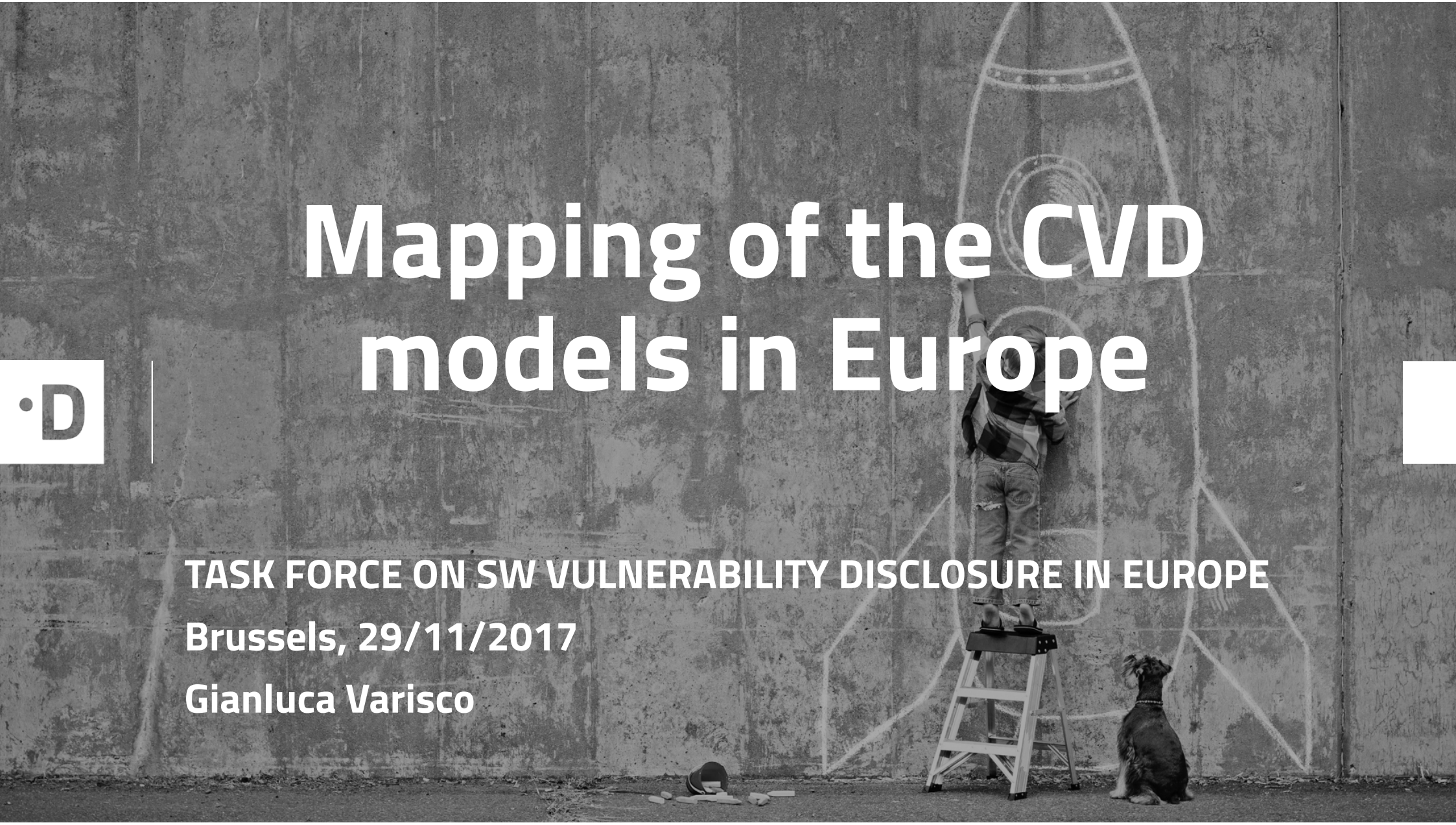

Mapping of the CVD models in Europe

TASK FORCE ON SW VULNERABILITY DISCLOSURE IN EUROPE

Brussels, 29/11/2017

Gianluca Varisco

Disclaimer

This **preliminary mapping** has been put together by:

- **reaching out** to official bodies/parties such as national **CSIRTs** and **Gov's cybersecurity departments**.
- **collecting** official, verified **information** from **public sources**
- **collecting opinions** and **feelings** from **people** involved in the **national processes**

As of today, it's still **incomplete** as **many answers** from **member states** are still **missing** and **no public information** were **found**

Austria

- **No** CVD policy at national level
- **Failed attempts** to include CVD in the **NIS transposition law** being drafted
- **Why?** According to the people drafting it, the **generic laws** *should* be already "**good enough**" for a sensible disclosure process
- Some sort of government statement that defines the criteria of a good disclosure process would be very welcomed. Whether this is a law, a regulation or just a white-paper by a suitable national agency, is not that important.
- No **ongoing** discussions

Belgium

- The **Centre for Cyber Security Belgium** has published its "**Cyber Security Guide for SME**" in 2014 where it **briefly** states "**Publish a Responsible Disclosure Policy**" under the "Advanced Protection' - 02: Publish A Corporate Security Policy and a code of Conduct" section
- Companies such as Telenet.BE, SNCB/NMBS (the national railway company) or Roamler Retail have defined and published **their own policies**
- There are **NO coordinated efforts** at **national level**

Bulgaria

- **CERT Bulgaria** mentioned that there is **NO** plan to implement a CVD policy
- **They recognise** the **importance** of a **well-defined process of vulnerability detection** and its **quickest mitigation** and **fixation**.
- **They hope** that **discussions** on this issue **will start as soon as possible** given its **exceptional importance**.

