citizens' Security Unit, carried out research on the vulnerability disclosure process. In the first quarter of 2017, it organised a workshop on zero-day vulnerabilities with representatives from academia, industry and government. The main conclusions were:

1) Research should be the main driver for discovery,

2) An EU-wide independent third party should act as coordinator and

---

[8] Ross Anderson, "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, 27 September 2017, Brussels (https://www.ceps.eu/sites/default/files/Ross%20Anderson%2C%20Cambridge.pdf).

[9] E. Leverett, R. Clayton and R. Anderson (2017), "Standardization and Certification of the 'Internet of Things'", mimeo, May 2017.

[10] ENISA, "Good Practice Guide on Vulnerability Disclosure", 18 January 2016.

3) A pilot EU vulnerability management centre should serve as a test-bed platform for responsible and coordinated vulnerability disclosure.[11]

The 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" to the European Parliament and the Council of September 2017, referred to the "important role of third party security researchers in discovering vulnerabilities in existing products and services need to be acknowledged and conditions to enable coordinated vulnerability disclosure should be created across Member States, building on best practices and relevant standards".[12]

Some governments, such as the Netherlands, have been quite active in this area and, together with the private sector and the security research community, developed as early as 2013 a model of coordinated vulnerability disclosure.

As this report will show in more detail later, however, only a few countries across Europe have managed to put vulnerability disclosure processes in place. Therefore, following a workshop on these issues in June 2017,[13] CEPS decided to launch a Task Force on Software Vulnerability Disclosure in Europe to focus on key aspects surrounding the debate on this issue. The Task Force explored ways to formulate guidelines for governments and businesses to harmonise the process of handling SVD. The Task Force aimed to outline specific principles and formulate policy recommendations for member states and the EU institutions in the development of an effective policy framework for introducing a process of so-called coordinated vulnerability disclosure in Europe.

---

[11] Ignacio Sanchez and Laurent Beslay (2017), "EU zero-day vulnerability management", presentation at the CEPS Workshop on SW Vulnerability Disclosure: The European Landscape, 23 June 2017, Brussels (https://www.ceps.eu/sites/default/files/JRC_presentation_ceps_final%20%28Sanchez%29).

[12] European Commission, 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", 13 September 2017, p. 6.

[13] See report of the event from 23 June 2017 (https://www.ceps.eu/events/software-vulnerabilities-disclosure-european-landscape).

1.2. Some definitions

Before moving forward, let's start with some definitions.

What is a vulnerability?

"A vulnerability is a set of conditions or behaviours that allows the violation of an explicit or implicit security policy. Vulnerabilities can be caused by software defects, configuration or design decisions, unexpected interactions between systems or environmental changes. Successful exploitation of a vulnerability has technical and risk impacts. Vulnerabilities can arise in information processing systems as early as the design phase and as late as system deployment."[14]

Definitions of an exploit, malware, an incident, a patch and zero-day vulnerability

An *exploit* is a software programme that uses a vulnerability to generate some effect. *Malware* is software programme used to compromise the security of a system. An *incident* is a "violation or an attempted violation of a security policy and may involve malware, exploits or vulnerabilities".[15] A *patch* is a piece of software designed to update a computer programme or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and other bugs.[16] A *zero-day vulnerability*, also known as a computer zero day, is a flaw in software, hardware or firmware that is unknown to the party or parties responsible for patching or otherwise fixing the flaw.[17]

1.3. What is vulnerability disclosure?

As defined in ISO/IEC 29147:

Vulnerability disclosure is a process through which vendors and vulnerability finders may work cooperatively in finding solutions that reduce the risks associated with a vulnerability.

---

[14] See "The CERT Guide to Coordinated Vulnerability Disclosure", by Allen D. Householder, Garret Wassermann, Art Manion and Chris King, Software Engineering Institute, Carnegie Mellon University, August 2017, p. 2. This part of this report draws from this source.

[15] Ibid., p. 2.

[16] https://en.wikipedia.org/wiki/Patch_(computing).

[17] http://searchsecurity.techtarget.com/definition/zero-day-vulnerability.

It encompasses actions such as reporting, coordinating and publishing information about a vulnerability and its resolution.

The goals of vulnerabilities disclosure include: i) ensuring that identified vulnerabilities are addressed, ii) minimising the risk from vulnerabilities and iii) providing users with sufficient information to evaluate risks from vulnerabilities to their systems.[18]

It is important to emphasise that **vulnerability disclosure is a process and not an event**![19] It starts with an awareness of the vulnerability and continues with asking (at a minimum) the following two questions:

1. Now that I am aware of this vulnerability, what should I do in response?
2. Who else needs to know, what and when?

The vulnerability disclosure process ends only when these two sets of questions are completely answered.

This process is delimited by two extreme approaches:

1. Full disclosure: Public release of all details of the vulnerability, often without any mitigation measures to protect users.
2. No disclosure: Nothing is disclosed, i.e. a researcher may be discouraged from disclosure, as a way for governments or vendors to acquire vulnerabilities for exploitation or advantage at a later stage.

Research shows that neither of these approaches socially optimal. Instead, there are two other modalities of disclosure that give better results. They fall in the middle of the two extremes cases above and are called "responsible disclosure" and "coordinated vulnerability disclosure" or CVD. Since what constitutes responsible behaviour is a matter of opinion, however, the use of the term CVD helps to reduce misunderstandings and promotes cooperation. Indeed, both responsible disclosure and coordinated vulnerability disclosure aim at sharing information on vulnerabilities with vendors, but they differ on the degree of the coordination process to protect users.

1.4. Coordinated vulnerability disclosure

Coordinated vulnerability disclosure (CVD) is a process aimed at mitigating/eradicating the potential negative impacts of vulnerabilities. It can be defined as "the process of gathering information from vulnerability finders,

---

[18] ISO/IEC, "ISO/IEC 29147:2014 Information technology-Security techniques-Vulnerability disclosure", 2014.

[19] CERT Guide, op. cit., p. 2.

coordinating the sharing of that information between relevant stakeholders, and disclosing the existence of vulnerabilities and their mitigation to various stakeholders, including the public".[20] Input into this process includes reports from vulnerability discovery practices, and its output takes the form of patches, vulnerabilities report and database records. Other operational vulnerabilities, such as router misconfigurations, website vulnerabilities and cloud problems, can be fixed directly by the operator and quite often do not require a public disclosure.

1.5. Actors in CVD

Let's begin by examining the CVD process in more detail, starting from the various actors that play a role in this process. The CERT Guide[21] identifies five major actors:

- **Finder (discoverer) –** the person or organisation that identifies the vulnerability
- **Reporter –** the person or organisation that communicates the vulnerability to the vendor[22]
- **Vendor –** the person or organisation that created or manages the product that is vulnerable
- **Deployer –** the person or the organisation that has to deploy the patch or take other remediation actions
- **Coordinator –** the person or organisation that facilitates the coordinated disclosure process

Figure 1 diagrams the relationships among these various actors. Very often persons and organisations play multiple roles: a cloud provider can act as vendor and deployer, a researcher can be both finder and reporter and a vendor may also be deployer and coordinator, especially in cases where an official coordinator, i.e. a CERT, does not exist.

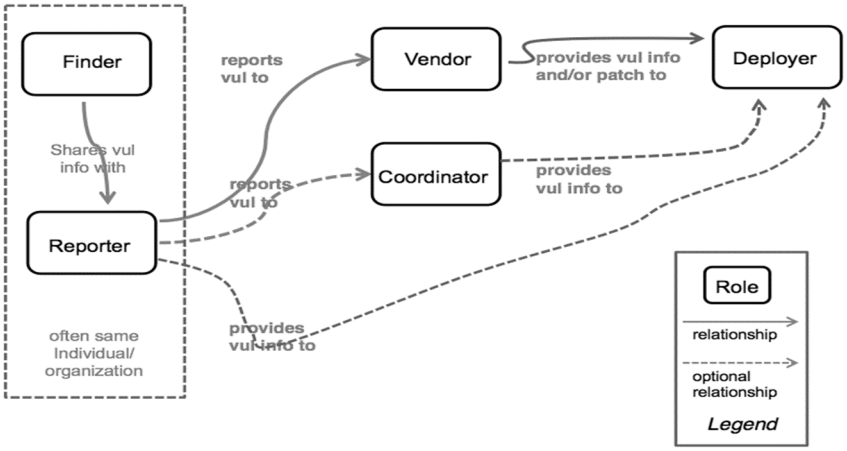
---

[20] "CERT Guide", op. cit., p. 3.

[21] Ibid., p. 15.

[22] This role often overlaps with other roles and ideally should always be the finder or the coordinator.

Figure 1. Relationships among actors in the CVD process



Source: Allen D. Householder, Garret Wassermann, Art Manion and Chris King, "The CERT Guide to Coordinated Vulnerability Disclosure", Software Engineering Institute, Carnegie Mellon University, August 2017.

1.6. Phases of CVD

Starting from the standards specified in ISO/IEC 30111 and considering various models of CVD, it is possible to identify the following phases of the CVD process:[23]

- **Discovery –** One or more security researchers uncover a vulnerability using one of the available methodologies.
- **Reporting** – A security researcher presents a vulnerability report to a software or product vendor or, if necessary, to a third-party coordinator.
- **Validation and triage** – In this phase the report is validated by analysts to guarantee accuracy before any practical action is taken in terms of timing and modality of response.
- **Remediation** – A remediation plan (such as a software patch) is developed and tested.
- **Public awareness** – The vulnerability itself and its patch are disclosed to the public.
- **Deployment** – The patch is applied to deployed systems.

[23] Ibid., p. 29. This Guide also contains a more detailed discussion of the different phases of CVD.

Table 1 presents a mapping of these various phases and actors involved in carrying out CVD.

Table 1. CVD actors, by phase

Actors ->	**Finder**	**Reporter**	**Vendor**	**Coordinator**	**Deployer**
Phases					
Discovery	Finds vulnera-bilities				
Reporting	Prepares report or submits bug information	Reports vulnerabilities to vendor(s) and/or coordinators	Receives reports	Receives reports Acts as reporter proxy	
Validation and triage			Validates report received Prioritises reports for response Determines if bub needs to/can be mitigated	Validates report received Prioritises reports for response	
Remediation		Confirms fix	Works with other vendors or finder to develop a mitigation Prepares patches Submits mitigation to partners and other vendors to ensure compatibility Develops advice, workarounds	Coordinates multi-party response Develops advice, workarounds	

Public awareness	Publishes report	Publishes report	Publishes report	Publishes report	Publishes report
Deployment					Deploys fix or mitigation

Source: Adapted from "The CERT Guide to Coordinated Vulnerability Disclosure", by Allen D. Householder, Garret Wassermann, Art Manion and Chris King, Software Engineering Institute, Carnegie Mellon University, August 2017.

1.6.1. Bug bounty programs

When it comes to coordination, it is worth mentioning the role that *ad-hoc* bug bounties programs are playing in the process of coordinated vulnerability disclosure. Many companies have created their own programs to compensate security researchers for their efforts in finding vulnerabilities. For instance, Microsoft, Mozilla, Kaspersky Lab and ING run their own bug bounty programs. [24] In other cases, these programs are managed by other companies that use their own platforms and teams of experts, connect organisations to a global crowd of trusted security researchers to identify vulnerabilities. This is the case of companies such as BugCrowd or HackerOne. One example is HACK THE PENTAGON, a bug bounty programme of the US Department of Defense on the Hackerone platform. Bountyfactory.io, ranked in 1st place in crowd security in Europe, is a European bug bounty platform facilitating collaboration among companies and the largest community of European security experts (involving more than 3,700 bug hunters).

1.7. Special cases of CVD

1.7.1. Multiparty CVD[25]

When there are only two parties involved in the CVD process – the finder of the vulnerability and the vendor that will fix the vulnerability – things are more manageable overall and it is easier to create the right communication and trust between the two parties. When the CVD involves more than two actors, however, as in the recent case of Spectre and Meltdown where a variety of companies – Intel, AMD, ARM, Google, Microsoft, Apple, Oracle, Amazon and others – scrambled to send out software changes to protect against the hardware flaws, it becomes more complex due to the need to synchronise the

[24] A list of European companies running Bug Bounties programs can be found at: https://bountyfactory.io/programs

[25] See CERT Guide (2017), op. cit., pp. 45-47.

development, testing and release process of the different organisations. The Vulnerability Coordination Group of the Forum of Incident Response and Security Teams (FIRST) has also published an *ad-hoc* report on this issue: "Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure". [26]

Following the suggestions from the CERT Guide to CVD, we will now discuss in more detail some of the issues related to multiparty CVD.

Independent rediscovery

It sometimes happens that the same vulnerability is independently discovered by two or more individuals. This process is called "vulnerability rediscovery". Different views exist on the frequency of this phenomenon. For example, for a given stockpile of zero-day vulnerabilities, Lillian Ablon and Andy Bogart from the Rand Corporation estimated that after a year approximately 5.7% have been rediscovered by others.[27] Trey Herr, Bruce Schneier and Christopher Morris of the Belfer Center at the Harvard Kennedy School, however, show that rediscovery takes place even more often than previously estimated. Indeed, they report that 15-20% of vulnerabilities are discovered independently at least twice within a year. In particular, for the Android operating system, 13.9% of vulnerabilities are rediscovered within 60 days, increasing to 20% within 90 days and above 21% within 120 days. And for the Chrome browser, they found 12.57% rediscovery within 60 days. The researchers conclude that "the information security community needs to map the impact of rediscovery on the efficacy of bug bounty programs and policymakers should more rigorously evaluate the costs of non-disclosure of software vulnerabilities".[28]

Complicated supply chains

Already today, and especially with the development of the IoT, many products are or will be developed by more than a single organisation. This is also the case of software libraries licensed for inclusion in other products. When a vulnerability is discovered in one part of a library, it is clear that not only the originating vendor of that part will be involved in the disclosure but also all the downstream vendors that use that library. There are vertical and horizontal

---

[26] See FIRST (https://first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.0), July 2017.

[27] Lillian Ablon and Andy Bogart, *Zero Days, Thousands of Nights – The Life and Times of Zero-Days Vulnerabilities and Their Exploits*, Rand Corporation, Santa Monica, CA, 2017, p. xii.

[28] Trey Herr, Bruce Schneier and Christopher Morris, "Taking Stock: Estimating Vulnerability Rediscovery", Working Paper, Belfer Center, Harvard Kennedy School, Cambridge, MA, July 2017, p. 1.

supply chains. In a **vertical supply chain,** multiple products all share dependency on a vulnerable library or component. When the patch is developed for a given component, it can be used for all products. In a **horizontal supply chain,** multiple products implement the same vulnerability (from underspecified protocols or design flaws). Therefore, each vendor must develop patches for their own implementation of the vulnerability. The management of the latter is more complicated.

Response pacing, synchronisation and communication

It may occur that the various parties respond to a discovery at different paces. The originating vendor is interested in disclosing as soon as the patch is ready, putting the downstream users at risk. At the same time, some vendors would like to release the patch sooner than others. All these coordination problems require better communication among the various parties. In this case, it could be very helpful to put all parties in contact with one another directly through the use of conference calls, group meetings and a private mailing list, instead of having a coordinator.

1.7.2. Forever day vulnerabilities

To complete the analysis, it is worth mentioning the special case in which it may be impossible to mitigate or patch a discovered vulnerability. This is the case when the vulnerability is discovered in legacy products nearing the end of their life cycle. In this case, vendors do not patch the vulnerabilities but simply advise the user on how to work around the threat.[29]

1.8. Future issues in CVD

The most important issues for the future development of CVD are related to the diffusion of the Internet of Things. The diffusion of 'smart things' will soon outnumber computers and in the near future, mobile phones as well. Their vulnerabilities may be remotely exploited, posing great security risks to society.[30] Furthermore, many companies today producing 'smart things' do not

---

[29] Dan Goodin, "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, 10 April 2012 (https://arstechnica.com/information-technology/2012/04/rise-of-ics-forever-day-vulnerabiliities-threaten-critical-infrastructure/).

[30] The case in point here is the 2016 Dyn Cyberattack that took place 21 October 2016, and involved multiple distributed denial-of-service attacks (DDoS attacks) targeting systems operated by Domain Name System (DNS) provider Dyn, which caused major internet

specialise in security, so we can expect a steep learning curve for them, code re-use across products and the need to acquire external expertise in security.

