Criminal liability for ethical hackers in the EU

N. Falot LLM

CONSIDERATI

Hacking

Convention on Cybercrime
Article 2 – Illegal access
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.

Directive 2013/40/EU on attacks against information systems
Article 3 - Illegal access to information systems
Member States shall take the necessary 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.

Hacking

Criminal offence

- Convention on Cybercrime
- Directive 2013/40/EU on attacks against information systems
- National legislation

”Criminal liability of ethical hackers in the EU” – N. Falot LL.M.

Hacking in the Netherlands

Purposefully and **unlawfully** entering an automated work, or part thereof.

Examples of entering:
- By breaching security measures
- Through technical interference
- Through false signals or false keys
- By assuming a false identity

”Criminal liability of ethical hackers in the EU” – N. Falot LL.M.

CONSIDERATI

Ethical hacking = Lawfull hacking?

”Criminal liability of ethical hackers in the EU” – N. Falot LL.M.

Black hat or white hat? Does it matter?

@Legosteentje

GHZ (Groene Hart Hospital)

Radboud University vs Volkswagen

IN·DEI·NOMINE·FELICITER

Radboud Universiteit Nijmegen

CONSIDERATI

Discussion

Does RD condone criminal behaviour?

What if the user and owner of the IT system are different entities?

When is behaviour ethical?

Can a policy exclude research methods?

What happens in cross-border situations?

Responsible Disclosure

Security through obscurity vs. Full disclosure

Responsible Disclosure / Coordinated Vulnerability Disclosure

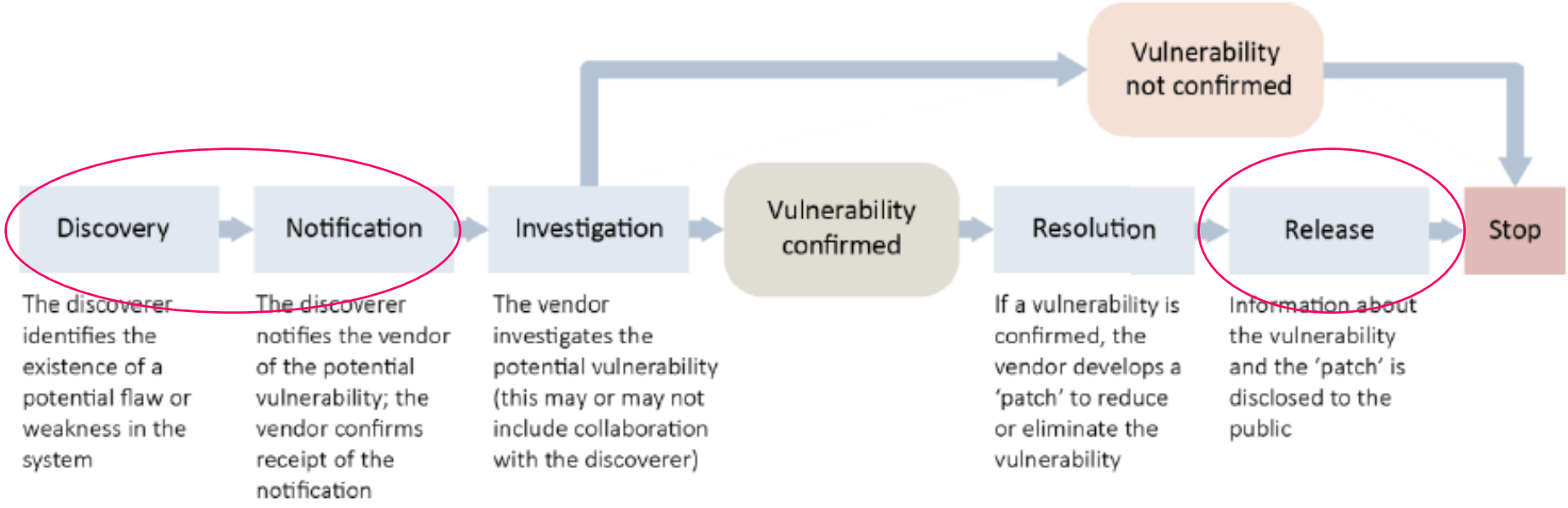
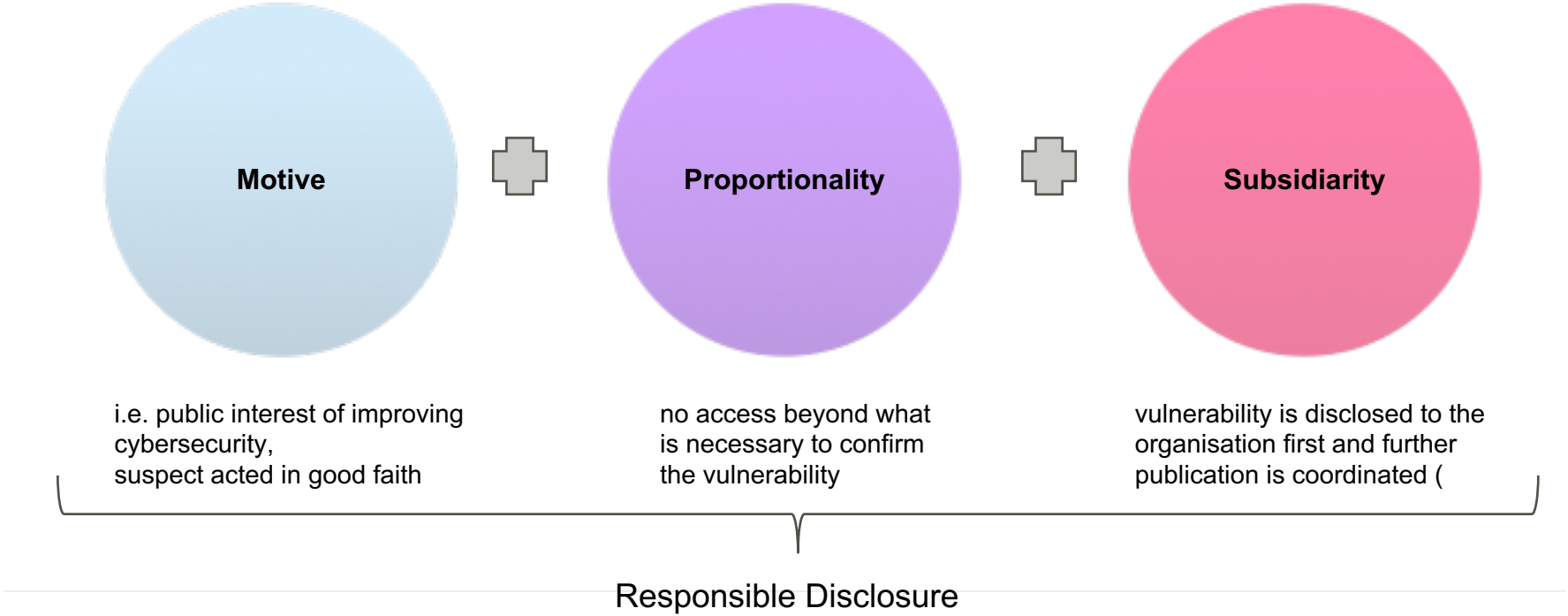