Czech Republic

- **CZ's Government CERT** mentioned that there is **NO** CVD policy at **national level** and there are **no discussions ongoing** currently.
- On the other hand, **they would like to start** with **a similar discussion next year**.
- They see CVD as **a topic they need to catch up with**.

Finland

- The National Cyber Security Centre Finland (NCSC-FI) published in **2010** a Vulnerability Coordination Policy.
- **CERT-FI's 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**, not merely during the disclosure phase.
- **No** national laws or directives
- **No** updates on this topic since **2012**

Hungary

- **Interest** expressed during the GFCE expert meeting on Responsible Disclosure (23 March **2016**, Budapest Hungary)
- **No further updates** since then

Italy

- **The Digital Transformation Team** has started drafting a **Coordinated Responsible Disclosure Policy** that **aims** to be **generic** and **potentially** covering both the **private** and **public sectors**
- The work is being done 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 program** aiming at **supporting private companie**s in **implementing CVD policies** and **improving internal/external processes** has been **prepared** but is currently **on hold** until the **legal aspects** are **sorted out**

Lithuania

- According to a report released in **November 2017**, **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.
- A **vulnerability disclosure framework is in place**, which includes a **disclosure deadline**, **scheduled resolution**, and an **acknowledgement report**. **Organisations** have **established processes** to **receive** and **disseminate vulnerability information**.

Luxembourg - CIRCL

- CIRCL mentioned that **there are already some works ongoing** within their **cybersecurity strategy** (the **third edition** is an ongoing process and **will be released in February 2018**)
- The goal is to cover with **generic guidelines** the private, public and research sectors
- A responsible vulnerability disclosure process for the private sector is **already provided** - which is already a good basis for the generic foreseen guideline for their national strategy
- Main challenges: **legal aspects**, especially the **responsibility of the security researchers** and **dual-use export control**

Luxembourg - GOVCERT.LU

- **CERT Gouvernemental** mentioned that **they do not have a CVD policy at national level yet**
- They are having discussion about the CVD topic **on the highest possible level**: the Cyber Security Board, chaired by their Prime Minister
- The setup of **a national CVD plan** will **probably be covered** by the **third revision** of the **national strategy**
- **All the actors involved** agreed that **they need** a **CVD strategy on a national level**

Romania

- CERT.ro publishes a **CVD policy** on its website, although it clearly states:

*"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)"*

- *They are **encouraging** at **national level** the **adoption by companies and institutions of mechanisms** enabling the **reporting**, **rapid evaluation** and **remedy of the vulnerabilities** and t**he identification** of and **adoption** of a **dedicated legal framework** for **reporting vulnerabilities***

Slovenia

- **SI-CERT** mentioned that there is **NO** policy on a **national level**.
- They have proposed to add this topic to the upcoming "**Law on Information Security**", but **no consensus was reached** for support at that time.
- Together with the **Information Commissioner's Office**, they intend to continue this **debate** with the **representatives** of the **Ministry of Justice**.
- **Challenges**: the **awareness of decision makers** on the political level of what the **current best-practices** in the **information security community** are.

United Kingdom

- **NCSC's Vulnerability Co-ordination Pilot** is **ongoing**
- They are working with an **invited group** of **UK-based security practitioners** to **help them** to **identify** and **resolve vulnerabilities** across **three publicly facing systems** used in **UK Public Sector**.
- To help them **get this right** they are working with **LutaSecurity** for **advice** and will look to use a **recognised platform** for **vulnerability co-ordination**.
- 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 (non-EU)

- MELANI / GovCERT mentioned that there is **NO** policy at the moment
- Currently **enhancing** the **National Strategy for the protection against cyber risks** (NCS). During the implementation, it **could be possible to discuss** a CVD **policy**.
- They are **seeking** and **encouraging** a **responsible behaviour** of **all participants** based on **voluntariness** and **self-governance**.
- **Regulation by the state should** only **be the last resort if all other approaches fail**.
- **Responsible Disclosure** has been discussed in their **Semi-annual report 2/2015**
- **Challenges**: **different expectations** about **timeliness** of a **reaction** between **researchers** and **vendors**; **finding** the **right security contacts** as not all vendors do publish theirs.

No answers / public info collected

- Germany
- Poland
- Croatia
- Spain
- France
- Sweden
- Greece
- Portugal

- Denmark
- Malta
- Republic of Ireland
- Estonia
- Slovakia
- Cyprus

Latvia

Baiba Kaškina (CERT Latvia & Chair TF-CSIRT) will be talking about the CVD model in Latvia at 9:45AM today!

The Netherlands

Jeroen van der Ham (National Cyber Security Centre, The Netherlands) will be talking about the possibilities to extend the (successful) Dutch model of CVD to other Member States at 11:15am

Contacts

Gianluca Varisco

- Email: gianluca@teamdigitale.governo.it
- Twitter: @gvarisco
- Medium: @gvarisco

Sito Web: https://teamdigitale.governo.it

DIGITAL
TRANSFORMATION
TEAM
Italian Government