This prospect presents engineers, researchers and regulators with numerous new challenges, such as embedding security and safety into technical standards, e.g. based on security-by-design and security-by-default principles. However, ensuring sustainability in software and in the supporting tool-chains is proving to be more challenging than one might expect: How does one write code for which security patches must be made available for the next 30 years?

platforms and services to be unavailable to large swathes of users in Europe and North America. Dyn disclosed that, according to business risk intelligence firm FlashPoint and Akamai Technologies, the attack was a botnet coordinated through a large number of Internet of Things-enabled (IoT) devices, including cameras, residential gateways, and baby monitors, that had been infected with Mirai malware (see https://en.wikipedia.org/wiki/2016_Dyn_cyberattack).

3. STATE OF PLAY IN CVD BY COUNTRY

3.1. CVD within member states

An important focus of this Task Force has been to conduct a survey of the progress made by EU member states in implementing a national CVD policy. The Netherlands has led the EU's efforts in establishing CVD policies and has heavily contributed to supporting other member states in their efforts to address their own challenges and concerns. The country has a proper legal framework in place, as well clear procedures for reporting vulnerabilities that include the protection of the researcher. France has recently put together a clear and effective legislative framework and incorporated CVD in their Law for a Digital Republic (Art. 47). According to recent reports, Lithuania also deserves to receive special mention: a vulnerability disclosure framework for a specific sector ("providers of public communications networks") is in place, which includes a disclosure deadline, scheduled resolution and an acknowledgement report. Organizations have established processes to receive and disseminate vulnerability information.

As can be seen in the list below and in Figure 2, many countries plan to implement such a policy but haven't yet reached a consensus at the political or legislative level. This is the status, for instance, in Austria, Belgium, Bulgaria, Czech Republic, Finland, Germany, Hungary, Italy, Latvia, Luxembourg, Romania, Slovenia and the United Kingdom. More details on these and other countries' progress are given below.

Austria

Austria hasn't yet implemented a CVD policy. CERT.at members have sent some proposals for introducing a CVD policy to those responsible for transposing the Directive on security of network and information systems (**NIS** Directive) into national law. According to these members, however, implementing a specific CVD policy is not needed as existing law already allows for disclosure.

Belgium

Belgium hasn't implemented a CVD policy, but it plans to do so. Based on the Task Force's independent and preliminary research, the Belgian Parliament

intends to create room in its legal framework to allow for ethical hacking,[31] although it is currently focusing its attention on implementing the NIS Directive first. A representative of the Center for Cyber Security Belgium told the Task Force that it has made a proposal and is currently waiting for comments from the Cybercrime group of the Ministry of Justice and the Government's approval.

Bulgaria

Bulgaria hasn't yet implemented a CVD policy and there is no plan to implement one at this stage. Recognising the importance of a developing a well-defined and speedy process of vulnerability detection, mitigation and correction, CERT Bulgaria is hopeful that discussions on this issue will start as soon as possible.

Croatia

Croatia has not provided the Task Force with an official response. Based on our independent and preliminary research, there is no CVD policy in place or under consideration at this time.

Cyprus

Cyprus hasn't provided the Task Force with an official response. Based on our independent and preliminary research, there is no CVD policy in place or under consideration at this time.

Czech Republic

Czech Republic does not have a CVD policy at the national level and there are no current discussions at the present time. On the other hand, their national Government CERT (NCKB, NUKIB) sees CVD as a topic it needs to catch up with and would like to start a discussion at the national level in the course of 2018.

Denmark

Denmark hasn't provided the Task Force with an official response. Based on our independent and preliminary research, there is no CVD policy in place at this time.

---

[31] See https://cert.lv/uploads/pasakumi/Nathalie_Falot.pdf.

Estonia

Estonia hasn't provided the Task Force with an official response. Based on our independent and preliminary research, there is no CVD policy in place at this time.

Finland

In 2010, the National Cyber Security Center Finland (NCSC-FI) published a Vulnerability Coordination Policy. Such policy (updated in 06/2012) is an ongoing effort to spell out their position and to initiate discussion on the topic. NCSC-FI promotes responsible handling of vulnerability information during all stages of the vulnerability lifecycle, and not merely during the disclosure phrase. There are no ongoing discussions.

Former Yugoslav Republic of Macedonia

Regarding CVD policy, the national CSIRT of the Former Yugoslav Republic of Macedonia (FYROM) has a general policy on information disclosure, which is publicly available on its website, but only in the local Macedonian language. They are in the process of drafting a more specialised CVD policy for reporting vulnerabilities in its systems and services as well as in third-party systems, which is expected to be published by the end of Q2 2018.

France

France has established a CVD policy. In the event that a researcher reports a suspected vulnerability to ANSSI (Agence nationale de la sécurité des systèmes d'information, the country's service created in 2009 with responsibility for computer security), Art. 47 of the Law for a Digital Republic supersedes Art. 40.[32] Art. 47 exempts the researcher ("goodwill person") who reports the

---

[32] Art. 47 reads: «Art. L. 2321-4.-Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données.»

«L'autorité préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée.»

«L'autorité peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace mentionnés au premier alinéa du présent article aux fins d'avertir l'hébergeur, l'opérateur ou le responsable du système d'information.»

And Art. 40 reads: "Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en

vulnerability from the provisions contained in Art. 40. The Agency also undertakes to protect the confidentiality of the identity of the researcher who reports the vulnerability.

Germany

Germany's Federal Agency for Information Security (BSI) has a clear mandate for IT network security and by extension for the security of IT products. As a part of BSI, the national CERT section CERT-Bund protects German stakeholders by reporting vulnerabilities and coordinating their disclosure. A CVD policy is still a work in progress, with implementation planned for later this year (2018).

Greece

The Task Force has not received an official response from Greece concerning its efforts in this area. Based on our independent and preliminary research, there is no CVD policy in place at this time.

Hungary

Hungary hasn't implemented a CVD policy. The country's representatives expressed interest in doing so at the Expert Meeting on Responsible Disclosure" of the Global Forum on Cyber Expertise (GFCE) in March 2016, but there have been no further updates since.

Ireland

Ireland hasn't provided the Task Force with an official response. Based on our independent and preliminary research, there is no CVD policy in place at this time.

Italy

The Digital Transformation Team has started to draft a CVD policy that aims to be generic and potentially will cover both the private and public sectors. The work is being carried out in collaboration with the two national CERTs. There are ongoing discussions on how to harmonise CVD, given the national laws regulating computer crime and (unauthorised) access as well on the legal aspects such as the legal protection of the researcher. A pilot programme aimed at supporting private companies in implementing CVD policies and improving internal/external processes has been prepared, but it is currently on hold pending the resolution of certain legal questions.

---

donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs."

Latvia

Latvia has been very active in European discussions on Responsible Disclosure Policy (RDP), including the GFCE RDP forum. This report devotes an entire chapter to their experience.

Lithuania

A report[33] facilitated by the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford and released in November 2017 observes that "Lithuania has reached a strategic stage in national capacity to design a cyber resilience strategy and lead its implementation as well as in the existence of reliable Internet services and infrastructure".

Based on our discussions with experts at GCSCC who worked on this report, Lithuania is still in the process of developing its own Cybersecurity Strategy, which is likely to incorporate CVD within the strategy. The final discussion and its submission to a final vote is planned for the summer of 2018.

They've also reported that the following steps have been taken in Lithuania:

> According to the Order on the Approval of the Rules on the Insurance of Security and Integrity of Public Communications Networks and Public Electronic Communications Services in Lithuania, providers of public communications networks will report certain types of security incidents and they must inform the Authority within one working day. The National Cyber Security Center is responsible for collecting all incident disclosures and notifications when it comes to CI (Critical infrastructure) assets. Also another important point is the role of CERT-LT, in reporting to other authorities as required. Regarding national level issues, CERT-LT reports to the Government; on security issues related to the Critical National Infrastructure (CNI), CERT-LT reports directly to the MoND; on personal data protection issues, to the State Data Protection Inspectorate; and on suspected criminal activity, to the Lithuanian Cyber-Police. Overall, it seems that different procedures are in place in different communities.
>
> A vulnerability disclosure framework for the public communications networks is in place, which includes a disclosure deadline, scheduled resolution and an acknowledgement report. Organisations have established procedures for receiving and disseminating vulnerability information."

---

[33] See https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/lithuania-cybersecurity-capacity-review-2017.

Luxembourg

Luxembourg has not implemented a CVD policy. GOVCERT mentioned that they are having discussions about the CVD topic at the highest possible level, the Cyber Security Board, chaired by their Prime Minister. The setting up of a national CVD plan will probably be covered by the third revision of the national strategy on cyber-security (currently being written and to be published in Q2 2018). All the actors involved agreed that Luxembourg needs a CVD strategy on a national level.

For the private sector, CIRCL (Computer Incident Response Center Luxembourg) has mentioned that there already are security vulnerability disclosure procedures in place for the private sector (see https://www.circl.lu/pub/responsible-vulnerability-disclosure/).

CIRCL reports that it already has a good basis for the generic guidelines for its cyber security strategy.

Malta

Based on our independent and preliminary research, there is no CVD policy operating in the country at this time.

The Netherlands

The Netherlands has implemented a CVD policy. The Dutch experiences with coordinated vulnerability disclosure policies have been very positive. Many organisations in the Netherlands have actively adopted coordinated vulnerability disclosure and have been satisfied with the results. There's a dedicated chapter in this report regarding their experience.

Poland

Poland has not provided the Task Force with an official response. Based on our independent and preliminary research, there is no CVD policy in place at the time of writing.

Portugal

Portugal hasn't provided the Task Force with an official response. Based on our independent and preliminary research, there is no CVD policy at this time.

Romania

CERT.ro publishes a CVD policy on its website, although it clearly states that "CERT-RO must answer successfully to this challenge even in the absence of a proper legislation regarding disclosure of vulnerabilities, through implementing

Coordinated Vulnerabilities Disclosure mechanisms (CVD)". Companies and institutions are strongly encouraged at national level to adopt mechanisms enabling the reporting, rapid evaluation and remedy of the vulnerabilities and the identification of and adoption of a dedicated legal framework for reporting vulnerabilities.

Slovakia

Slovakia has not provided the Task Force with an official response. Based on our independent and preliminary research, there is no CVD policy in place in the country at this time.

Slovenia

Slovenia has not yet implemented a CVD policy. Their national CERT (SI-CERT) has proposed to add this topic to the upcoming Law on Information Security, but no consensus has reached for such support at this time. Together with the Information Commissioner's Office, SI-CERT intends to continue this debate with the representatives of the Ministry of Justice. The challenges they face are related to the awareness of decision-makers on the political level concerning current best-practices in the Information Security community.

Spain

Spain has not provided the Task Force with an official response. Based on our independent and preliminary research, there is no CVD policy in place at this time.

Sweden

Sweden has not provided the Task Force with an official response. Based on our independent and preliminary research, there is no CVD policy in place at this time.

United Kingdom

The UK government's pilot project for vulnerability coordination, involving the National Cyber Security Centre (NCSC), is ongoing. It is working with a selected group of UK-based security practitioners to help them to identify and resolve vulnerabilities across three systems used in the UK public sector. To help them get this right, they are working with a private security company for advice and intend to use a recognised platform for vulnerability coordination. The pilot is a formalisation of previous *ad-hoc* UK government vulnerability coordination efforts, with the goal of designing a mature process to receive, triage and remediate ongoing vulnerability disclosures from the security community.

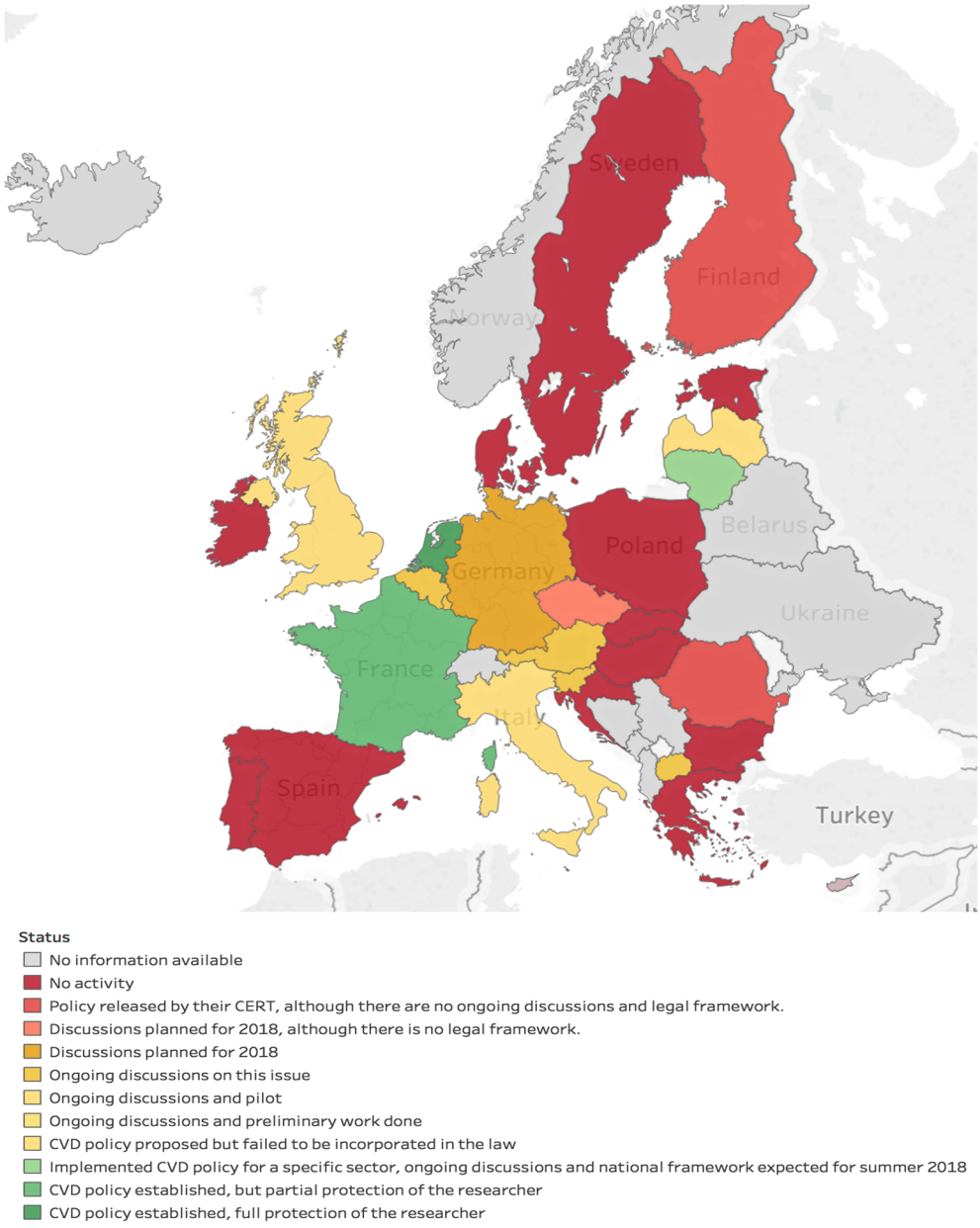
Switzerland

(Neither an EU nor EEA member but part of the single market)

Switzerland has not yet implemented a CVD policy, but it currently enhancing the national strategy for protecting against cyber risks (NCS). During its implementation, MELANI (Reporting and Analysis Center for Information Assurance) allowed that it might be possible to discuss a CVD policy. MELANI/GovCERT has adopted a special approach towards regulating vulnerability disclosure in particular by seeking and encouraging responsible and voluntary behaviour on the part of all participants based on self-governance. Regulation by the state should only be used as a last resort. The Swiss authorities encourage each participant and vulnerability researcher to follow the rules of responsible disclosure. They are coordinating and supporting such efforts by mediating between researchers and affected organisations. They have done this in the past several times and were mostly successful in striking a good balance between protection, timeliness and disclosure.

MELANI/GovCERT discuss the question of Responsible Disclosure in its semi-annual report 2/2015 (see https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2015-2.html). They plan to facilitate the process by establishing a website where vulnerabilities can be communicated in case a direct contact to the vendor fails. When asked about the major challenges they're facing, MELANI cited the different expectations about timeliness of a reaction between the researchers and the manufacturers/vendors. Finding the right security contacts also presented challenges, as not all vendors make their security/incident contacts public.

