



(Ethical) Hacking

Sofie Royer

May 5, 2020

Overview

Essentials of criminal law & procedure

European perspective

- Cybercrime Convention
- EU Directive on attacks on information systems

Countries' approach

- Belgium
- The Netherlands

Responsible disclosure policies

Each offence consists of

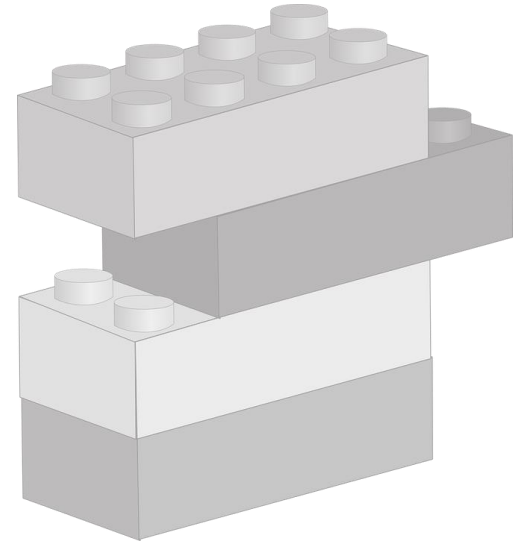
- A material element = behavior

No criminal liability for thoughts!

- A moral element = intent

- General intent: knowingly and willingly
- Negligence (lack of caution)
- Special intent

E.g. Procuring an economic advantage, damaging computer system/data...



To keep in mind

Motive does not matter

Unless when determining the sentence

Unless aggravating circumstance (e.g.: racist motives)

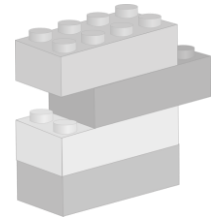
Bekende Nederlandse actrice in cel
voor drugshandel op Tomorrowland:
"Ze wou zich inleven in nieuwe
filmrol"

Consent of the victim does not "neutralize" existence of an offence

E.g. (grave) assault and battery

Unless indispensable materiel element of an offence

E.g.: rape = sexual intercourse without consent





Investigation
Public prosecutor
= Procureur des Konings/ du
Roi/ Parket/ Openbaar
Ministerie/ Officier van justitie



Investigating judge
Onderzoeksrechter/ juge
de l'instruction/
rechter-commissaris

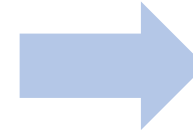
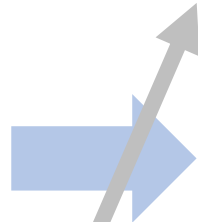


