Legal constraints in the implementation of CVD policies in the EU

Andriani Ferti
Senior Associate, Karatzas & Partners

CEPS, 29 November 2017

Background

- Council conclusions of 20 November 2017 on Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU
  - The Council "*welcomes the call to acknowledge the important role of third party security researchers in discovering vulnerabilities in existing products and services and calls upon Member States to* ***share best practices for coordinated vulnerability disclosure***" (conclusion no 27)
- ENISA's "Good Practice Guide on Vulnerability Disclosure"
  - "*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***" (page 70)
- As noted in our presentation of 29th June 2017, the legal challenges include:
  - Cyber criminal law
  - Data protection law
  - Intellectual and industrial property law
  - Export control regulation

A quick refresher concerning the legal challenges

- Copyright claims
  - Information disclosed may include copyrighted parts of the vendor's computer program
  - Disclosure may circumvent DRM technology applied on the software
  - Existing exceptions would be difficult to apply to CVD
- Trade secret claims
  - Especially when the researcher has previously worked for the vendor
- Patent law claims (to the extent applicable)
- Trademark claims
  - Disclosure infringes on the vendor's trademark rights (although unlikely to lead to consumer confusion)
- Export control regulation
  - Would bug bounty programmes fall into the scope of "intrusion software"?
- Data protection law
  - *E.g.*, unlawful processing of personal data, security breach involving personal data
- Cyber criminal law

Examples of coordinated vulnerability disclosure (CVD) policies around the EU

- Dutch CVD Initiative
- CVD model in Latvia
- Italian initiative of the Digital Transformation Team
- Initiative by French National Cybersecurity Agency (ANSSI)

What are the concerns when looking into CVD and its relation to criminal law?

- Substantive
  - When would CVD be considered a criminal offence?

- Procedural
  - Should CVD be considered a criminal offence, in which circumstances can it be prosecuted?

Which are the relevant legislative instruments in the EU dealing with hacking as a criminal offence?

- 2001 Council of Europe Convention on cybercrime (the "Cybercrime Convention")
  - 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,* [(a)] ***when committed intentionally,*** [(b)] *the* ***access*** *to* [(c)] *the* ***whole or any part of a computer system*** [(d)] ***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,* [(a)] ***when committed intentionally,*** [(b)] *the* ***access*** [(c)] ***without right,*** [(d)] *to* ***the whole or to any part of an information system****, is punishable as a criminal offence* [(e)] ***where committed by infringing a security measure****, at least for cases which are not minor*"
  - Sets *minimum* protection to be afforded by Member States (*i.e.*, they can introduce stricter requirements)

- National legislation

No single interpretation of what constitutes hacking – examples

- Netherlands
  - *Purposefully* and *unlawfully* entering an automated system
  - Entering an automated system can happen by means of, *e.g.*, breaching security measures, technical interference, false signals / false keys, assuming a false identity
- Belgium
  - Broad interpretation of hacking – no need to show that security measures are breached
  - Distinguishes between internal or external hacking
    - Internal hacking would require access to be done purposefully and with fradulent intent
  - Unlawfulness (*i.e.*, access happening without right) is not required
- Germany
  - Broad interpretation of hacking – no need to show that security measures are breached
  - Unlawfulness element is not required
- Greece
  - Definition of illegal access reflects Directive 2013/40
  - Distinguishes between internal and external hacking
  - Unlawfulness is required

Ethical hacking

- What is ethical hacking?
  - It requires that prior authorisation is granted to the researcher by the system owner
- Does the notion of ethical hacking exist in criminal law?
  - No
  - This is also confirmed in the letter sent by the Dutch Public Prosecutor to all its departments in relation to CVD

How did the Dutch prosecutor ensure compliance with criminal law?

- How did the Dutch prosecutor work around the absence of the notion of ethical hacking in the law?
  - Establish *unlawfulness/lawfulness* of the act – three principles
    - Motives
      - What are the ethical motives of the hacker?
    - Subsidiarity
      - If once a hacker discovers a vulnerability, he discloses this to the system owner → ethical hacking
    - Proportionality
      - If he ***does more*** than that (intentionally or unintentionally), the prosecutor will probably launch a criminal investigation
      - *E.g.*, copying of sensitive data or personally identifying information

What would be the impediments implementing the Dutch policy in other Member States?

- Divergent transposition of Article 3 of Directive 2013/40
  - Requirements to show illegal access can vary
  - Unlawfulness is key to the implementation of the Dutch policy, but not transposed in all Member States
    - However, general principle in criminal law that there should no criminal liability for whatever action if this action is carried with according rights
    - This principle is also acknowledged in EC Report regarding transposition of Directive 2013/40
- A practical impediment as to how the adoption of such policies works in other Member States, and what its legal effect would be

Criminal prosecution in the EU

- As a general rule, prosecution takes place *ex officio* (*i.e.,* there is no need for a complaint in order for the public prosecutor to prosecute)
  - The law explicitly provides for the crimes in which prosecution is dependent on a complaint by the victim

- 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*

- However, the situation is different, 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
  - Nonetheless, it appears more common to deal with *ex officio* prosecution in relation to computer crimes rather than not

Criminal prosecution of ethical hacking

- It appears therefore that in most Member States, prosecution of actions in the process of a CVD that may constitute illegal access will happen *ex officio*
  - This includes the Netherlands
- Then, why wouldn't the Dutch model work in other Member States as well that provide for *ex officio* prosecution?
  - In the Netherlands, prosecutor has the right to exercise prosecutorial discretion (*opportuniteitsbeginsel*)
  - Similarly, in the UK, Crown Prosecution Service has wide discretion
  - However, even in cases where no prosecutorial discretion *per se* exists, there may be other ways to exercise discretion (*e.g.*, mediation penale in France)
  - Moreover, normally, if there is lack of evidence, the prosecutor would not be able to pursue the prosecution
- Of course, in the case of Member States where a complaint by the victim is required (*e.g.*, Germany and Greece), then needless to say that the adoption of the policy would of course be helpful guidance, but not necessary

How about France?

- What does 2016 *Loi pour une République Numérique* provide?
  - *« 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* [*i.e.,* ANSSI] ***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. »
- It appears that the French legislature explicitly provides for an exception to the prosecution in the case of CVD
- Couldn't other countries follow the French example and legislate accordingly?

Cross-border nature of hacking / CVD

- There are no geographic silos when it comes to CVD

- For example, CVD may concern a computer system in the Netherlands, but the researcher may be located in Belgium
  - The researcher may be subject to the laws of both jurisdictions
  - What happens?
    - Legal conundrum – the researcher may not be subject to prosecution in the Netherlands, but he may be in Belgium
  - Lack of legal certainty

Lessons learnt

- The positive example of the Dutch model underscores the importance of improving legal certainty within the community
  - Public prosecutors in Member States adopting relevant policies would help, but only to the extent this guidance would have a practical impact
  - Query whether introducing relevant legislation similar to the French law would be an additional step to enhance legal certainty

- Coordination between Member States is needed
  - The differences in the transposition of Directive 2013/40 are telling
  - Sharing best practices is key to ensure legal certainty

- Need for more harmonisation at EU level
  - But how?
  - And to what extent?