Figure 2. CVD policy in Europe: A mapping of the state of play, by country



Source: CEPS' own elaboration.

Table 2. Matrix of implementation of CVD policy at national level in Europe

CVD policy at national level	Status	Country
YES	CVD policy established, full protection of the researcher	Netherlands
	CVD policy established, but partial protection of the researcher	France
IN PROGRESS	Implemented CVD policy for a specific sector, ongoing discussions and national framework expected for summer 2018	Lithuania
	Ongoing discussions and preliminary work done	Italy
	See dedicated chapter	Latvia
	Ongoing discussions and pilot	United Kingdom
	Ongoing discussions on this issue	Austria
		Belgium
		Former Yugoslav Republic of Macedonia
		Luxembourg
		Slovenia
	Discussions planned for 2018	Germany
NO	Discussions planned for 2018, although there is no legal framework	Czech Republic
	Policy released by their CERT, although there are no ongoing discussions and legal framework.	Finland
		Romania
	No activity	Bulgaria
		Croatia
		Cyprus

NO	No activity	Denmark
		Estonia
		Greece
		Hungary
		Ireland
		Malta
		Poland
		Portugal
		Slovakia
		Spain
		Sweden

3.2. Case studies of CVD in selected EU member states

3.2.1. The Netherlands[*]

Introduction

In 2011, two high-profile incidents involving ICT (Information and communications technology) became public: a vulnerability in the Dutch public-transport chip card and the Diginotar certification authority case. Both cases affected large parts of the Dutch infrastructure, initiating political discussions on how to prevent these from happening again. One result was that an investigation was started on possible guidelines for coordinated vulnerability disclosure policies. The Dutch Government's Nationaal Cyber Security Centrum (NCSC) cooperated with major sectors of critical infrastructure, including the telecoms and financial sector, to write guidelines for coordinated vulnerability disclosure policy, which was published in January 2013. Companies in the telecommunications sector started publishing their disclosure policies at the end of 2012, with many companies in other sectors following in 2013 and 2014. This

[*] This section of the report was contributed by Jeroen van der Ham, National Cyber Security Centre, The Netherlands.

created some security for researchers to perform their security research and to disclose their findings to the companies.

The practice of vulnerability disclosure has proven to have made a valuable contribution to digital security in the Netherlands. Both public and private parties have received numerous reports of vulnerabilities, which have helped these parties to improve the security of their systems. In addition, the practice of reporting these vulnerabilities has increased the security awareness of companies in the Netherlands.

The past few years have shown that many security researchers are willing to work within the guidelines as published in vulnerability disclosure policies. Reports have been submitted to companies directly or indirectly. Daily practice shows that benevolent reporters and vulnerable organisations were able to come into contact and to exchange information regarding possible vulnerabilities. This has made it possible to increase the security of the network and information systems of these organisations.

Implementation guideline

An important document on coordinated vulnerability disclosure is the Guideline for Responsible Disclosure.[34] This guideline contains implementation advice for organisations, as well as for researchers and disclosers. Below is a brief summary of this guideline.

Guidelines for an organisation

Coordinated vulnerability disclosure starts with an organisation that owns information systems or is the vendor of a product. After all, the owner or vendor has the primary responsibility for the information security of the system or product. It is up to the organisation to adopt and pursue a responsible disclosure policy that can give the organisation an effective approach to resolving vulnerability issues.

By publishing its own coordinated vulnerability disclosure policy, the organisation makes clear how it intends to handle reports of vulnerabilities. As we have seen from a number of parties that have already implemented a policy, the following elements can be used (not limited):

- The organisation drafts a policy for coordinated vulnerability disclosure and makes it publicly accessible.
- The organisation ensures that the threshold for someone wishing to report a vulnerability is low. The method can be standardised, for example, by

[34] See https://www.ncsc.nl/english/current-topics/news/responsible-disclosure-guideline.html.

means of an online form for making reports. The organisation may wish to consider whether anonymous reports should be allowed.

- The organisation makes sure that adequate capacity is available to respond to any report received.
- When an organisation receives a report of a vulnerability, it ensures that the report is routed as quickly as possible to the department best able to evaluate and act on the report.
- The organisation sends the discloser a confirmation of receipt of the report, preferably digitally signed to emphasise the priority. The organisation and the discloser then try to agree on the next steps.
- During the process, the organisation sends regular updates to the discloser, keeping him/her informed on the process and the progress made.
- If the vulnerability is to be made public, the organisation and discloser agree on a date for publication. A reasonable response time for software vulnerabilities is 60 days. Remedying hardware vulnerabilities, however, is often more difficult. A response time of six months for hardware vulnerabilities can be considered reasonable under normal circumstances.
- In consultation with both parties it may be prudent to extend or reduce the above periods, depending on the number of systems involved.
- If a vulnerability is difficult or even impossible to resolve, or if resolving the vulnerability will involve high costs, both parties may agree not to disclose the vulnerability.
- The organisation may decide to provide a discloser with credit for the report, if the discloser so desires.
- The organisation may choose to give the discloser some form of remuneration for reporting the vulnerability if the discloser followed the rules of the responsible disclosure policy. The amount of the reward may be based on the quality of the disclosure.
- In consultation with the discloser, the organisation may decide to inform the broader ICT community of the vulnerability if it is likely that the vulnerability occurs elsewhere.
- In the coordinated vulnerability disclosure policy, the organisation will express its position on declining to take legal action if the discloser acts in accordance with the policy.

Guidelines for the discloser

The discloser in some way observes a vulnerability and wants to contribute to the security of the information system by revealing the vulnerability to the

respective organisation. In doing so, the discloser recognises that they have a social responsibility to disclose vulnerabilities in a coordinated fashion. The following elements can be used in order to set the minimum guidelines for the discloser:

- The discloser is responsible for his/her own actions and should act in a way that is proportionate to prove that a vulnerability exists.
- The discloser should report the vulnerability as quickly as is reasonably possible, to minimise the risk of hostile actors finding it and taking advantage of it.
- However, the discloser should do so in a confidential manner so that others will not gain access to the information.
- The discloser should not set restrictions on providing information regarding a vulnerability. The initiative for giving a reward should be with the receiving organisation, which can set guidelines in its published policy.
- The discloser and receiving organisation will make clear arrangements on publishing details on the vulnerability. If multiple organisations are involved, this should only happen when all organisations are in agreement. It is advisable to discuss the public disclosure at an early stage.
- The discloser and the organisation can make arrangements for informing the broader ICT-community of the vulnerability. This may be the right choice if the vulnerability is newly detected and it is evident that it may be present in other systems or at other organisations. In the Netherlands, the NCSC can provide assistance for coordination in these cases.

The national CERT

Principally, coordinated vulnerability disclosure is a matter between an organisation and a discloser. Nonetheless, in the Netherlands one of the tasks of the national CERT, the NCSC, is to promote the implementation of coordinated vulnerability disclosure policies within organisations. Furthermore, if necessary, the NCSC can pass on information on technical vulnerabilities towards the larger ICT community. This will always be done in close consultation with the respective organisation and discloser. The NCSC can publicly disclose a description of the vulnerability, write or update a fact sheet or white paper, or inform organisations in a coordinated manner.

The NCSC can also act as a mediator. In any situation in which a report is made to the NCSC, the NCSC will attempt to put the discloser or potential discloser into contact with the affected organisation. As mentioned above, the NCSC also coordinates vulnerability disclosure for vulnerabilities that affect governmental organisations or organisations of critical infrastructure.

Responsible Disclosure and prosecution

In March 2013, the Dutch Public Prosecution Service (PPS) published a framework for dealing with disclosers, or ethical hackers who engage in responsible disclosure. In general, there is no mention of 'ethical' hacking in Dutch law on cybercrime. Nor does the law provide for a specific ground for exemption from criminal liability for a discloser acting out of ideological or ethical motives. Although the law does not provide for it, this does not mean that 'ethical' motives cannot play a role in assessing the criminal liability of the actions of the offender.

Principally, no criminal investigation will be instituted in case of legal rehabilitation between the discloser and the relevant company. However, if a vulnerability is reported and there are indications that the discloser did more than what was absolutely necessary to discover the vulnerability, this will need to be investigated further. Examples are copying of sensitive personal data or installing malware on the system. An assessment framework is provided below. This is comparable to the Dutch provision allowing journalists to commit criminal offences for the purpose of newsgathering.

A coordinated vulnerability disclosure guideline defines the preferred actions to be taken when a vulnerability is discovered. In itself, the manner in which this is discovered does not play a role in responsible disclosure. The purpose of coordinated vulnerability disclosure is to contribute to increasing the security of IT systems by reporting possible vulnerabilities in a careful manner, to prevent or limit any damages as much as possible.

If the company does not have a coordinated vulnerability disclosure policy, then no coordinated vulnerability disclosure will exist. When assessing these cases, it is, of course possible to look at the general principles used for coordinated vulnerability disclosure as described in the general disclosure guideline. Further criminal investigation is often needed in order to assess whether the actions taken by a discloser were necessary and proportional under the given circumstances. If a discloser directly and safely communicates with the owner of the IT system on a discovered vulnerability and no data were deleted or manipulated, this could constitute coordinated vulnerability disclosure and there will be no reason for (further) criminal investigation or prosecution. If, however, data were deleted, manipulated or copied, or disproportionate actions were taken by the discloser when gaining access to the IT system, this will not constitute coordinated vulnerability disclosure and a further criminal investigation and criminal prosecution will be indicated.

In summary, the public prosecutor will, in assessing proportional and necessary conduct of a discloser, have to take the following circumstances into account:

- Did the suspect break criminal laws in the process of finding and reporting the vulnerability?
- Were the suspect's actions necessary within a democratic society, i.e. did they concern an important general interest?
- Did the suspect's conduct involve proportional actions (were the means chosen in proportion to the goal to be achieved)? In other words, how did the hacker gain access to the IT system? If any disproportional actions were carried out for this purpose, e.g. as described in the Guidelines (p. 8 under 4.2.), this will not constitute 'ethical' hacking.
- Could the discloser have taken other possible actions? In other words, was the vulnerability immediately reported to the owner of the IT system or did the discloser fail to do so in order to erase his tracks or to manipulate, copy or delete data, for example? If any tracks were erased or data manipulated, copied or deleted, this will not constitute coordinated vulnerability disclosure.

As stated above, it may still be necessary to institute a criminal investigation first and to consider the discloser as a suspect, so that the questions above can be answered. In case of any doubt, the public prosecutor handling the case can consult the cybercrime officer at his or her public prosecutor's office or the Cybercrime Knowledge and Expertise Center at the National Public Prosecutor's Office. At a minimum, it is recommended that any considerations related to the above-mentioned framework should be entered into an official log for the purpose of explaining the decision to prosecute at the hearing.

Adoption

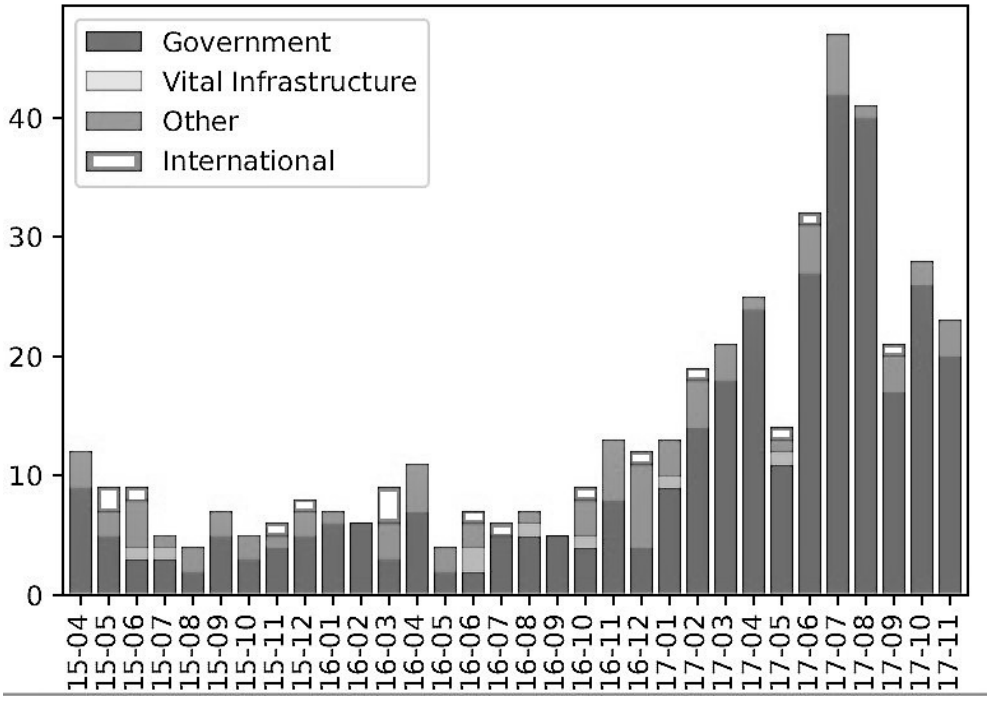
Many Dutch companies have taken the guidelines to heart and implemented coordinated vulnerability disclosure policies. In 2016, some of these companies took a step further by signing the Coordinated Vulnerability Disclosure Manifesto, in which they announce public reporting mechanisms on vulnerabilities in their ICT systems and call upon other organisations to do the same.

These efforts have been augmented by the Dutch government, which has also created a central point of contact to report vulnerabilities. Anyone who finds vulnerabilities in websites and digital infrastructure of the Dutch central government can report their findings there. Other governmental entities, such as provinces, municipalities, the Dutch Tax and Customs Administration and the Dutch Public Prosecution Services, have also created points of contact for reporting vulnerabilities.

Statistics

Since the publication of the coordinated vulnerability disclosure guidelines by the Dutch government in January 2013, it has not been possible to obtain accurate and up-to-date statistics on the number of reports filed because not all disclosures go through the NCSC. As mentioned earlier, however, a coordinated vulnerability disclosure procedure is principally a matter between an organisation and a discloser, and if all goes well, involvement of a third party is not necessary. The figure below provides an overview of notifications that the Dutch NCSC received. In some cases, these reports concerned vulnerabilities found in the NCSC's own systems. In other cases, the reports concern information systems of other government entities or private organisations operating critical infrastructures.

Figure 3. Number of reports submitted to the Dutch NCSC by concerned party, April 2015-November 2017



3.2.2. *Latvia*[*]

Current status of IT security and CVD in Latvia

As of the end of 2017, Latvia has taken several steps in the area of vulnerability disclosure and broader IT security, as follows:

- Some organisations have published their Responsible Disclosure Policy (RDP)/CVD policies, starting with Swedbank (2015), but others have also done so, e.g. CERT.LV.
- There have been many cases of CVD, most of which are coordinated by CERT.LV. In 2017, around 50 instances of vulnerabilities affecting Latvian websites or nationally developed software were reported. For example:
    - Several vulnerabilities were discovered in Latvian eID software. A full-scale CVD process was followed, at the end of which the information was published.
    - There have been cases of vulnerabilities found in the Riga city transport system, social network and e-banking. In those cases only some parts of the process have been implemented and the public was not always properly informed.
- Information technologies security Law has been in place since 2011. This law defined all IT security landscape elements, created the CERT.LV institution (Latvian national and governmental CSIRT), defined tasks and duties for CERT.LV, state institutions, local municipalities, IT critical infrastructure and ISPs. The law will be amended soon to implement the Directive on security of network and information systems (NIS) and include providers of essential services and digital services.
- The ministry responsible for IT security in Latvia is the Ministry of Defence.
- No particular legislation is in place for CVD. The only attempt to legalise CVD occurred in 2016, as described in detail below.
- Latvia's national cyber strategy is due to be renewed in 2018; CVD will be included in that strategy.

CVD in legislation

In 2016, the Ministry of Defence (MoD) proposed to address one problem of the RDP (Responsible Disclosure Policy)/CVD process via legislation. In particular, the proposal intended to specify the responsible disclosure process in the law on

[*] This section of the report was contributed by Baiba Kaskina, CERT Latvia and Chair TF-CSIRT.

IT security. And if a researcher/hacker would follow the specified RDP process, he would then receive a liability waiver for that particular vulnerability disclosure. This proposal attempted to address the problem that a researcher is not protected from being sued after s/he discovers the vulnerability and reports it to either the particular organisation or to a coordinating entity.

