ecrime
The Economic Impacts of Cyber Crime

Session 2: Regulatory reforms that could assist in the fight against cyber crime

24 March 2017

Prof. Jeanne Pia Mifsud Bonnici & Dr. Bo Zhao
Security, Technology and e-Privacy Research Group
University of Groningen, The Netherlands

SEVENTH FRAMEWORK PROGRAMME

Overview and plan

ecrime
The Economic Impacts of Cyber Crime

1. Reflection on the current regulatory and enforcement frameworks

2. Particular attention to issues of privacy, proportionality and cross-border implications

3. Reflection on recent developments

4. Top-level policy and regulatory recommendations

Trends and shifting cybercrime landscape

ecrime
The Economic Impacts of Cyber Crime

- the internet (as information infrastructure) becoming the backbone of most critical infrastructures of our society, including healthcare, emergy, finacial services, transportion, retail, etc.
- widespread dataficiation and digitalization
- growing use of automatic technologies: robotics and neuro-technologies
- more IoT: the weakest link in connected networks
- focus of human life shifted to a hybird of both online and offline spaces
- the ‘invisible hands’ of states
- darknet, encryption and cryptocurrencies

New challenges in sight

ecrime
The Economic Impacts of Cyber Crime

- cybercrimes increased in number, variety and damages; most simple and traditional attacks but a few abusing new techniques
- attacks and threats from abusing vulnerabilities in fast deployment of new technologies, i.e., the 4th generation attacking IoT
- via human errors, and low price and low security devices
- cross-border & cross continent cybercriminal activities
- national states backed criminal activities: military or economic espionage
- most non-ICT sectors are impacted and targeted for different purposes: credential data are new target for complicated fraud, ransom, or for extortion
- virtual currencies and darknet
- jurisdictional issues especially non-EU jurisdictions
- last: balancing (human) rights and public interests in cybersecurity

Current legal framework

ecrime
The Economic Impacts of Cyber Crime

- The landscape is constantly changing: not only the nature of crimes and technologies change, but also policies, best practices and players in the field.

- There is fragmentation as regards legislation and policies as well as actors

- On a European level the Cybercrime Convention remains the central frame of reference….supported by various EU documents…and national frameworks (as ratified by almost all EU Member States).

Benefits of the Cybercrime Convention

ecrime
The Economic Impacts of Cyber Crime

- Legal basis and uniform definitions, concepts and standards
  - On substantive level
  - On procedural level

- In particular on procedural level
  - Common and specific rules and procedures of collection of evidence
  - Agreed specific investigative measures
  - Set up for expedited collaboration between states following the Convention

ecrime
The Economic Impacts of Cyber Crime

Remaining difficulties of the Convention

- Effective cross-border investigation is problematic – jurisdictional difficulties
- Lacking clear rules on how to obtain information/evidence from private sector actors
- Mutual assistance procedures still very slow (especially when information/evidence is required from private sector)
- Rules on transfer of transfer of actionable intelligence from intelligence agencies and LEAs and vice-versa non-existant

Cybercrime convention

ecrime
The Economic Impacts of Cyber Crime

What works	Limitations	Reforms needed to address gaps in
Legal status (binding)	Possible reservations	
Number of states that have ratified the Convention		Number of states that are not party to Convention
Definitions of Crimes	Arguably newer crimes might not be covered	
Framework for international cooperation between law enforcement	Mutual Legal Assistance arrangements are too slow an arrangement to get timely evidence	No arrangements for investigations outside the territorial/physical boundaries of a state
		Lack of safeguards for fundamental human rights
	Lack of harmonisation of national laws	Lack of standardised ways of exchanging digital evidence
	Different national approaches to jurisdictional coverage of the substantive and investigative provisions	
	Different national powers of investigations and enforcement	

ecrime
The Economic Impacts of Cyber Crime

European Union Framework

- Complex set of directives and framework decisions

- Relevant recent examples:
- EU Directive on Security of Network and Information (the NIS Directive) – into force since August 2016
- The Europol Regulation (EU 2016/794) - On May 11 2016, the Europol Regulation was adopted and will come into effect on May 1 2018, replacing the Establishing Europol Council Decision (2009/371/HGA) and extending Europol's role and responsibilities in coordinating crime investigations
- Directive 2014/41/EU on the European Investigation Order (EIO) in criminal matters -from 22 May 2017 it replaces some of the most used Conventions of mutual legal assistance so far including the EU Convention on Mutual Legal Assistance in Criminal Matters of the Council of Europe of 20 April 1959, its two protocols, etc. The EIO Directive will establish a framework for a judicial authority of a member state to have one or more specific investigative measures carried out in another member state to obtain evidence.