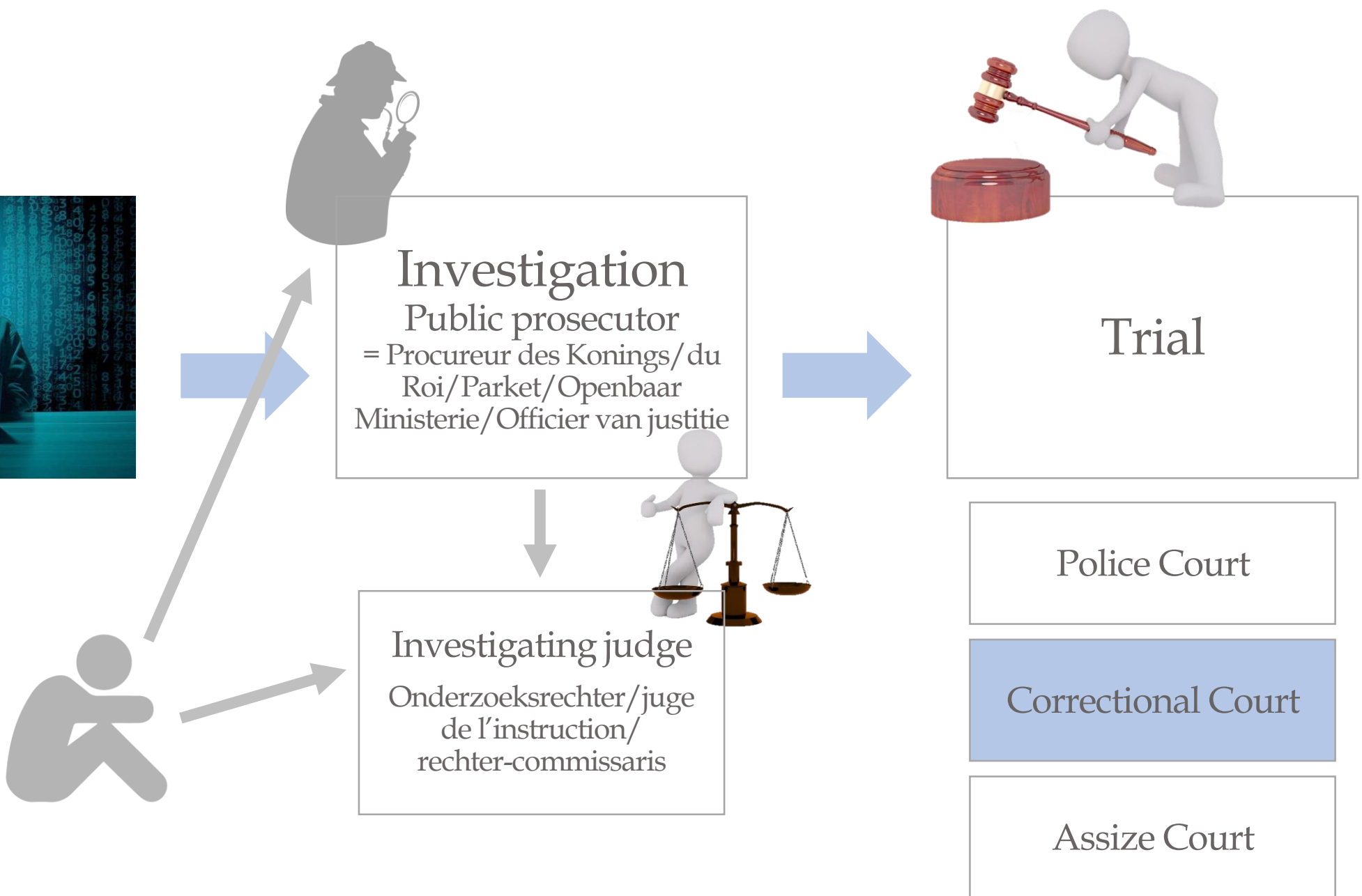
Trial

Police Court

Correctional Court

Assize Court





European Perspective

Cybercrime Convention

°2001: more than 60 ratifications & signatures

Article 2 – Illegal access to computer systems

Article 3 – Illegal interception of communication

Article 4 – Data interference

Article 5 – System interference

Article 6 – Misuse of devices

Any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data (art. 1, a) [Cybercrime Convention](#))

Art. 2 Cybercrime Convention

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed **intentionally**, the **access** to the whole or any part of a computer system **without right**.

A Party **may** 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.

EU Directive on attacks against information systems

°2013

- Necessary to increase resilience of information systems
- Need for harmonization of national criminal law

Illegal access: the **access without right** to the whole or to any part of an information system when committed **intentionally** + by **infringing a security measure**

Without right: conduct that is **not authorized** by the owner or by another right holder of the system or **not permitted** under national law

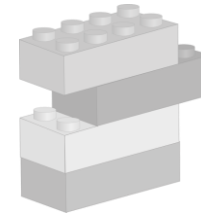
A device or group of interconnected or related devices, one or more of which, pursuant to a program, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance.

Which criminal law is applicable?

Principle: An offence committed on the territory of the Kingdom of Belgium, by Belgians or by foreigners, will be punished in accordance with the provisions of the laws of Belgium. (art. 3 [Criminal Code](#))



One of the materiel elements was situated in Belgium



What does this mean in a digital world? Extensive interpretation

- Where hacker is operating his/her computer system
- Where victim can no longer access his/her files

Someone obtains access to a computer system in order to discover a vulnerability* without...

... having access rights to the computer system;

... damaging the system or the data;

... revealing any confidential information or reaching out to the press;

... obtaining any economic advantage.

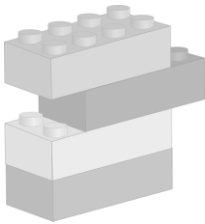
Can this person be criminally liable
under the Belgian/Dutch Criminal Code?

* a set of conditions or behaviors 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 ([The CERT Guide to Coordinated Vulnerability Disclosure](#))

Belgian approach

Every system used to store, process or transfer data.

E.g. computers, servers, networks, telecommunication systems, smartphones, USB-sticks, smart watches...