In Latvia, there is a legal system where only the law is relevant in the court. So it was not possible to follow the example of the Netherlands where policy on RDP/CVD cases is taken into account by the court.

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.

After long discussions, amendments were proposed in two laws:

1. *Criminal law.* In the articles related to attacks on automated data systems, it was proposed to add that liability is waived in the event that the attacker follows the responsible disclosure process (which is defined in the IT security law).
2. *IT security law.* The RDP process is thoroughly defined, including the obligations of researchers, CERT.LV, state institutions, local municipalities and critical infrastructure organisations. The RDP process would be applicable only to these groups and would exclude the private sector (where it would apply only to those entities that are recognised as Critical infrastructure providers).

Proposed approach in the IT security law

Main principles:

- Each stage of the RDP process (discovery, reporting, response, disclosure) has to be reflected in the law; each process must have a beginning and an end.
- Rules have to be precise and strict.
- Implementation has to be fair and effective.
- The RDP applies only to state institutions, local municipalities and CII providers.
- CERT.LV (or MilCERT for military networks) acts as the main coordinating entity.

Process:

- Independent researcher/hacker is obliged to follow the process if s/he wants to receive a waiver for liability.

  - S/he has to log his/her actions which led to the vulnerability disclosure.
  - To find the vulnerability, the researcher can gather only the minimal amount of data required for the discovery process (cause minimal possible damage). That is, if the vulnerability is found, no further probing is allowed.
  - Researcher has to inform CERT.LV (or MilCERT in case of military networks) within 5 days since the discovery.
- CERT.LV in such case:
  - Verifies whether the vulnerability is really there, as claimed.
  - Informs the researcher if the vulnerability is really there (true or false) and what will be the next actions.
  - If it is true, then CERT.LV informs the owner of the system explaining the problem and requesting it be fixed.
- Owner of the vulnerable system is obliged to:
  - Fix the vulnerability within 90 days. The term can be extended by CERT.LV to 180 days if there are sound reasons.
  - Inform CERT.LV when the system is fixed.
- After CERT.LV receives information from the owner of the vulnerable system, it:
  - Verifies whether the vulnerability is fixed and if it appears not to be fixed, the work continues with the system owner.
  - Informs the researcher, if the vulnerability is fixed.
- After receiving this information, the researcher can publish information about the vulnerability.

If the researcher has followed the above-described process, liability will be waived if the system owner at any point sues the researcher in court.

Issues in incorporating RDP/CVD into law

Latvia found it very difficult to specify many parts of the RDP in law. The issues and questions raised below illustrate some of these difficulties.

- When does the vulnerability discovery process start?
  - Immediately after discovery or a maximum of 5 days prior to submission of the report?
- How much information would a researcher be allowed to gather during this phase?
  - Causing minimal possible damage?

  - Gather only the minimum amount of data required for discovery process
- Legitimacy of methods and instruments
- Publishing information about the vulnerability
  - If it is published before the vulnerability is fixed – then the liability would not be waived.
  - How does that condition relate to freedom of speech?

It also should be noted that an obligation to fix a problem within 90-180 days works only for locally developed systems or websites. In cases where patching depends upon an external vendor, the person in charge of the system can do very little to fix the vulnerability, apart from using some mitigation techniques.

Failure to incorporate RDP/CVD in the law

The proposed amendments to these two laws (IT Security and Criminal Law) went to the cabinet of the Ministers, where they were approved, but objections were subsequently raised by the State police. The latter insisted on the creation of a register of researchers, which would have eliminated any possibility of anonymity, which is an essential feature of any such scheme. After long debates in the working group involving all parties, no solution was found, and the authors decided to drop the proposed initiative.

There were other objections to the proposal as well. The general fear was that these amendments in the law would enable anonymous hackers to hack state systems without the possibility of suing them. This demonstrated a lack of understanding about the general principles of the RDP/CVD process and would require extensive educational work in all layers.

The authors of the proposal admitted that its provisions were already very complicated and had it been implemented in the law, it would be quite difficult for researchers to follow the process.

Conclusions and the next steps

The authors of the proposal did not see this experience as a total defeat, but rather as a lesson that will be helpful in the next round of implementing CVD in the law. It is worth pointing out that the government approved the idea of introducing a CVD process into the law in general. The private sector in Latvia is also encouraged to have a CVD policy in place to raise awareness and understanding at various levels and to gather examples of good practices.

It is advised to take a different approach in the next iteration of the policy, in which CERT.LV is established as the *de facto* trusted party and made responsible for making many of the decisions. Also what constitutes

proportional and disproportional activities should be more precisely defined, and researchers' concerns about protecting their anonymity should be thoroughly addressed.

3.3. Case studies of CVD outside the EU

3.3.1. United States[*]

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 Internet Engineering Task Force (IEFT), which develops and promotes voluntary Internet standards noted that the issue had been "a divisive topic for years."[35] Security experts, industry leaders, and policy-makers 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 we all use. Fortunately, what was once a contentious area rife with conflict has seen an emerging consensus in the US, 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 government 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 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

[*] This section of the report was contributed by Allan Friedman, Director of Cybersecurity Initiatives at the National Telecommunications and Information Administration (NTIA), US Department of Commerce.

[35] https://tools.ietf.org/html/draft-christey-wysopal-vuln-disclosure-00.

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.[36]

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 criminalizes 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 help clarify what they meant.

Chaos and Contention

As the security community slowly grew in the early '00s, 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. Many remember when a major vendor physically cut out pages from the proceedings of a large conference, while others had friends or knew people who had been threatened with lawsuits or by law enforcement. There was real concern among the security community that vendors simply weren't taking software security as seriously as the researchers. For their part, vendors didn't 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.

---

[36] For a survey of this, see http://www.gwlr.org/wp-content/uploads/2016/11/84-Geo.-Wash.-L.-Rev.-1644.pdf.

Absent clear guidance, some security researchers worked to create their own broad policies. NMRC, a hacker collective, established their own policy in 1999 on disclosure with windows of one week or one month depending on severity.[37] 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.[38] This policy gave a two (later five) day window 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 criticized 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.[39] One low point in this period of distrust can be seen in 2009 by a presentation at the security conference CanSecWest proselytising 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.[40]

Collaboration and CVD

By the early 2010s, it was clear by many across 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 consumer protection agency Federal Trade Commission filed a complaint against mobile device manufacturer HTC for failing to employ "reasonable security."[41] While numerous lapses were alleged, the fifth of five charges was the failure "to

---

[37] https://www.nmrc.org/pub/advise/policy.txt.

[38] https://wiretrip.net/rfp/policy.html.

[39] For example, 5 different papers on the economics vulnerability discovery and disclosure were presented at 2004's Workshop on the Economics of Information Security at Harvard University, http://infosecon.net/workshop/schedule.php.

[40] https://threatpost.com/no-more-free-bugs-software-vendors-032309/72484/.

[41] https://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htccmpt.pdf.

implement a process for receiving and addressing security vulnerability reports from third-party researchers."

As the issue become more common, it became clear that the private sector could benefit from clarity. In 2015, the National Telecommunication and Information Administration (NTIA) in the 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."[42] This process brought together very diverse view points, while emphasizing that there was no one-size-fits-all solution. Participants in this process developed a template disclosure policy to make it easier for organizations 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.[43]

Other government agencies followed in quick order. In 2015, the FTC included vulnerability disclosure in the cybersecurity guide for businesses.[44] By the end of 2016, regulators like the Food and Drug Administration (FDA) and the National Highway Transportation and Safety Administration (NHTSA) highlighted CVD as an important part of cybersecurity guidance and best practices for medical devices[45] and modern vehicles.[46] 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

---

[42] https://www.ntia.doc.gov/blog/2015/enhancing-digital-economy-through-collaboration-vulnerability-research-disclosure.

[43] https://www.ntia.doc.gov/blog/2016/improving-cybersecurity-through-enhanced-vulnerability-disclosure.

[44] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[45] https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

[46] https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf.

systems. Then Secretary of Defence Ash Carter described it in common sense terms, as "a 'see something, say something' policy for the digital domain".[47]

As CVD practices spread across the American economy, the law had to catch up as well. In October of 2015, the United States Copyright Office recommended exemptions under the Digital Millennium Copyright Act (DMCA) for "good faith security research" on the computer systems that are built into voting machines, motorized land vehicles and implantable medical devices.[48] 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.[49]) 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 or 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 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 "authorized 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 organizations may have differing goals and priorities." CERT/CC still plays a role as a coordinator, but acting as a single neutral party hasn't 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

---

[47] https://www.defense.gov/News/News-Releases/News-Release-View/Article/1009956/dod-announces-digital-vulnerability-disclosure-policy-and-hack-the-army-kick-off/.

[48] https://www.copyright.gov/1201/2015/introduction-analysis.pdf.

[49] https://www.usatoday.com/story/tech/2017/07/30/hackers-defcon-conference-exploit-vulnerabilities-voting-machines/523639001/.

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 Draft 2 of the Cybersecurity Framework Version 1.1, which notes the importance of "processes… established to receive, analyse and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)".[50]

3.3.2. Japan[*]

In Japan, the coordinated disclosure of vulnerabilities in products such as software is performed in accordance with the "Information Security Early Warning Partnership Guideline" (herein "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 has been amended in 2014 and 2017. The notification was renamed "Standards for Handling Vulnerability-related Information of Software Products and Others" in 2017. The Guideline was created and jointly announced in cooperation with several industry organizations, Japan Electronics and Information Technology Industries Association (JEITA), Japan Information Technology Service Industry Association (JISA), Computer Software Association of Japan (CSAJ), 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, firmware, etc. will be within our scope.

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 for 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 1,504 advisories have been published on JVN as of 30 September 2017.

---

50 https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf.

[*] This section of the report was contributed by Uchiyama Takayuki, CERT Japan.

While this coordinated vulnerability disclosure process has worked fairly well over the years, the number of reports received has increased significantly over the past few years. Various reasons can be adduced for this increase, among them being an increase in overall awareness of security vulnerabilities, an increase in the number of researchers searching for vulnerabilities, increase in the number of products available, the availability of easy-to-use tools for vulnerability discovery, etc. The increase in reports has led to a process overflow where some reports are not being handled in a timely manner. Until very recently, the Guideline 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 still remain many 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:

- Incentives should be provided to researchers to report vulnerabilities to an organisation that can directly address the vulnerability or at the very least coordinate with an organisation that can address the vulnerability.
- Monetary incentives 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).
- Coordination process should be clarified so that researchers know how a reported vulnerability will be coordinated and disclosed.
- Vendors should be educated to create a coordination process so that researchers know vendors will address reported vulnerabilities.

4. LEGAL CHALLENGES FROM SOFTWARE VULNERABILITY DISCLOSURE IN THE EU*

4.1. Circumstances in which disclosure of software security vulnerability is advantageous

Past experience shows that software security vulnerability disclosure can indeed be a helpful means under specific circumstances for vendors to identify security issues in advance and thereby prevent exploitation of these vulnerabilities by hackers. If not properly handled, however, disclosure of software security vulnerabilities may give a window of opportunity to hackers to exploit the identified vulnerabilities before a patch is deployed. Therefore, the appropriate legal framework should exist that would allow discovery of software vulnerabilities under certain specifically prescribed circumstances, including complementary policy guidance for processes of coordinated disclosure of vulnerabilities.[51] This proposition is supported, among others, by the Council itself, which, in its 20 November 2017 Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, "welcome[d] the call to acknowledge the important role of third party security researchers in discovering vulnerabilities in existing products and services and call[ed] upon Member States to share best practices for coordinated vulnerability disclosure."[52]

Finally, policy-makers need to consider and address important questions when deciding on the changes required to the legal or policy framework to allow

---

* This chapter of the report was contributed by Andriani Ferti, Senior Associate, Karatzas & Partners law firm.

[51] ENISA has been the first to acknowledge the need for a clear legal framework allowing vulnerability reporting in the circumstances where it can be helpful to manufacturers to prevent widespread cybersecurity attacks. Indeed, in its Good Practice Guide on Vulnerability Disclosure, it stressed that "[o]ne of the primary challenges […] is the need for an advanced legal landscape to ensure that vulnerability reporting is not endangered by the unintended consequences of criminal and civil legislation" (p. 70).

[52] Council Conclusions on the Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU – Council conclusions (20 November 2017), Conclusion No. 27.

for coordinated vulnerability disclosure. Such questions involve defining at which point in time the disclosure should happen, what information should be disclosed, in what format and to whom this information should be disclosed. These questions arise especially in view of the number of stakeholders involved in this complex process, including the software vendors, independent researchers, governments and actual users, but also the general public.

4.2. Legal challenges in relation to software vulnerability disclosure and the relevant legislative framework

As acknowledged in the Good Practice Guide on Vulnerability Disclosure of ENISA, there are numerous pressing legal challenges associated with the vulnerability disclosure process as "[i]ndividuals who discover a vulnerability often face legal threats when they decide to report it. These threats can have implications on not only civil and criminal law, but also contract law, licensing, patent law and other types of legislation."[53]

This section sets out the legal issues that arise in the context of software security vulnerability disclosure. These issues cover (as also acknowledged in the ENISA Practice Guide) various areas of law ranging from industrial and intellectual property (including copyright, trade secrets, patents and trademark law) to export control regulation and data protection law, as well as criminal law.

4.3. Criminal law

There are two questions when looking into security research for software vulnerabilities which refers to the process of finding vulnerabilities as opposed to reporting them, from a criminal law perspective. 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 an information system. The second one is a procedural one and relates to the conditions that need to be met for any crimes associated with finding vulnerabilities to be prosecuted.

The relevant legislative instruments in the EU are: i) the 2001 Council of Europe Convention on cybercrime (**Cybercrime Convention**), ii) Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (the **Cybercrime Directive**) and iii) any relevant national legislation in Member States across EU

[53] ENISA, "Good Practice Guide on Vulnerability Disclosure – From challenges to recommendations", January 2016, p. 7.

(including the national legislation transposing the Cybercrime Directive), and in particular the provisions concerning illegal access to information systems.

Article 2 of the Cybercrime Convention provides what constitutes illegal access to an information system and stipulates: "[e]ach 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." That means that four conditions need to be met for illegal access to apply under the Cybercrime Convention: i) the person should have accessed the system intentionally, ii) that person should have actually had access to the computer system, iii) that access should concern either the whole or part of the computer system and iv) that person should have no right to access the system. The Convention allows countries that are signatory parties to it to require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

The Cybercrime Directive very much reflects the Cybercrime Convention in relation to what constitutes illegal access to an information system. In particular, in its Article 3 the Directive provides that Member States are required to adopt legislative measures "to ensure that, when committed intentionally, the access without right, to the whole or to any part of an information system, is punishable as a criminal offence where committed by infringing a security measure, at least for cases which are not minor". The Directive sets minimum protection to be afforded by Member States (i.e. Member States can introduce stricter requirements). In light of this, under the Cybercrime Directive, there are five conditions that need to be met: i) the person should have accessed the system intentionally, ii) he should have actually accessed the information system, iii) in whole or in part, iv) without any right, and v) he should have accessed the system (at least in major cases) by infringing a security measure.

Nonetheless, as can be understood from the above, especially given that the Directive affords only a minimum level of protection, Member States have adopted varying interpretations of what constitutes illegal access (i.e. hacking), and which varies significantly. For example, in the Netherlands, illegal access would be considered purposefully and unlawfully entering an automated system by breaching security measures (e.g. by means of technical interference, false signals/false keys, or assuming a false identity). In a similar vein, the Greek definition of illegal access reflects the Cybercrime Directive. On the other hand, in Belgium, hacking/illegal access is interpreted broadly, and there is no need to show that security measures have been breached, or that the person has accessed the software system without the right to do so. The case is similar in

Germany, where there is neither a need to show that security measures have been breached nor to show unlawfulness.

Having examined what constitutes illegal access, it is key to understand the notion of ethical hacking, because it is central to security research for software vulnerabilities. Whereas CVD is about how software vulnerabilities are reported, how vendors respond and how disclosure is coordinated, in essence, security research can be the result of ethical hacking as the latter refers to the act of identifying weaknesses and vulnerabilities of information systems by duplicating the intent and actions of malicious hackers. Nonetheless, even though ethical hacking is also cited by the policy documents in place in countries where a robust legal/policy framework has been set for vulnerability disclosure, such as Netherlands, the notion does not exist as such in criminal law. This is explicitly confirmed in the letter sent by the Dutch Public Prosecutor to all its departments in relation to vulnerability disclosure.