Figure 9: Key steps involved in the disclosure of security vulnerabilities[36]

Establishing (un)lawfulness of hacker's behaviour (NL)



"Criminal liability of ethical hackers in the EU" – N. Falot LL.M.

CONSIDERATI

Does the same framework apply in cross-border cases?

Criminal liability in cross-border cases

1. Extradition in the EU
2. Criminalisation of hacking in other Member State
3. Applicability of responsible disclosure in that Member State

1. Extradition in the EU

Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States

Article 2: The following offences, if they are punishable in the **issuing** Member State by a custodial sentence or a detention order for a maximum period of **at least three years** and as they are defined by the law of the issuing Member State, shall, under the terms of this Framework Decision and **without verification of the double criminality of the act**, give rise to surrender pursuant to a European arrest warrant:

[…]
Computer-related crime
[…]

2. Criminalisation of hacking in other EU Member States: Germany & Belgium

Germany: §202 etc. StGB - unauthorized access to data

- Broad classification of hacking
- Unlawfulness is not an element
- Detention of maximum three years

Belgium: art. 550bis Sw

- Internal and external hacking
  - Internal: purposefully and with fraudulent intent
  - External: Any form of attack
- Unlawfulness is not an element
- Detention varies, can be three years

3. Responsible disclosure in other EU countries: Germany and Belgium

Germany:

- Hacking is an ***Antragsdelikt*** **(**offence which cannot be prosecuted without a complaint by the victim)
- Room for self-regulation through Responsible Disclosure policy
- Public Prosecutor has to investigate after complaint
- Criminal liability therefore depends on commitment from organisations

Belgium:

- Public Proscecution can create policy on criminal investigation and proscecution: no such policy for ethical hacking
- DoJ: any form of hacking, even with good intentions, is unlawfull
- Little to no room for justification of hacking in legal system
- Belgian parliament intents to create room in legal framework for ethical hacking

Enisa: Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations

“To conclude, one of the primary challenges to focus upon, and the primary recommendation to put forward with respect to policy development, 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. A critical evaluation of the legal landscape, both in terms of criminal law as well as copyright legislation, is needed to ensure security research is appropriately facilitated rather than inappropriately obstructed.”*

Manifesto

Representatives of organisations who signed the Manifesto at the EU High Level Meeting on Cyber Security on 12 May 2016 in Amsterdam.

Conclusion

- Little legal certainty for ethical hackers regarding their criminal liability in cross-border cases

How to improve cross-border vulnerability reporting?

International law and policy:

- International views on accepted behaviour
- Cross-border cooperation in disclosure cases
- Cross-border legal protection

CONSIDERATI

Questions?

Contact

Contact

Nathalie Falot LL.M.
+ 31 6 31766087
falot@considerati.com

Considerati Algemeen:
info@considerati.com
+ 31 20 737 0069