	External hacking	Internal hacking	Abuse of confidence
Article	550, § 1 <u>Crim. Code</u>	550, § 2 <u>Crim. Code</u>	491 <u>Crim. Code</u>
	Obtaining or maintaining access to a computer system <i>Security breach not required</i>	Exceeding his/her rights of access to computer system	Misappropriation of goods, money, notes, writings... which have been given on the condition that they be returned or made use of or for a specific purpose to the detriment of others
	Knowing that he/she is not entitled to do so	Intent to defraud or to cause damage	Intent to defraud
Sentence	Imprisonment between 6 months and 2 year AND/OR a fine between 26 and 25.000 euros (x8)	Imprisonment between 6 months and 3 years AND/OR a fine between 26 and 25.000 euros (x8)	Imprisonment between 1 month and 5 years AND a fine between 26 and 500 euros (x8)

What about ethical hackers/ security researchers?

He who obtains access to a computer system or maintains access to a computer system, while knowing that he is not entitled thereto, shall be punished [...].

Celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient, est puni [...].

Correctional Court Eupen, 15 December 2003

Attempt to hack: suspension (minor offence, young age, no criminal record...)

Correctional Court Leuven, 15 June 2010

Penetration of website of Fortis:

- External hacking
- Acts of preparation: illegitimately possessing, producing, selling... any instrument primarily designed or adapted to enable one the criminal offences
- Attempt to digital forgery: entering of a fake code in the Fortis Banking computer system
- Attempt to data interference

Related offences

Dissemination of hacker tools (art. 550bis, § 5 [Criminal Code](#)) = illegitimately possessing or disseminating any instrument designed or adapted to enable external/internal hacking

Usage/dissemination of data (art. 550bis, § 7 [Criminal Code](#)) obtained through hacking

Imprisonment between 6 months and 3 year and/or a fine between 26 and 100.000 euros (x8)

Data/system interference (art. 550ter, § 1 [Criminal Code](#)) = introducing, altering, deleting or changing the normal use of any data in a computer system + **damaging data**

Imprisonment between 6 months and 3/5 years and/or a fine between 26 and 25.000/75.000 euros (x8)

Digital forgery (art. 210bis [Criminal Code](#)), **violation of private communication** (art. 314bis [Criminal Code](#)), **violation of data protection laws, violation of trade secrets, confidentiality breaches...**

V. VANDERGEETEN, "La criminalité informatique et les politiques de divulgation coordonnée des vulnérabilité" in *Les obligations légales de cybersécurité et de notifications d'incidents*, 2019, pp. 215-266.

J. HENROTTE & P. LIMBREE, "Le pirate éthique à l'épreuve du droit penal et de la protection des données", *LEGITECH* 2019, 18-25.

Possible way(s) out

Celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient, est puni [...].

“Unauthorized access” ⇔ **Consent** of the one who is being hacked?

Consent:

- In advance
- Free
- Of whom? The one being protected by the offence...

Trespass: internal hacking/abuse of confidence

Motive does not matter... But what about **state of necessity**?

Criminal nature of the behavior is neutralized when protecting a value that is **at least equally important** to the one that is protected by the offended rule



National Responsible Disclosure Strategy?

1 September 2016: [Challenges for law enforcement in cyberspace](#)

Koen Geens

VICE-EERSTEMINISTER, MINISTER VAN
JUSTITIE EN MINISTER VAN EUROPESE
ZAKEN



NIEUWS

MAGAZINE

MINISTER

BELEID

OPINIES

IN DE MEDIA

JUSTITIE IN TRANSITIE

CONTACT

HOME / NIEUWS / OVERHEID HAALT ETHISCHE HACKERS UIT ILLEGALITEIT

Tweeten

Delen

Vind ik leuk 14 d.

Terug naar het overzicht:

■ Alle nieuwsberichten

■ Opiniestukken

■ Persberichten

■ Artikels

■ Radio

■ Televisie

■ Fotoreeksen



Overheid haalt ethische hackers uit illegaliteit

op 08 december 2016 10:16 • De Tijd

De overheid gaat ethische hackers uit de grijze zone halen. Sommige bedrijven geven al groen licht aan 'vriendelijke hackers', maar nu biedt de overheid hun een kader aan.

Net als elke poging tot inbraak in uw woning, is sinds 2000 elke poging tot hacking in België strafbaar. Zeker als onbevoegde buitenstaanders (externe hackers) een netwerk binnendringen. Maar het is ook het geval als mensen in het bedrijf of de organisatie hun bevoegdheden misbruiken (interne hackers).