But how did the Dutch Prosecutor ensure therefore that security research is in compliance with criminal law in view of the absence of the notion of ethical hacking in the law? To that effect the Dutch prosecutor provided for three principles in accordance with which one can establish the lawfulness of the relevant acts. These three principles relate namely to: i) the motives of the researcher, ii) subsidiarity and iii) proportionality. First, the relevant department would need to examine the motives of the researchers and whether or not these are ethical. Second, the actions of the researcher after he discovers a vulnerability will be considered. For example, in any legal analysis, it should be considered whether the researcher disclosed the vulnerability once he discovered it. Finally, if the researcher – either intentionally or unintentionally – ends up doing more (such as copying sensitive data or personally identifying information) than merely accessing the system, and discovering the vulnerability, the prosecutor will probably launch a criminal investigation.

The question therefore arises whether the Dutch Prosecutor's reasoning in relation to vulnerability disclosure could also be implemented in other member states. The brief answer is that in view of the divergent transposition of Article 3 of the Cybercrime Directive and the fact that the requirements to show illegal access vary across the 28 different jurisdictions, the Dutch example cannot necessarily be implemented in other member states as such. In particular, unlawfulness is a key element to show illegal access in the Netherlands, and it is the element the Dutch Prosecutor used as a basis to develop his reasoning as to when vulnerability disclosure can be legitimate. Nonetheless, unlawfulness has not been incorporated in all 28 jurisdictions across the European Union. It is important, to note that in criminal law there is a general principle (also acknowledged in the European Commission Report addressing the transposition of the Cybercrime Directive) that there should be no criminal

liability for whatever action if this action is carried out with according rights. Therefore, even if unlawfulness is not incorporated in all 28 jurisdictions, there could be a potential workaround referring to general principles of criminal law.

Across the European Union, criminal prosecution in most cases takes place *ex officio*, which means that there is no need for a complaint in order for the public prosecutor to prosecute, unless otherwise provided by law. In fact, if a crime can only be prosecuted upon a complaint by the victim, the law will explicitly provide for this. Therefore, in most jurisdictions examined, such as, for example, Italy, the Netherlands, Belgium and Malta, given that the law does not provide otherwise, illegal access to a computer system can be prosecuted *ex officio*. The situation is different although in a limited number of member states, for example, in Germany and Greece where the law explicitly provides that illegal access to a computer system is only prosecuted following a complaint by the victim.

Under Dutch law, illegal access is prosecuted *ex officio*. The question therefore arises how the Dutch prosecutor has been able to provide guidelines as to when security research constitutes illegal access, and allow for it to be prosecuted only under specific circumstances. In the Netherlands, the public prosecutor has the right to exercise prosecutorial discretion (*opportuniteitsbeginsel*). In a similar vein, in the UK, the Crown Prosecution Service has wide discretion in deciding when to prosecute. In order to do so, the Crown Prosecution Service should *inter alia* show that it is in the public interest to prosecute. There are guidelines that clarify the meaning of "public interest", which among others provide that the Crown Prosecution Service will not prosecute *bona fide* security researchers even though it is considered a crime under the Computer Misuse Act to possess hacking tools. In other countries, such as France, while no prosecutorial discretion exists *per se*, there may be other ways to exercise discretion (e.g. the case of *mediation penale* in France). Finally, of course as a general principle in criminal law normally, if there is lack of evidence, the prosecutor would not be able to pursue the prosecution. Needless to say, however, while this issue of when to prosecute CVD arises in jurisdictions that illegal access is prosecute *ex officio,* in the case of member states where a complaint by the victim is required (e.g. Germany and Greece), the adoption of the policy such as the letter sent by the Dutch prosecutor on security research would of course be helpful guidance, but not necessary.

Having examined a number of jurisdictions in terms of how they address vulnerability disclosure, it is worth mentioning the example of France where the legislature explicitly provides for the non-prosecution of a researcher who reveals a vulnerability to ANSSI (see Art. L. 2321-4 of the 2016 *Loi pour République Numérique*). The law, however, is quite detailed about how ANSSI acts upon

receipt of the information, and how it transmits this to the owner or the manufacturer of the information system.

Finally, there is an important consideration when looking into the criminal law aspects of vulnerability disclosure. This consideration relates to the cross-border nature of hacking given that there are no geographic silos as to where the researcher is located, and where he identifies the vulnerability. For example, security research may concern a computer system in the Netherlands, but the researcher may be located in Belgium. As a result, the researcher may be subject to the laws of both jurisdictions, and the question is (which unfortunately is pretty much left open) how to address the legal conundrum this creates as the researcher may not be subject to prosecution in the Netherlands, but s/he may be in Belgium. This consideration creates even further legal uncertainty, which when addressing security research should be taken into account as part of coordinated vulnerability disclosure.

In sum, having examined the criminal law aspects of security research, one cannot but acknowledge that the positive example of the Dutch model underscores the importance of improving legal certainty among all the stakeholders involved and encouraging positive behaviour for coordinated vulnerability disclosure. However, even though in certain member states the legal validity of policies like those in the Netherlands may be able to stand (also and most importantly, in court), it is questionable how such policies would have a practical impact in the remaining jurisdictions where such policy documents would not be accepted in the judicial system. In addition, it goes without saying that even in the cases where a jurisdiction is involved where such policies would be meaningful (such as, for example, the Netherlands), if one must deal with other jurisdictions where the conditions for prosecuting illegal access (and therefore security research) are more stringent, then questions arise as to whether the researcher in question can avoid prosecution at all. It can therefore be easily concluded that member states need to coordinate closely as a step towards enhancing legal certainty as to the circumstances under which security research is prosecuted and vulnerability disclosure is coordinated. Sharing best practices is a first step, but it is important also to identify ways better to harmonise the applicable law at EU level (e.g. by considering potential changes to the cybercrime Directive, which has already been transposed in a very different manner in each of the member states).

4.4. Data protection law

Having discussed the criminal aspects of security research and software vulnerability disclosure we now turn to the civil aspects and other legal challenges that arise. As to data protection legislation, unlawful processing of

personally identifiable information is prohibited. Given the broad meaning of processing under EU legislation (and also under the most recently adopted and soon to come into force General Data Protection Regulation (GDPR), security research may be illegal to the extent that the researcher who engages in security research also accesses personal data of the users stored in the relevant information system. CVD may include the processing of that personal data. Nonetheless, CVD can also help mitigate data protection and data security risks, and in fact is one of the good practices encouraged by data protection and other competent authorities as a means to promote compliance with GDPR. Indeed, the GDPR provides for a principles-based approach to data security, in which case encouraging CVD would actually be in compliance with the relevant legislation.

4.5. Industrial property

4.5.1. Copyright

Another area of concern that mainly governs the relationship between the researcher and the software vendor is that of copyright law. In fact, researchers may be faced with claims that the information being disclosed includes portion of software code, and thus infringes the vendor's copyright. In addition, under certain circumstances activities of the researchers engaging in security vulnerability disclosure may interfere with copyright holders' right to prevent circumvention of digital rights management (DRM) technology applied on the software.

The existing exemptions under EU copyright law (i.e. Directive 2009/24/EC), such as those concerning the reproduction of the code and translation of the form for the purposes of achieving interoperability (i.e. reverse engineering), may not be applicable, especially because information obtained through this reverse engineering can only be used for interoperability purposes. Similarly, even if there is an exemption to use a copy of a software programme in order to observe, study or test its functioning to determine its ideas and principles, if security vulnerability disclosure involves reproduction, then engaging in any similar activity would not be permitted by EU copyright law. In the context of multiple finders or a feedback loop between finder and a reporting authority before official disclosure, the protection of copyright could prevent sharing vulnerability information from anyone other than the original vendor, thus making CVD legally challenging. It is worth noting that while in the United States, there is a security testing exemption provided in the Digital Millennium Copyright Act (DMCA), there is no such thing in EU law. Nonetheless, academics even in the US consider that exemption for security

testing narrow and call for legal reforms to expand it to cover security vulnerability disclosure.

4.5.2. Trade secrets

On a number of occasions, independent researchers – especially those who may have previously worked for the vendor in question as an employee or consultant – may face trade-secret infringement claims. In those circumstances, the software vendor can possibly claim that his prior knowledge led him to his discovery, and therefore easily prove that there has been a trade secret infringement.

The recently adopted trade secrets Directive does provide for a reverse engineering exemption as a means leading to lawful acquisition of trade secrets. This exemption though can be restricted in the End User Licence Agreement (EULA), which makes it less likely to apply in the case of security vulnerability disclosure.

4.5.3. Patents

While for the purposes of this report we will not enter into a debate as to when computer-implemented inventions can be patentable in the EU, in the case where such an argument can stand, a researcher may be pursued on the basis of patent infringement.

The existing law does not provide for an exemption that would be applicable in the circumstances we are looking at. On this point, it is worth noting that the aborted draft computer-implemented inventions Directive in the early 2000s included an exemption for reverse engineering for interoperability purposes.

4.5.4. Trademarks

Even though they are less likely to prevail, it is true that under certain circumstances and given that a researcher may use a trademark for making a security vulnerability disclosure, s/he may be faced with a possibly legal claim that disclosure infringes on their trademarks. The researcher, however, can easily combat such claims by arguing that the use of the trademark is necessary to make the disclosure and there is no intention to confuse the consumers.

4.6. Export control regulation

Finally, under export control regulation, and in particular the Wassenaar Arrangement, a company wishing to sell "intrusion software" abroad needs to obtain a government license to export those items. Until recently, it was an open

question as to the scope of this requirement, especially with respect to bug bounty programs and to zero-day exploits. In December 2017, however, a number of changes were made to the relevant part of the Arrangement to ensure only "software specially designed for command and control" of intrusion would be subject to export controls, and adding exemptions *inter alia* for software that carries out updates authorised by the owner or operator of the system, and explicitly to vulnerability disclosure or cyber incident response activities. The relevant EU legislation is currently being reviewed by the European Parliament and the Council based on a European Commission proposal presented in September 2016, and it remains to be seen if and how the recent changes to the Wassenaar Arrangement will impact the decision-making at EU level.

4.7. Conclusion

In sum, and having examined the legal challenges associated with security research and vulnerability disclosure, there are a number of open questions as to how to improve legal certainty with respect to the circumstances under which security research and vulnerability disclosure can be unlawful. Based on previous experience, policy changes may be more fruitful at least in the shorter term, but it is important to consider potential legal vehicles that could allow for security research to feed into a process of Coordinated Vulnerability Disclosure, provided that certain conditions are met. It does indeed require some fine-tuning, with the aim of clearly defining any proposed exemptions (even, for example, in copyright law) to ensure that such exemptions are not misused by researchers, but also to provide some sort of "safe harbour" to the researcher. Therefore, any proposals should be handled with care.

5. POLICY IMPLICATIONS

The analysis of this Task Force shows that only a few countries across Europe have managed to put SVD processes in place. The Netherlands has been the most proactive member state in establishing vulnerability disclosure policies and has supported other member states to address their challenges and concerns. Supported by the Dutch Ministry of Justice and Security and the Public Prosecution Service, which supports and advocates this process, the government has a proper framework in place, as well as clear processes for reporting vulnerabilities, including protection of the researcher. France has recently included vulnerability disclosure in its revised legislative framework – Law for a Digital Republic (Article 47) – even though it still lacks proper protection of the researcher. According to recent reports, Lithuania has joined these ranks by putting in place a vulnerability disclosure framework for a specific sector ("providers of public communications networks"), including a disclosure deadline, scheduled resolution and an acknowledgement report. In addition, some organisations in Lithuania have successfully established processes to receive and disseminate vulnerability information.

A significant barrier to the implementation of CVD policies across the EU is the lack of a single interpretation of what constitutes 'hacking' among the member states, which has led to the conflation of this term – typically associated with cybercrime in the EU – with security research and its role in vulnerability discovery as opposed to vulnerability disclosure. Therefore, the first step is to provide the necessary legal certainty to security researchers involved in vulnerability discovery as well as setting appropriate vulnerability disclosure processes through complementary guidance and best practices. Based on current best practices in Europe, the US and Japan, the Task Force recommends implementation of the following CVD-related policies.

CVD Policy

The Task Force calls upon the European Commission and the member states to collectively draft a European-level framework complemented by national legislation in accordance with the guidelines and recommendations defined in ISO/IEC 29147:2014 and ISO/IEC 30111 in order to provide legal clarity for software vulnerability discovery and disclosure. The Nationaal Cyber Security Centrum (NCSC) in the Netherlands has published a general guideline for responsible disclosure, *which can serve as a useful model that EU member states can*

follow in drafting their own responsible disclosure policy. In addition, it gives reporters guidance on how to act in finding and reporting a vulnerability.[54]

The Coordinated Vulnerability Disclosure Template from the National Telecommunications and Information Administration (NTIA) of the US Department of Commerce could also offer helpful suggestions.[55]

It's also worth mentioning that the Cybersecurity Unit, Computer Crime and Intellectual Property Section Criminal Division of the US Department of Justice, in July 2017 released the first version of the framework for a "Vulnerability Disclosure Program for Online Systems"[56] that EU member states could examine as a possible model. Recognising that different organisations may have different goals and priorities for their vulnerability disclosure programs, the US framework does not dictate the form of or objectives for vulnerability disclosure. Instead, the framework outlines a process for designing a vulnerability disclosure programme that will clearly describe authorised vulnerability disclosure and discovery behaviour, thereby substantially reducing the likelihood that such described activities will result in a civil or criminal violation of law.

The Task Force recommends that national CERTs (computer emergency response teams) should put in place frameworks that are similar to the ones adopted in the Netherlands and the US. Moreover, such frameworks should be prominently announced on the websites of organisations that establish a CVD, which researchers can consult and rely on for legal certainty.

The Task Force suggests the steps outlined below for implementing coordinated vulnerability disclosure processes in Europe.

Private sector

The private sector could take the lead in implementing coordinated vulnerability disclosure defining and publishing on companies' website public reporting mechanisms on vulnerabilities disclosure according to the ISO standards. The Netherlands Responsible Disclosure Guidelines, the NTIA template and the DOJ Vulnerability disclosure programs could also be followed as best practices.

---

[54] See https://www.ncsc.nl/english/current-topics/news/responsible-disclosure-guideline.html.

[55] See https://www.ntia.doc.gov/files/ntia/publications/ntia_vuln_disclosure_early_stage_template.pdf.

[56] See https://www.justice.gov/criminal-ccips/page/file/983996/download.

CERTs

CERTs should help in putting in place a framework to implement coordinated vulnerability disclosure processes playing the role of thrusted third party and coordination center in this process.

Member states

Member states should act in creating the necessary legal certainty for security researchers involved in vulnerability discovery, changing national legislation to allow for the recognition of ethical hacking.

EU

The EU should change the European legislation to allow for legal certainty for 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.

6. RECOMMENDATIONS FOR IMPLEMENTING CVD IN EUROPE

6.1. Introduction

There is a need to improve legal certainty surrounding CVD within the EU. ENISA's "Good Practice Guide on Vulnerability Disclosure", from January 2016, states: "One of the primary challenges […] is the need for an advanced legal landscape to ensure that vulnerability reporting is not endangered by the unintended consequences of criminal and civil legislation."

Moreover, there is also a lack of coordination between member states on their respective positions with respect to CVD (see differences in the transposition of Directive 2013/40), while sharing best practices is key to ensuring legal certainty. However, a number of member states and third countries are working on national solutions that could result in conflicting obligations for service providers. The current system is fragmented and generates legal uncertainty for all parties concerned: service providers, law enforcement and judicial authorities and also EU citizens.

6.1.1. Opportunity cost

Currently, there are many interpretations across Europe of what constitutes hacking, let alone ethical hacking. Given that the principle of territoriality does not apply to cyberspace, if the EU institutions do not try and harmonise this field, then Europe may end up in a situation in which its cybersecurity researchers suffer from a lack of legal protection. As a consequence, companies in certain countries will find that such researchers will not help them with CVD and vulnerabilities will go unreported, harming the Digital Single Market.