Data Protection Framework

- The General Data Protection Regulation 2016/679 and
- Directive (EU) 2016/680 on protecting personal data processed for the purpose of criminal law enforcement)

    - Both will come into effect in May 2018

- Particularly relevant as more and more different environments where an investigation may be taking place also include access to personal information of not only the suspect and victim but also possibly of multiple other persons

Principle of proportionality

- Two important judgments of the European Court of Justice
  - Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others* (8 April 2014)
  - Joined Cases C-203/15 and 698/15 *Tele Sverige/Watson & Ors* (21 December 2016)

- Both cases relate to the now annulled Data Retention Directive. In both cases Court emphasises proportionality:
- The Court effectively adopted a two-pronged proportionality test:
  - considering whether the measure was appropriate to achieve its objectives and did not go beyond what was necessary to achieve them.
  - factors such as the importance of personal data protection for privacy and the extent and seriousness of the interference means that discretion to interfere with fundamental rights is limited.

EU framework

ecrime
The Economic Impacts of Cyber Crime

What works	Limitations	Reforms needed to address gaps in
Legal status of Directives and Regulations	Legal status of reports, communications, strategies, studies, resolutions	Patchwork of documents that are only applicable to Member States of the EU
Focus on a high level of NIS for the prevention of cybercrime	NIS Directive just came into force	Private sector involvement and preparedness
Strict Data Protection standards	Data Protection reform still to come into force	Data Protection rules do not apply outside the EU….though arguably in new framework they do
	Legal status of Privacy Shield in questions	

Cross-border issues

- The most used convention on mutual legal assistance so far is the Convention on Mutual Legal Assistance in Criminal Matters of the Council of Europe of 20 April 1959, its two protocols

- Processes based on convention are slow…and paper based

- Process in particular slow for information to be obtained from private actors in receiving country ….unanimous lament by all LEAs on slowness of process when needing information e.g. from internet service providers

A reflection on the EU cybercrime policy and legal development

- a right regulatory/governing approach?

  - the real impact/effectiveness of new legislation and policies in MSs and private sectors?
  - the momentum: more problems, more laws and more institutions?
  - difficulties in law implemetation and enforcement in the EU
  - the economic impacts of new legislations
  - too much regulation and intereference v. innovation
  - authority of EU legislators and the competency of the EU as a political institution
  - ----------
  - legal/political paternalism

ecrime
The Economic Impacts of Cyber Crime

Top-level policy/law recommendations

“Making hard laws really hard and soft laws really soft.”

Hard law

-Less hard laws and less direct interference in private sector

-Qualitatively better legal frameworks with generality and predicability

….and forward-looking

-very well implemented and transposed in MSs

-more investment in cybercrime law enforcement and public awareness

Soft laws

- move towards more self-regulation in form of industrial policies, gudelines, standarization, or aimed at platform building

- more initiatives from the private sectors to incoporate and test innovative measures in cybersecurity

- better and clearer collaboration between private sector and law enforcement: e.g. through memoranda of understanding and more efficient collaboration frameworks

Top-level policy/law recommendations

Cybecrime prevention should be the main focus of European regulators, especially of member state regulators.

To fight cybercrime needs systematic, collaborative efforts of both the ICT sector and the non-ICT sector, as well as service users including individual consumers and industrial customers, to create much safer cyber eco-systems.

To improve systematic cybersecurity requries imposing more accountability and responsibility on the players in the European cyber ecosystem.

National states should play a major role in securing critical information infrastructures by means of assisting with establishing mandatory industrial standards, while encouraging multistakeholder involvement.

Thank you for your attention

ecrime
The Economic Impacts of Cyber Crime

Any questions?

Bo Zhao
b.zhao@step-rug.nl

Jeanne Pia Mifsud Bonnici
g.p.mifsud.bonnici@step-rug.nl

Extra – just in case slides

The EU cybercrime policy and legal framework

ecrime
The Economic Impacts of Cyber Crime

General strategies:

-Cybersecurity strategy for the European Union (2013)

-European Agenda on Security (2015-2020)

-The Council Conclusions on Improving Criminal Justice in Cyberspace

-The Conclusions on the European Judicial Cybercrime Network

-The EU Cyber Defense Policy Framework

Major legislations:

-The Cybercrime Directive 2013/40/EU on attacks against information systems

-The EU Directive on Security of Network and Information (NIS Directive)

-The GDPR & Directive on processing personal data in LE & justice sectors

-The Directive on the European Investigation Order in Criminal matters

-The ePrivacy Directive (2002/58/EC)

- *other relevant policy documents, including:*
  - *communications*
  - *Council conclusions*
  - *resolutions*
- *new regulatory proposals and moves, e.g.,*
  - *Council Framework Decison 2001/413/JHA combating fraud and the counterfeiting of non-cash means of payment*
  - *Europan travel information and authorisation system (ETIASO and amending Regulations (EU) No. 515/214, (EU)216/399, EU(216 (794) and (EU) 216/1264*
  - *establishing a framework for security certification of ICT products and services*
  - *other sectoral initiatives...*
- *New EU institutions and agencies*
- *other countermeasures and activities*

- impoved international cooperations at the EU level regarding China, US, EaP partners, Candada, Austrilia, New Zealand, etc.

- Summary:
- There has already been a basic legal/policy framework responding to the present cybercrime challenges and many initiatives and collborative activities at the EU level, implementing the policy and law recommedations of E-crime's previous deliverables. however, their effectiveness and efficiency cannot be measured in a cost-benefit manner, especially the reality of adoption and implemention of EU law and policies at MS level