Het Centrum voor Cybersecurity België, dat onder de eerste minister valt, had vorige week een ongezien overleg met ethische hackers. Dat zijn computerspecialisten die binnendringen in de netwerken van bedrijven, overheidsdiensten en andere organisaties, maar geen kwade bedoelingen hebben. Ze zoeken naar mogelijke veiligheidsrisico's in computernetwerken. Ondanks hun goede intenties zijn zulke pogingen tot hacking strafbaar in ons land. Een overleg met een overheidsdienst die de cyberveiligheid in België moet garanderen, is dus uitzonderlijk.

2020: [Bill New Criminal Code](#)

Responsible disclosure Policy of City of Ghent

Report the vulnerability **as soon as possible** after discovery.

Provide **sufficient information** to reproduce the vulnerability so that we can solve the problem as quickly as possible.

Don't disclose the vulnerability until we have been able to correct it.

Don't exploit the vulnerability by unnecessarily copying, deleting, adapting or viewing data.

Don't apply the following actions:

- Placing malware (virus, worm, Trojan horse, etc.).
- Copying, modifying or deleting data in a system.
- Making changes to the system.
- Repeatedly accessing the system or sharing access with others.
- Using automated scanning tools.
- Using the so-called "brute force" of access to systems.
- Using denial-of-service or social engineering (phishing, vishing, spam,...).

Offences

Don't use attacks on physical security, social engineering, distributed denial of service, spam or third-party applications.

Immediately **erase all data obtained** through vulnerability as soon as it is reported to the Stad Ghent.

Don't perform actions that could have an impact on the proper functioning of the system, both in terms of availability and performance, but also in terms of confidentiality and integrity of the data.

Acts under this Responsible Disclosure Policy should be limited to conducting tests to identify potential vulnerabilities, and sharing this information with the Stad Ghent.