6.1.2. What can be done at EU level?

While the approach to CVD by member states is fragmented and needs harmonisation at EU level, the debate about how and to what extent to harmonise CVD is mostly absent. On the other hand, at this particular moment, early 2018, there are several pieces of cybersecurity-related legislation that are either in discussion in the EP and the Council (e.g. the EU Cybersecurity Act) or being transposed into national legislation (e.g. the NIS Directive). Therefore, CVD-related legislation may be integrated in the above in such a way that cybersecurity is enhanced in Europe. We give our recommendations below on how the EU legislative momentum might be used to promote CVD in a coherent

manner. One clear advantage of using this approach is that their legal bases are already established.

6.2. EU legislation

6.2.1. Amending Directive 2013/40/EU on attacks against information systems ("EU cybercrime Directive") to support CVD

In the context of a potential future revision of the EU cybercrime Directive, the European Commission should consider an amendment to the Directive that would allow for CVD if certain circumstances prescribed by law are met, thereby creating a safe environment for security researchers community to report vulnerabilities that they identify. Such an amendment would ensure a more harmonized interpretation of the relevant rules across the EU, and the security researcher community would have a clearer idea of what constitutes or not an infringement of the relevant laws.

6.2.2. Protection of security researchers

Researchers involved in vulnerability discovery are often exposed to criminal or civil liability.[57] The Task Force notes that there is no legal instrument at the European-level aimed at protecting security researchers and "white-hat hackers" from prosecution as part of vulnerability disclosure. Given the importance of their work to the overall security of society, the legal liability and responsibilities of security researchers should be fully clarified to enable them to continue their work without fear of prosecution.

6.2.3. Incentives for security researchers

This Task Force would welcome appropriate policies aimed at encouraging 'white-hat hackers' to actively participate in coordinated vulnerability disclosure programs. No policy on this specific matter has yet been established at the EU level.

6.2.4. Directive on security of network information systems

Member states are currently developing their accompanying guidelines on the "technical and organisational measures" prescribed in Article 14 and falling with the scope of the NIS Directive. In this respect, a recent new draft of the NIST Cybersecurity Framework could be used as inspiration, as it includes the following subcategory of CVD: "RS.AN-5: Processes are established to receive,

[57] See https://techcrunch.com/2017/07/25/hungarian-hacker-arrested-for-pressing-f12/.

analyse and respond to vulnerabilities disclosed to the organisation from internal and external sources (e.g. internal testing, security bulletins, or security researchers)". Therefore, in transposing the NIS Directive, and in particular its Article 14, member states may explicitly consider including CVD as one of those measures.

Furthermore, companies may proactively consider establishing a CVD as part of their own "technical and organisational measures", since the NIS Directive leaves open the range of measures a company can take in order to ensure compliance with Article 14.

Moreover, in a future review of the NIS Directive, member states could be encouraged to share information and best practices among themselves on CVD. In a similar vein, promoting CVD could be considered as an explicit objective on the part of member states when defining their national strategy on the security of network and information systems as provided in Article 7 of the NIS Directive. However, given the difficulties in fine-tuning the scope of CVD-related legislative proposals (as mentioned in the section of this report concerning the legal challenges), the legislature should be cautious in putting forward such proposals, and make sure their provisions are clearly spelled out.

6.2.5. General Data Protection Regulation

The General Data Protection Regulation, which came into force in May 2018, offers some relevant points that could serve as vehicles to stimulate software vulnerability discovery and disclosure. According to the GDPR, software owners, vendors and tech firms become data controllers insofar as they process personal data within their systems. Assuming 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.

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 paragraph 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 programme 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.

Furthermore, with respect to the open question as to if and when CVD may constitute unlawful processing of personal data, it is worth referring to recital 49, which seems to suggest that researchers may potentially be able to argue that to the extent they disclose such activities to the data controller in the context of CVD, such disclosure may fall within the scope of a legitimate interest

of the controller in preventing security breaches by fostering network and information security. It would therefore then be up to the data controller to demonstrate that CVD was implemented with the intention of ensuring a higher level of network and information security, thereby serving its legitimate interest.

6.2.6. Cybersecurity Act

According to the proposed Regulation submitted by the European Commission in October 2017 concerning the European Network and Information Security Agency (ENISA) and cybersecurity certification (the Cybersecurity Act), in its coordination and capacity-building roles, ENISA can contribute to the harmonised development of CVD in the EU by having its mandate amended, thereby allowing it to engage in the following activities:

- Writing EU-wide guidelines for the reporting process, addressing the issues it raised in its January 2017 "Good Practice Guide on Vulnerability Disclosure" report;[58]
- Installing and operating a web portal where disclosure of software and hardware vulnerabilities can be coordinated at the European-level and contributed to anonymously. In the portal back-office ENISA would analyse the vulnerability, contact the owner/vendor/manufacturer of the software solution or hardware product, make sure that the vulnerability is safely patched, and keep a confidential record of all operations, in close coordination with ISACs (Information Sharing and Analysis Centers), CSIRTs (Computer Security Incident Response Teams), and the CSIRT network, for which it provides the secretariat. An 'assurance' seal for owners/vendors/manufacturers could be explored.
- Building a team of "white-hat hackers" who would conduct campaigns to assist EU member states and operators of essential services to mitigate software vulnerabilities, with the objective of increasing the security of all infrastructures;
- Implementing training in all issues that may arise in the context of CVD, e.g. technical, legal, etc., to build capacity on CVD in the EU; and
- Liaising formally with other key international actors on CVD in order to enhance cooperation, collaboration and the sharing of best practices.

Furthermore, **Article 47 (1)j of the Cybersecurity Act** states that a European cybersecurity certification scheme is expected to include *inter alia* "rules concerning how previously undetected cybersecurity vulnerabilities in ICT products and services are to be reported and dealt with." This provision of the Cybersecurity Act provides the possibility to introduce CVD in a European

[58] See https://www.enisa.europa.eu/publications/vulnerability-disclosure.

Cybersecurity Certification Scheme, which in fact may encourage CVD as a good practice. In addition, the scope of the Cybersecurity Certification Framework could explicitly cover the certification of processes that qualify as good practices in overall cybersecurity risk management, for instance as secondary guidance. In this manner, companies could be encouraged to deploy Coordinated Vulnerability Disclosure policies and have them certified.

6.2.7. Software vulnerabilities in durable goods such as cars and medical devices

The Commission should amend the Radio Equipment Directive so that article 3 paragraph 3 provides that "radio equipment is cybersecure by design, by default and by implementation". The Commission should incorporate the standards for vulnerability management (ISO 29174, 30111) directly into the CE mark system.

6.3. National legislation

Amending national legislation to support CVD. As a medium-to-long term solution and given that the revision of the EU cybercrime Directive (from 2013) may take several years, the Task Force recommends member states to consider amending their national legislation bearing on CVD, using the framework on CVD introduced in the Netherlands as a model. The Task Force acknowledges that such a recommendation may lead to certain discrepancies in the regulatory framework covering CVD across member states, but it would allow for the establishment of a safer environment for the security research community to report vulnerabilities until legislation addressing the relevant issues to a sufficient degree comes into effect at the EU level.

6.4. National non-legislative activities

Member states can also take direct action to support and enable CVD practices outside of legislation. One of the key challenges in the ecosystem is fostering awareness and adoption of good practices. At the end of the day, most software and systems are developed and maintained by the private sector. Relevant government agencies—or even regional governments—can highlight the importance of CVD as part of a cybersecurity risk program, and share documents to make it easier and cheaper for organisations to experiment with finding approaches that are fit for purpose. The examples cited above from the Dutch and US model aimed at awareness and adoption could be a good model.

Another issue concerns the legal question of CVD, as it pertains to anti-hacking statutes. Agencies focused on justice and law enforcement can offer guidance, either in formal opinions and policies, or more flexible guidance documents.

Leaders in the private sector can also play a role in helping their peers understand the value of CVD, and the path towards maturity. This could be an ideal project for emerging public-private partnerships: it is relatively lightweight, and requires relatively little investment, allowing for these efforts to demonstrate their value to both government and industry stakeholders.

6.5. Framework programmes for research and innovation

The Framework Programs for Research and Technological Development, also called Framework Programmes or abbreviated FP1 to FP7 with FP8 being named Horizon 2020, are funding programs created by the European Union/European Commission to support and foster research in the European Research Area. The specific objectives and actions vary between funding periods. In FP6 and FP7 (2002-2013) focus was still on technological research, in Horizon 2020 (2014-2020) the focus is on innovation, delivering economic growth faster and delivering solutions to end users that are often governmental agencies. The proposal for a Framework Programme 9 is currently being drafted by the European Commission and should be submitted for co-decision in the spring 2018.

There are several ways to leverage funding from these programmes to promote CVD among public and private researchers in Europe. For instance, the following H2020 calls described in the Work Programme 2018-2020 could be used to finance research and innovation in this area:

- SU-ICT-03-2018: Establishing and operating a pilot project to create a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap. The networks of competence centres could be used to put in place multidisciplinary consortia that would experiment with CVD under the framework of the project and come up with sound legislative recommendations as part of the roadmap to be delivered.
- SU-DS02-2020: Management of cyber-attacks and other risks. This topic is not yet defined and will be the subject of a later amendment to the Work Program, where explicit mention to CVD could be introduced.
- SU-DS03-2019-2020: Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises. The Work Programme already states that "The proposals should develop targeted, user-friendly

and cost-effective solutions enabling SMEs & MEs to: i) dynamically monitor, forecast and assess their security, privacy and personal data protection risks55; ii) become more aware of vulnerabilities, attacks and risks that influence their business; iii) manage and forecast their security, privacy and personal data protection risks in an easy and affordable way;…".

- SU-DS04-2018-2020: Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches. The Work Programme already states that "The proposals shall implement the following series of activities to make the electric system cyber secure: (i) assessing vulnerabilities and threats of the system in a collaborative manner (involving all stakeholders in the energy components provision supply chain)…".
- SU-DS05-2018-2019: Digital security, privacy, data protection and accountability in critical sectors. The Work Programme already states that "(1): In collaboration with all stakeholders in the healthcare ecosystem and CERTs/CSIRTs, develop dynamic vulnerability data basis for collecting, uploading, maintaining, and disseminating vulnerabilities of ICT-based medical systems, technologies, applications and services (enhancing the ICT generic ones e.g. NIST, MITRE)…".

The next Framework Programme for Research and Innovation, FP 9, could also carry explicit funding for CVD across Europe.

PART II
GOVERNMENT DISCLOSURE DECISION PROCESSES

7. GOVERNMENT DISCLOSURE DECISION PROCESSES

Governments learn about vulnerabilities in many ways: through their own research and development, by purchasing them, through intelligence work, or by reports from third parties. While vulnerabilities are the cause of significant security risks and harms to users, businesses, and even governments themselves, these same weaknesses can be exploited for law enforcement investigations, intelligence collection, and 'offensive' exploitation. The policies and practices to assess the risks and interests associated with disclosing a vulnerability immediately to the affected vendor(s) and/or manufacturer(s) or whether to delay disclosure will be referred to as a government vulnerability disclosure review process. Regardless of the timing of disclosure, when a government decides to disclose a vulnerability, that is when the process and norms of Coordinated Vulnerability Disclosure (CVD) begins (discussed in detail above).

When considering policies and practices concerning how governments make decisions about vulnerabilities, it is useful to distinguish between three areas of policy:

1) Acquisition - how governments acquire knowledge about vulnerabilities
2) Disclosure - how governments make decisions about how and whether to disclose a vulnerability immediately or to delay disclosure
3) Exploitation - how governments may use vulnerabilities for operational or offensive purposes

Government disclosure decision processes (GDDP), the topic of this chapter, address only this second area of policies, practices and disclosure. It is critical for governments to have robust, accountable and transparent policies in place in this area in order for companies and users to have trust and confidence that governments are responsibly managing any vulnerabilities that they learn about.

Disclosing these vulnerabilities to affected vendors and manufacturers allows companies to:

- patch them quickly;
- increase the security, privacy, and safety of their systems and users;
- reduce conflict and improve trust between companies and government; and

- benefit from external discovery of vulnerabilities in their products and systems that they may not otherwise have the resources to find, which is especially important for small- and medium-sized enterprises.

Some governments have created inter-ministerial government vulnerability disclosure review processes to consider all of the relevant risks and interests associated with the decision whether to disclose a vulnerability that is not publicly known immediately to the appropriate vendor(s) or to delay disclosure. The US Government has the most extensively documented and, as far as we know, most robust government vulnerability disclosure review process in place (discussed in detail below).

7.1. GDDP in Europe

While the Task Force found evidence of practices and implemented models for coordinated vulnerabilities disclosure (CVD) in Europe, it is believed that only a few member states have GDDP in place. Germany is publicly discussing implementing a process, and the Netherlands and the UK have processes in some form or another. In practice, the only public information available to date on this process is the vulnerabilities equities process (VEP) in the US, which therefore becomes the reference model for any discussion about these activities.

7.2. The US experience with GDDP

The US Government's process for reviewing and coordinating the disclosure of vulnerabilities that come to its attention is known as the Vulnerabilities Equities Process (VEP).

History

The origins of the VEP can be traced to the National Security Policy Directive 54, signed by President George W. Bush in 2008. The process was finalised in a document dated February 2010, but was not broadly or consistently implemented until April 2014, following the revelations of the Heartbleed vulnerability which is estimated to have affected two-thirds of the world's web servers. At that time, the White House Cybersecurity Coordinator Michael Daniel announced in a blog post that he had "reinvigorated" the VEP. At this time, the VEP became operational. In November 2017, current White House Cybersecurity Coordinator Rob Joyce announced a new charter for the VEP, including many reforms to the process. For a full history of the VEP, see Annex 2.

Mandate

According to the 2017 VEP Charter:

> The Vulnerabilities Equities Process (VEP) balances whether to disseminate vulnerability information to the vendor/supplier in the expectation that it will be patched, or to temporarily restrict the knowledge of the vulnerability to the USG, and potentially other partners, so that it can be used for national security and law enforcement purposes, such as intelligence collection, military operations, and/or counterintelligence… In the vast majority of cases, responsibly disclosing a newly discovered vulnerability is clearly in the national interest.

Notably, both the 2010 VEP Document and the 2017 VEP Charter have a presumption that most vulnerabilities will be disclosed immediately to the affected vendors and manufacturers, and that the government may only temporarily restrict knowledge of a vulnerability; this process is not intended to allow the government to permanently withhold disclosure.

Options

The 2017 VEP Charter contemplates several options available to the government when reviewing a vulnerability that comes to the government's attention:

- Full disclosure to the affected vendor(s) or manufacturer(s)
- Disseminating mitigation information to certain entities without disclosing the particular vulnerability
- Limiting use of the vulnerability by the US Government in some way
- Informing US and allied government entities of the vulnerability at a classified level
- Using indirect means to inform the vendor(s) or manufacturer(s) of the vulnerability
- Other methods not specified

Scope

The 2017 VEP Charter makes clear that all parts of government (including government contractors) must submit vulnerabilities that they learn about to the VEP, and that the VEP applies to vulnerabilities in virtually all products and systems:

> This policy applies to all USG components and personnel (i.e. civilian, military and contractors) and includes Government off-the-shelf (GOTS), Commercial off-the-shelf (COTS), or other commercial information systems (to include open-source software), Industrial

> Control Systems (ICS) or products, and associated systems such as Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS).

The 2017 VEP Charter further notes that this process is not intended to prevent US Government entities from taking immediate actions to protect its network(s) or warn entities actively threatened by a malicious cyber event, including ongoing unauthorised access to information systems.

Membership

In an effort to properly consider all of the risks and interests associated with the decision to restrict knowledge of a vulnerability, the VEP provides for the participation of several different government agencies. The VEP Director is the White House Cybersecurity Coordinator. Other permanent members of the Equities Review Board (the deliberation body of the VEP) include representatives from:

- Office of Management and Budget
- Office of the Director of National Intelligence (to include Intelligence Community-Security
- Coordination Center (IC-SCC))
- Department of the Treasury
- Department of State
- Department of Justice (to include the Federal Bureau of Investigation and the National Cyber Investigative Joint Task Force (NCIJTF))
- Department of Homeland Security (to include the National Cybersecurity Communications and Integration Center (NCCIC) and the United States Secret Service (USSS))
- Department of Energy
- Department of Defense (including the National Security Agency (NSA) (including Information Assurance and Signals Intelligence elements)), United States Cyber Command, and DoD Cyber Crime Center (DC3))
- Department of Commerce
- Central Intelligence Agency

Notably, this list includes agencies that have missions to defend consumer, business, critical infrastructure and government security (i.e. this process is not limited to law enforcement and intelligence agencies).

The 2017 VEP Charter also allows for other USG agencies to participate in the VEP when demonstrating responsibility for, or identifying equity in, a vulnerability under deliberation.

Each agency participating in the VEP designates an agency point of contact (POC) to act as the focal point for vulnerability submissions for their respective organisation and the primary contact for the VEP Executive Secretariat. The VEP POC further ensures one or more Subject Matter Experts (SME) from their agency are identified to support equities determinations and discussions as needed.

Threshold and process

All US government components and personnel (i.e. civilian, military and contractors) must submit a vulnerability to the VEP (by notifying the VEP Executive Secretariat) of any vulnerability that is newly discovered and not publicly known. These terms are defined in the 2017 VEP Charter as follows:

> Newly discovered: After February 16, 2010, the effective date of the initial Vulnerabilities Equities Process, when the USG discovers a zero-day vulnerability or new zero-day vulnerability information, it will be considered newly discovered.
>
> Not publicly known: A vulnerability is considered publicly known if the vendor is aware of its existence and/or vulnerability information can be found in the public domain (e.g., published documentation, Internet, trade journals).

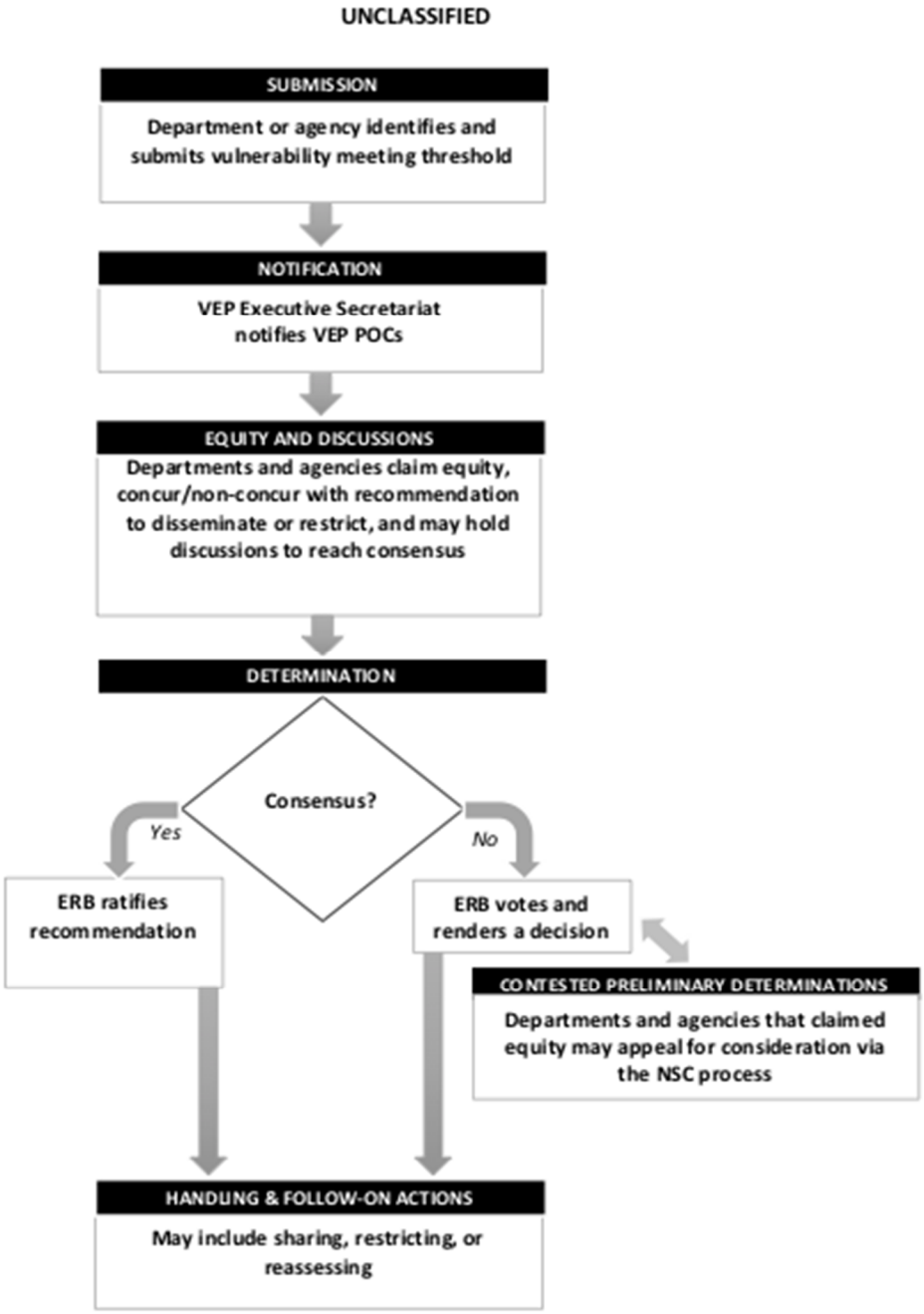
When an agency determines that a vulnerability reaches this threshold for entry into the process, it will notify the VEP Executive Secretariat as soon as is practicable and provide its recommendation to either disseminate or restrict the vulnerability. The submission will include, at a minimum, information describing the vulnerability, identification of the vulnerable products or systems, and a recommendation on dissemination of the vulnerability information.

The 2017 VEP Charter prescribes the following process, as diagrammed in Figure 4):

- The VEP Executive Secretariat will notify VEP POCs within one day of notification of a vulnerability.
- Agencies with equities then have five days to respond to the recommendation of the agency that submitted the vulnerability into the process.
- Any disagreement on the recommendation to disclose the vulnerability immediately to the affected vendor(s) or manufacturer(s) or to restrict knowledge of the vulnerability will be discussed by the SMEs and the VEP Executive Secretariat within seven days. If there is no consensus between the SMEs and the VEP Executive Secretariat, then recommendations will be prepared for consideration by the Equities Review Board.

- The Equities Review Board will meet monthly, but may also be convened sooner if an immediate need arises.
- The 2017 VEP Charter states that "ERB determinations for follow-on actions and next steps should be reached in a timely fashion. When there is consensus among those agencies that claimed an equity, the timeline will be shortened." Decisions of the Equities Review Board are generally to be made by consensus. If consensus is not possible, Equities Review Board members will vote.
- Decisions of the Equities Review Board may be contested within five days by notifying the VEP Executive Secretariat. Disputes arising from the VEP, including any challenges by an agency to a preliminary determination by the ERB, will be resolved using the process described in National Security Presidential Memorandum (NSPM)-4, of 4 April 2017, Organization of the National Security Council, the Homeland Security Council, and Subcommittees.
- Decisions to restrict dissemination of information about a vulnerability will be reassessed at least annually until dissemination is accomplished, the vulnerability is publicly known, or the vulnerability is otherwise mitigated.

Figure 4. Overview of vulnerabilities equity process in the US



The 2017 VEP Charter also provides instructions for when a US government agency learns that a vulnerability that the VEP has restricted knowledge of is used by a third party. In these situations, the agency will immediately report this information to the VEP Executive Secretariat. In such circumstances, the discussion of the vulnerability's equities will begin no later than the business day following notification to the VEP Executive Secretariat, and participants will expeditiously reach a consensus on disclosure or appropriate mitigation actions, or raise issues to the Equities Review Board.

Considerations

The 2017 VEP Charter lists several equity considerations that must be taken into account by VEP participants for each vulnerability that is submitted to the VEP for review. These considerations are:

Part 1 – Defensive equity considerations

1.A. Threat considerations

- Where is the product used? How widely is it used?
- How broad is the range of products or versions affected?
- Are threat actors likely to exploit this vulnerability, if it were known to them?

1.B. Vulnerability considerations

- What access must a threat actor possess to exploit this vulnerability?
- Is exploitation of this vulnerability alone sufficient to cause harm?
- How likely is it that threat actors will discover or acquire knowledge of this vulnerability?

1.C. Impact considerations

- How much do users rely on the security of the product?
- How severe is the vulnerability? What are the potential consequences of exploitation of this vulnerability?
- What access or benefit does a threat actor gain by exploiting this vulnerability?
- What is the likelihood that adversaries will reverse engineer a patch, discover the vulnerability and use it against unpatched systems?
- Will enough USG information systems, US businesses and/or consumers actually install the patch to offset the harm to security caused by educating attackers about the vulnerability?

1.D. Mitigation considerations

- Can the product be configured to mitigate this vulnerability? Do other mechanisms exist to mitigate the risks from this vulnerability?
- Are impacts of this vulnerability mitigated by existing best-practice guidance, standard configurations, or security practices?
- If the vulnerability is disclosed, how likely is it that the vendor or another entity will develop and release a patch or update that effectively mitigates it?
- If a patch or update is released, how likely is it to be applied to vulnerable systems? How soon? What percentage of vulnerable systems will remain forever unpatched or unpatched for more than a year after the patch is released?
- Can exploitation of this vulnerability by threat actors be detected by USG or other members of the defensive community?

Part 2 – Intelligence, law enforcement and operational equity considerations

2.A. Operational value considerations

- Can this vulnerability be exploited to support intelligence collection, cyber operations or law enforcement evidence collection?
- What is the demonstrated value of this vulnerability for intelligence collection, cyber operations, and/or law enforcement evidence collection?
- What is its potential (future) value?
- What is the operational effectiveness of this vulnerability?

2.B. Operational impact considerations

- Does exploitation of this vulnerability provide specialized operational value against cyber threat actors or their operations? Against high-priority National Intelligence Priorities Framework (NIPF) or military targets? For protection of war fighters or civilians?
- Do alternative means exist to realize the operational benefits of exploiting this vulnerability?
- Would disclosing this vulnerability reveal any intelligence sources or methods?

Part 3 – Commercial equity considerations

- If USG knowledge of this vulnerability were to be revealed, what risks could that pose for USG relationships with industry?

Part 4 – International partnership equity considerations

- If USG knowledge of this vulnerability were to be revealed, what risks could that pose for USG international relations?

Importantly, none of these considerations is framed as red lines. In that regard, these considerations are not outcome-determinative, but they do have value in providing guidance to VEP participants to ensure that they are considering relevant risks and interests.

Disclosure

When the VEP participants determine that a vulnerability should be disclosed to the affected vendor(s) or manufacturer(s), the 2017 VEP Charter instructs that disclosure is to be made "in the most expeditious manner and when possible within 7 days. Disclosure of vulnerabilities submitted for equity review will be conducted according to agreed-upon guidelines that are consistently and responsibly followed by all members." The agency that submits the vulnerability to the VEP is presumed to know the most about the vulnerability and is generally responsible for disseminating information about the vulnerability to the affected vendor(s) or manufacturer(s), but the agency may delegate this responsibility to another agency. Agencies are instructed to disclose vulnerabilities consistent with international standards and/or current best practices, and/or take additional actions to reduce risk (i.e. in line with CVD norms and processes). If the affected vendor(s) or manufacturer(s) does not address the vulnerability or does not address the vulnerability with sufficient urgency, the US Government may take other mitigation steps.

Exceptions

Vulnerabilities reported by security researchers or through incident response activity (e.g. US CERT/CC) will not be submitted to VEP.

The following categories will also not be considered to be part of the vulnerability evaluation process:

- Misconfiguration or poor configuration of a device that sacrifices security in lieu of availability, ease of use or operational resiliency
- Misuse of available device features that enables non-standard operation
- Misuse of engineering and configuration tools, techniques and scripts that increase/decrease functionality of the device for possible nefarious operations
- Stating/discovering that a device/system has no inherent security features by design

The 2017 VEP Charter also provides for certain classified exceptions to the process:

> The United States Government's decision to disclose or restrict vulnerability information could be subject to restrictions by partner agreements and sensitive operations. Vulnerabilities that fall within these categories will be catalogued by the originating Department/ Agency internally and reported directly to the Chair of the ERB. The details of these categories are outlined in Annex C, which is classified. Quantities of excepted vulnerabilities from each department and agency will be provided in ERB meetings to all members.

Oversight and accountability

The VEP Executive Secretariat produces an annual report that is submitted to the VEP POCs, the National Security Council, and the White House Cybersecurity Coordinator. The 2017 VEP Charter instructs that the report "will be written at the lowest classification level permissible and will include, at a minimum, an executive summary written at an unclassified level. As part of a commitment to transparency, annual reporting may be provided to the Congress." The annual report will include statistical data as deemed appropriate by the VEP Director and will include any changes to:

- Equities Review Board membership
- Reassignment of the VEP Director responsibility to another position and
- Realignment of the VEP Executive Secretariat responsibility to another agency

7.3. Recommendations for establishing GDDP in the EU

Throughout their everyday functionality, governments often have unique insight into vulnerabilities. Thus, ensuring that governments and their agencies have strong policies for reviewing and coordinating the disclosure of vulnerabilities is a critical norm that should be advanced within the EU. Yet, it appears that most member states currently lack a government vulnerability disclosure review process.

Recognising the key role that finding and responsibly addressing vulnerabilities plays in cybersecurity, the NIS Directive aimed to facilitate information sharing from companies to governments. However, this mechanism is of little benefit if it remains a one-way street or if this process is limited only to critical infrastructure. We must ensure that there are robust, accountable, and transparent systems in place to ensure that member states are sharing information about vulnerabilities in any ICT products, networks, or systems

back out to affected vendors and manufacturers, as well as maintaining transparency regarding these activities towards the public.

We recommend that all member states implement policies and practices for their government institutions and agencies with the following characteristics:

- All security vulnerabilities are subject to a GDDP.[59]
- All relevant ministries, including those with missions for user, business, and government security, should participate in the GDDP and participants should work together using a standard set of criteria to ensure all risks and interests are considered.
- The policies, practices, and determinations of the GDPP should be subject to independent oversight and transparency.
- The executive secretariat of the GDPP should be housed within a civilian agency with expertise in existing coordinated vulnerability disclosure.
- The GDDP should be codified in law or other legally binding policy to ensure compliance and permanence.
- The default policy should be to disclose vulnerabilities immediately to the affected vendor(s) so they can be patched.
- Where the vulnerability potentially affects the safety of regulated products (such as cars, medical devices or railway signals, the relevant EU safety and standards bodies should be involved in the GDDP.

ENISA can play a vital role in sharing best practices around government vulnerability disclosure review processes and assisting and advising member states in implementing such processes.

The EU Cybersecurity Act offers a unique opportunity to advance the norm that member states should have robust, accountable, and transparent GDDP, thereby fostering greater cooperation, coordination and resilience in Europe

Survey of member states

It may also be useful for the European Commission or ENISA to conduct a study of member states' efforts to implement a government disclosure decision processes. A better understanding of how member states are handling vulnerabilities will contribute to a more robust conversation about cybersecurity

---

[59] Vulnerabilities identified through security researcher activity and incident response that are intended to be disclosed in a rapid fashion should not be subject to adjudication by GDDP.

in Europe and the types of measures that are needed to improve coordination and cooperation in the EU around cybersecurity incidents.

In these questions, "government disclosure decision processes" mean governmental process for reviewing vulnerabilities that a government or any of its affiliated bodies learns about in order to determine whether a vulnerability should be disclosed to the affected vendor(s) immediately or whether disclosure should be delayed. Government vulnerability disclosure process" may also have a role in coordinating the actual disclosure of the vulnerability to the affected vendor(s).

1. Does the member state have an established GDDP?
    a. If so, which agencies/ministries/departments/etc. of the member state regularly participate?
    b. If so, which agencies/ministries/departments/etc., if any, are required to submit vulnerabilities that they learn about to the government vulnerability disclosure review process?
    c. If so, is the process mandatory or voluntary?
    d. If so, where is the process established/articulated?
    e. If the member state does not have an established government vulnerability review process, what actions has the member state taken in order to ensure it is handling vulnerabilities responsibly?
2. If a decision to disclose a vulnerability is made, how is it disclosed? What are the member state's policies and practices for informing and coordinating the disclosure of vulnerabilities that it learns about to affected vendors and manufacturers?
3. What policies and practices has the member state adopted to coordinate and cooperate with other member states and the EU institutions on vulnerabilities with potential cross-border effects?