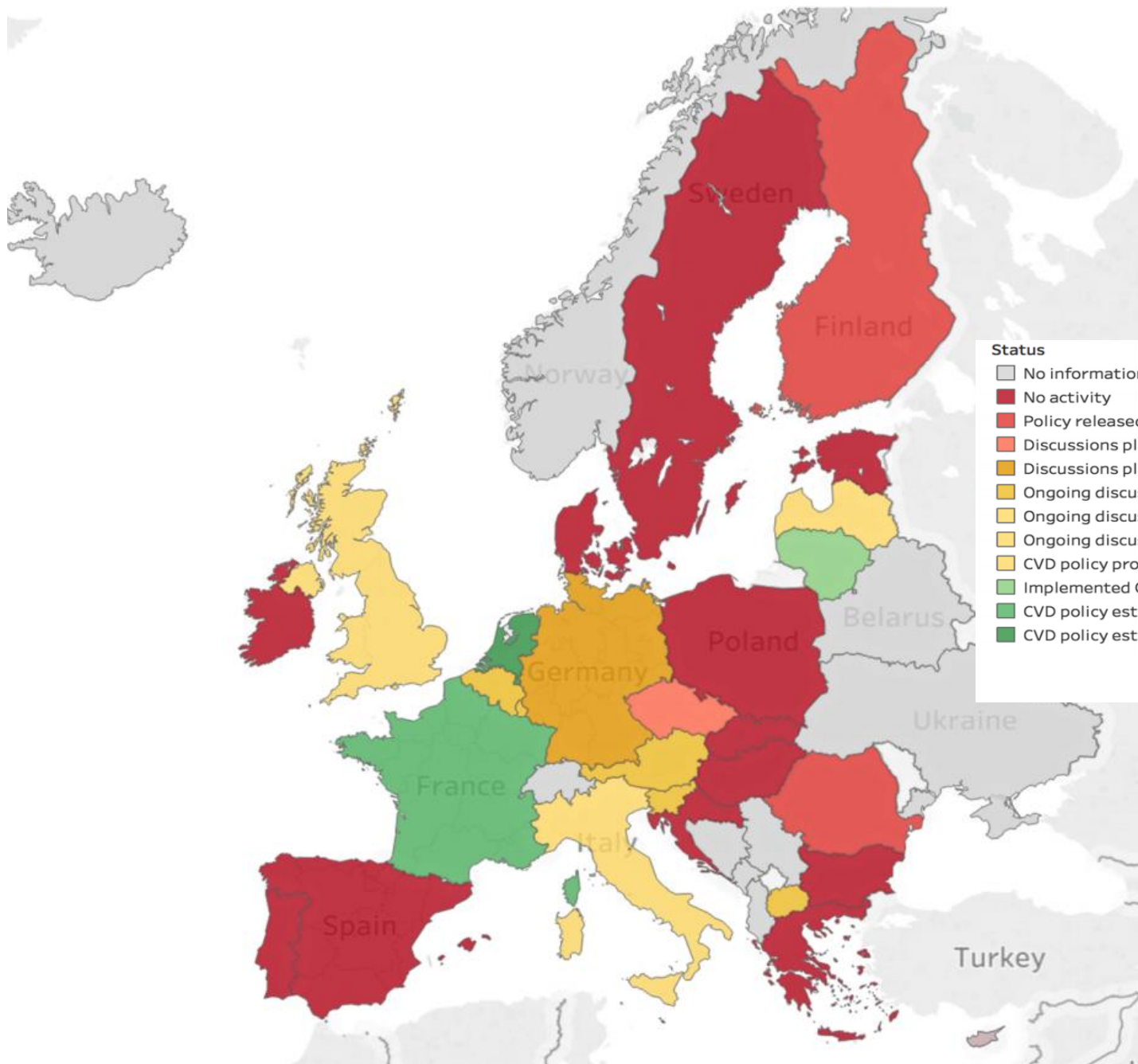
The City of Ghent will

BUT complaint is not required to
launch a criminal investigation

... not take any legal action against you.

... offer you the opportunity to be listed in their "Hall Of Fame".

... strive to solve all problems within a short period of time.



- Status**
- No information available
 - No activity
 - Policy released by their CERT, although there are no ongoing discussions and legal framework.
 - Discussions planned for 2018, although there is no legal framework.
 - Discussions planned for 2018
 - Ongoing discussions on this issue
 - Ongoing discussions and pilot
 - Ongoing discussions and preliminary work done
 - CVD policy proposed but failed to be incorporated in the law
 - Implemented CVD policy for a specific sector, ongoing discussions and national framework expected for summer 2018
 - CVD policy established, but partial protection of the researcher
 - CVD policy established, full protection of the researcher

Source: CEPS' own elaboration.

Dutch approach

Computervredereuk (art. 138a [Dutch Criminal Code](#)) = intentionally and illegally accessing a computer system:

- While breaching a security measure;
- With the use of a technical intervention;
- With the use of false signals, a fake key; OR
- By adopting a fake identity.

⇒ no distinction according to good/bad intentions of hacker

Punishment: imprisonment up to a maximum of two years OR a fine up to a maximum of 21.750 euros

Principle of **prosecutorial discretion**: internal guidelines (2013)

- Considerable general interest: security of personal data
- Proportionality: necessary in order to achieve the goal of general interest?
- Subsidiarity: other actions possible? Who was notified?



Ministry of Justice: ° 2013 [Guidelines](#) on “Coordinated Vulnerability Disclosure”

Cases?

- Court of Den Haag [17 December 2014](#)
Imprisonment of 12 months (8 months postponed) +
community service of 240 hours
- Court of Den Haag [30 August 2018](#)
 - Matter of general interest ✓
 - Pro~~portionality~~
 - Subs~~idiarity~~



N. FALOT, & B. SCHERMER, “De strafrechtelijke positie van de Nederlandse ethisch hacker”, *Computerr*. 2016, iss. 2, 94-100.

K. HARMS, “Positieve uitlokking van ethisch hacken. Een onderzoek naar responsible-disclosurebeleid”, *Netherlands Journal of Legal Philosophy* 2017, 196-207.

To conclude: when engaging in hacking activities...

(Ethical) hacking = (more than one) offence and thus punishable, but the judge decides in the end

Check Responsible Disclosure Policy (Unfortunately, no (inter)national approach (yet))

Or try to obtain the consent of the right holder of the computer system in advance

Do not “hack” more than necessary (do not damage or copy data)!

Notify the owner/responsible of the computer system immediately!

Question to the audience:

Should ethical hacking/security researching by “outsiders” be promoted as a part of the national cybersecurity strategy?

Legal intervention to exclude criminal liability, only civil liability when acting outside the scope of Responsible Disclosure Policy = desirable?

Thank you for your attention!

 sofie.royer@kuleuven.be

 @SofieRoyer