PART III
CONCLUSIONS AND RECOMMENDATIONS

8. CONCLUSIONS: IT'S TIME TO ACT

Cybersecurity is the talk of the town. It is regularly invoked with a growing sense of urgency in the most important fora across the globe. The European Union, in particular, is facing a number of cyberattacks, which are increasing exponentially in quantity and in quality since they come from both non-state and state actors. Unless the EU improved its own cybersecurity, the risk will increase with the digital transformation. Billions of IOT devices (internet of things) are expected to be connected to the internet and software will become omnipresent in our lives. But software and software-based products have inherent vulnerabilities. Each of these weaknesses could allow an attacker to compromise the integrity of the product and exploit it for personal gain. Moreover, with the development of the IOT, the attack surface is becoming broader, which greatly increases the potential impact of vulnerabilities on the ecosystem.

Software vulnerabilities therefore pose a serious concern for everyone and require the development of *ad-hoc* policies to coordinate the disclosure of vulnerabilities. The analysis of this Task Force shows that only a few countries across Europe have managed to put software vulnerability disclosure processes in place, but many others have discussions underway and are working to do so. Therefore, common action from the European institutions could help to jumpstart coordinated vulnerability disclosure (CVD) and government disclosure decision processes (GDDP) across Europe. A significant barrier to the implementation of CVD policies across the EU is the lack of a single interpretation of what constitutes 'hacking' among the member states. Therefore, the first step is to provide the necessary legal certainty to security researchers involved in vulnerability discovery as well as setting appropriate vulnerability disclosure processes through complementary guidance and best practices. Based on current best practices in Europe, the US and Japan, the Task Force recommends implementation of the following CVD-related policies.

8.1. CVD policies

The Task Force calls upon the European Commission and the member states to collectively draft a European-level framework complemented by national legislation in accordance with the guidelines and recommendations defined in ISO/IEC 29147:2014 and ISO/IEC 30111 in order to provide legal clarity for software vulnerability discovery and disclosure. The Nationaal Cyber Security Centrum (NCSC) in the Netherlands has published a general guideline for

responsible disclosure, *which can serve as a useful model that EU member states can follow in drafting their own responsible disclosure policy*.[60]

The Coordinated Vulnerability Disclosure Template from the National Telecommunications and Information Administration (NTIA) of the US Department of Commerce and the "Vulnerability Disclosure Program for Online Systems from the Cybersecurity Unit, Computer Crime and Intellectual Property Section Criminal Division of the US Department of Justice could also offer helpful suggestions. The Task Force suggests the steps outlined below for implementing coordinated vulnerability and government vulnerability disclosure processes in Europe.

Private sector

The private sector could take the lead in implementing coordinated vulnerability disclosure by defining and publishing public reporting mechanisms on vulnerabilities disclosure on companies' websites, according to the ISO standards. The Netherlands Responsible Disclosure Guidelines, the NTIA template and the DOJ Vulnerability disclosure programs could also be followed as best practices.

CERTs

Computer emergency response teams (or CERTs) should help to put in place a framework to implement coordinated vulnerability disclosure processes, playing the role of a trusted third party and coordination center in this process.

EU member states

Member states should create the necessary legal certainty for security researchers involved in vulnerability discovery, changing national legislation to allow for the recognition of ethical hacking.

EU institutions

The EU should change the European legislation to ensure legal certainty for security researchers involved in vulnerability discovery and to allow for common rules and procedures across member states, which would pave the way for a common process of coordinated vulnerability disclosure in Europe.

The list below presents the recommendations that have been agreed upon by the Task Force members in the course of their deliberations

---

[60] See https://www.ncsc.nl/english/current-topics/news/responsible-disclosure-guideline.html.

8.2. Recommendations for the implementation of CVD in Europe

8.2.1. EU legislation

1. **Amend Directive 2013/40/EU on attacks against information systems (the EU cybercrime Directive)** to allow the smooth and rapid development of CVD.
2. **Protection of security researchers.** Researchers involved in vulnerability discovery are often exposed to criminal or civil liability. The legal liability and responsibilities of security researchers should be fully clarified to enable them to continue their work without fear of prosecution. [61]
3. **Incentives for security researchers**. Appropriate policies should be adopted with the aim of encouraging 'white-hat hackers' to actively participate in coordinated vulnerability disclosure programs.
4. **Directive on security of network information systems (NIS).** In transposing the NIS Directive, particularly its Article 14, member states may explicitly consider including CVD as one of the technical and organisational measures.
5. **General data protection Regulation (GDPR**). According to the GDPR, software owners and tech firms become data controllers when they exercise overall control over the purpose for which, and the manner in which personal data are processed. Assuming that irresponsible handling of vulnerabilities could lead to personal data breaches falling within the scope of GDPR, CVD should be viewed as an effective tool to mitigate the relevant risks.
6. **Cybersecurity Act.** The proposed Regulation submitted by the European Commission in October 2017 concerning the European Network and Information Security Agency (ENISA) and cybersecurity certification notes that ENISA, in its coordination and capacity-building roles, can contribute to the harmonised development of CVD in the EU by having its mandate amended, thereby allowing it to engage in the following activities:
    - Writing EU-wide guidelines for the reporting process, addressing the issues it raised in its January 2017 "Good Practice Guide on Vulnerability Disclosure" report;[62;]

---

[61] See for instance https://blog.rapid7.com/2015/10/28/new-dmca-exemption-is-a-positive-step-for-security-researchers/

[62] See https://www.enisa.europa.eu/publications/vulnerability-disclosure.

- Installing and operating a web portal where disclosure of software and hardware vulnerabilities can be coordinated at the European level and contributed to anonymously;
- Building a team of 'white-hat hackers' who would conduct campaigns to assist EU member states and operators of essential services to mitigate software vulnerabilities, with the objective of increasing the security of all infrastructures;
- Implementing training in all issues that may arise in the context of CVD, e.g. technical, legal, etc., to build capacity on CVD in the EU; and
- Liaising formally with other key international actors on CVD in order to enhance cooperation, collaboration and the sharing of best practices.

Furthermore, **Article 47 (1)j of the Cybersecurity Act** states that a European cybersecurity certification scheme is expected to include *inter alia* "rules concerning how previously undetected cybersecurity vulnerabilities in ICT products and services are to be reported and dealt with." This provision of the Cybersecurity Act provides the possibility to introduce CVD in a European Cybersecurity Certification Scheme, which in fact may encourage CVD as a standard practice.

7. **Software vulnerabilities in durable goods, such as cars and medical devices.**
    - The European Commission should amend the Radio Equipment Directive so that Art. 3, paragraph 3 provides that "radio equipment is cybersecure by design, by default and by implementation".
    - The European Commission should incorporate the standards for vulnerability management (ISO 29174, 30111) directly into the CE mark system.

8.2.2. National legislation

Amending national legislation to support CVD. As a medium-to-long-term solution and given that the revision of the EU cybercrime Directive (from 2013) may take several years, the Task Force advises member states to consider amending their national legislation bearing on CVD, using the framework on CVD introduced in the Netherlands as a model.

8.2.3. EU research funding

8. **Framework Programs for Research and Innovation**. The various European Framework Programs for Research and Innovation offer several ways to leverage funding to promote CVD among public and private researchers in Europe. For instance, the following H2020 calls described in the Work Programme 2018-2020 could be used to finance research and innovation in this area:
    - SU-ICT-03-2018: Establishing and operating a pilot project to create a Cybersecurity Competence Network
    - SU-DS02-2020: Management of cyber-attacks and other risks
    - SU-DS03-2019-2020: Digital security and privacy for citizens and small and medium enterprises and micro enterprises
    - SU-DS04-2018-2020: Cybersecurity in the Electrical Power and Energy System (EPES)
    - SU-DS05-2018-2019: Digital security, privacy, data protection and accountability in critical sectors

    The next Framework Programme for Research and Innovation, FP9, should also provide explicit funding for CVD across Europe.

8.3. Recommendations to implement government disclosure decisions processes (GDDP) in Europe

In the course of their day-to-day functioning, governments often acquire insights into vulnerabilities. Thus, ensuring that governments and their agencies have strong policies for reviewing and coordinating the disclosure of vulnerabilities is a critical norm that should be advanced within the EU. It appears, however, that most member states have not yet implemented a government vulnerability disclosure review process.

GDDP characteristics. The Task Force recommends that all member states adopt the following policies and practices to inform the GDDP activities of their government institutions and agencies:

9. All security vulnerabilities should be subject to a government disclosure decision process.[63]
10. All relevant ministries, including those with missions for user, business and government security, should participate in the GDDP and

[63] Vulnerabilities identified through security researcher activity and incident response that are intended to be disclosed in a rapid fashion should not be subject to adjudication by GDDP.

participants should work together using a standard set of criteria to ensure that all risks and interests are considered.

11. The policies, practices and determinations of the GDDP review should be subject to independent oversight and transparency. Regular public reporting should be viewed as a critical part of this.
12. The executive secretariat of the GDDP should be housed within a civilian agency with expertise in existing coordinated vulnerability disclosure.
13. The GDDP should be codified into law or other legally binding policy to ensure compliance and permanence.
14. Any non-disclosure agreement with contractors, resellers or security researchers should be prohibited.
15. Any decision to delay disclosure of a vulnerability should be reviewed at least every six months.
16. The default policy should be to disclose vulnerabilities immediately to the affected vendor(s) so they can be patched.
17. Where the vulnerabilities potentially affect the safety of regulated products (such as cars, medical devices or railway signals), the relevant RU safety and standards bodies should be involved in the GDDP.

ENISA can play a vital role in sharing best practices in GVD review processes and in assisting and advising member states in their implementation.

Survey of member states' GDDP. It might also be useful for the European Commission or ENISA to conduct a study of member states' efforts to implement a GDDP. A better understanding of how member states are handling vulnerabilities will contribute to a more robust and informed debate about cybersecurity in Europe and the types of measures that are needed to improve coordination and cooperation vis-á-vis cybersecurity incidents in the EU.

ANNEX I. LIST OF TASK FORCE MEMBERS AND INVITED GUESTS AND SPEAKERS

Task Force Members

Chair:	Marietje Schaake, Member of the European Parliament
Coordinator:	Lorenzo Pupillo, Associate Senior Research Fellow, CEPS
Co-Rapporteurs:	Afonso Ferreira, Directeur de Recherche CNRS Gianluca Varisco, Cybersecurity Expert, Italian Digital Transformation Team
Research Assistant:	Antonella Zarra, CEPS

Advisory Board

Ross Anderson, Professor of Security Engineering at Computer Laboratory, University of Cambridge

Andriani Ferti, Senior Associate Karatzas & Partners Law Firm

Allan Friedman, Cybersecurity Director, US National Telecommunications and Information Administration

Tim Watson, Director of the WMG Cyber Security Centre, University of Warwick

Companies and European Organisations

Jochai Ben-Avie, Senior Global Policy Manager, Mozilla

Mariano Cunietti, Chief Technology Officer, Enter

Jeroen van der Ham, National Cyber Security Center, The Netherlands

Lise Fuhr, Director General, European Telecommunications Network Operators

Caroline Greer, Head of European Public Policy, Cloudflare

Evgeny Grigorenko, Head of Public Affairs, Europe, Kaspersky Lab

Baiba Kaskina, CERT Latvia and Chair TF-CSIRT

Stephane Lenco, Chief Information Security Officer, Airbus

Jan Neutze, Cybersecurity Policy Director, EMEA, Microsoft

Jan-Jacque Sahel, Vice President for Global Stakeholder Engagement, Europe and Civil Society, ICANN

Corinna Schulze, Director, EU Government Relations, Global Corporate Affairs, SAP

Mark Smitham, Senior Manager, Microsoft

European Institutions

Laurent Beslay, Project Leader, Joint Research Centre, European Commission

Monika Kopcheva, Political Administrator, Council of the European Union

Aristotelis Tzafalias, Policy Officer, Cybersecurity and Digital Privacy, European Commission

Claudia Warken, Policy Officer, DG Home Affairs, European Commission

Mathias Vermeulen, Policy Advisor to MEP Marietje Schaake, European Parliament

Civil Society

Jens-Henrik Jeppesen, European Policy Director, Center for Democracy and Technology

Lucie Krahulcova, EU Policy Associate, Access Now

Academia

Stefano Fantin, Legal Researcher, Center for IT and IP Law, Katholieke Universiteit Leuven

Extra-EU Organisations

Uchiyama Takayuki, CERT Japan

Invited Guests

Vassault-Houlière Guillame, CEO YesWeHack

Lecoeuvre Romain, CTO YesWeHack

ANNEX II. TIMELINE OF THE US GOVERNMENT'S VULNERABILITIES EQUITIES PROCESS

January 2008. President George W. Bush signed the National Security Policy Directive 54 (NSPD 54), which called for a US-government-wide effort called the Comprehensive National Cybersecurity Initiative (CNCI). CNCI required the Departments of State, Defence, Homeland Security and Justice, as well as the Director of National Intelligence, to develop "a joint plan for the coordination and application of offensive capabilities to defend US information systems".

2008. The joint plan coming out of the CNCI notes that the discovery of vulnerabilities "may present competing equities for [government] offensive and defensive mission interests" and recommended that "actions taken in response to knowledge of a specific vulnerability must be coordinated to ensure the needs of each of these 'equities' are addressed". The joint plan recommended the development of a "Vulnerabilities Equities Process," but the tasks assigned to the VEP in the joint plan remain classified.

2008-09. Starting in 2008, in accordance with the joint plan's recommendation, the Office of the Director of National Intelligence (ODNI) set up a working group to develop the VEP. The working group included representatives from ODNI, the National Security Council, Central Intelligence Agency, Defense Intelligence Agency, Justice Department, Federal Bureau of Investigation, Department of Defense, Department of State, Department of Energy, and Department of Homeland Security. The working group developed a document known as the "Commercial and Government Information Technology and Industrial Control Product or System Vulnerability Equities Policy and Process" (the VEP Document). The VEP Document is dated 16 February 2010.

11 April 2014. Bloomberg published an article claiming that the NSA had, for two years, been exploiting a vulnerability called Heartbleed which is estimated to have affected two thirds of the world's web servers - any server that used the popular OpenSSL cryptographic library.

28 April 2014. White House Cybersecurity Coordinator Michael Daniel published a blog post denying that the government had prior knowledge of Heartbleed and discussing how he is "reinvigorating" the VEP. It is widely

believed that the VEP was not operational at this time. Before the VEP was operationalized, it appears that various Federal agencies ran their own processes -- notably, the NSA had long run a process to navigate the potentially conflicting missions of its Information Assurance and Signals Intelligence Directorates.

6 May 2014. EFF filed a Freedom of Information Act (FOIA) request to obtain all records pertaining to the VEP.

15 December 2014. EFF received first (heavily redacted) batch of responsive documents, continued to get additional documents over the next year.

14 January 2016. EFF received a largely unredacted description of the VEP including the VEP Document following litigation to compel response to their May 6, 2014 FOIA.

March 2016. The FBI contracted with a security firm to break into an iPhone used by the San Bernardino shooter, in the midst of a high profile lawsuit to force Apple to write software to unlock the security features on the phone.

27 April 2016. The FBI released a statement saying the Bureau will not submit the iOS vulnerability in question for review by the VEP, saying it did not possess enough information about how it worked.

17 May 2017. Following one of the largest global cyberattacks in history (WannaCry), U.S. Senators Schatz, Johnson, and Gardner and U.S. Representatives Lieu and Farenthold introduce the Protecting our Ability to Counter Hacking (PATCH) Act, bipartisan legislation that would reform and codify the VEP.

15 November 2017. White House Cybersecurity Coordinator Rob Joyce announces new VEP Charter, including many of the reforms contained in the PATCH Act.

This report puts forward the analysis and recommendations for the design and implementation of a forward-looking policy on software vulnerability disclosure (SVD) in Europe. It is the result of extensive deliberations among the members of a Task Force formed by CEPS in September 2017, including industry experts, representatives of EU and international institutions, academics, civil society organisations and practitioners.

Drawing on current best practices throughout Europe, the US and Japan, the Task Force explored ways to formulate practical guidelines for governments and businesses to harmonise the process of handling SVD throughout Europe. These discussions led to policy recommendations addressed to member states and the EU institutions for the development of an effective policy framework for introducing coordinated vulnerability disclosure (CVD) and government disclosure decision processes (GDDP) in Europe.

9 789461 386878

CEPS