E-CRIME Policy Brief

Recommendations for Regulatory Innovations to Deter Cyber Crime

The E-CRIME Project (the economic impacts of cyber crime) is a three-year project that ran from April 2014 to March 2017. The aim of the project is to reconstruct the spread and development of cyber crime in non-information and communications technology (non-ICT) sectors from the perspective of its economic impact on the key fabrics (i.e., economic and social) and different levels of the European society, while also identifying and developing concrete measures to manage and deter cyber crime. (Website: http://ecrime-project.eu).

Cyber crime in the European Union (EU) is constantly evolving along multiple dimensions and thus posits fresh, dynamic challenges. This is reflected by new policies and regulatory measures being taken and implemented by EU and Member States' authorities to tackle growing cyber crimes in non-ICT sectors. This dynamic between the evolving EU cyber crime realities and the legal and policy developments, brings new challenges for EU regulatory authorities and non-ICT sectors; challenges that need to be addressed by exploring new policy and legal measures and innovations that can operate within these changing circumstances.

Most cybersecurity related issues are covered under a comprehensive EU legal framework in the forms of regulation, directives and other supplementary policy documents. There seem to be sufficient hard and soft law measures in the field, even though the prevailing momentum is that more legislation is needed to beat growing cybercrime challenges by criminalising more cyber behaviour, expanding investigative powers, and creating more institutions in cybersecurity. But the effectiveness and impact of producing more regulation and policies needs rethinking, especially in relation to hard law. Unresolved jurisdiction issues, limitations on expertise and resources, and differences and diversities in Member State cybercrime laws (possessing different legal cultures and political backgrounds) continue to negatively impact the implementation of the current plethora of EU hard laws. To simply create even more hard law both fail to address these existing issues, as well as adding to the corpus of EU hard laws that are not fully implemented. This non-implementation of hard law *per se* results in greater harm on EU law itself, and raises doubts about EU legislators. With respect to law enforcement and implementation, their resources are continuously diluted with each new regulation and directive that are enacted.

Thus our first strategic recommendation would be to ***make hard law really hard to best achieve the desired legislative goals, while simultaneously making soft law really soft to adapt to the diversified and complex circumstances in Member States***. This means the future policy and law focus should be on the implementation and enforcement of, and compliance with the existing laws and regulations. For instance, to make sure that the NIS Directive and Cybercrime Directive are best transposed into the national laws of Member States. By making hard law hard, it is meant that the obligations prescribed by EU regulations and directives to Member State authorities must be fulfilled on time with little compromise, such as the mandatory establishment of national institutions including competent national NIS authorities and CSIRTs, and national points of contact. It means the legislative ends of information, expertise and best practice sharing, and mutual legal assistance must be achieved by member states.

Another aspect to making hard law harder is ensuring that the national law enforcement agencies of member states have the capacity and competency – with adequate tools, techniques and expertise – to identify, locate, prosecute and punish key criminal individuals to create persuasive, permanent impact on the criminal community.

In contrast, to make soft law really soft means that policy makers at both the EU level and the national level should issue more non-binding guideline documents that are not mandatory but suggestive in nature. The guiding or directing force shall not come from the legislative or regulatory power, but from their professional expertise and experience, and in-depth knowledge of the regulated field. One such example is the large number of opinions issued by Article 29 Working Party regarding personal data protection that are commonly recognized as non-binding soft laws, but which have begun to be cited in multiple EU court decisions.

The compliance of those recommendations by the majority of players in the field can set up professional standards, while still allowing sufficiently deviated activities for innovation. Also, more soft law certainly means fewer hard laws and this will allow more judicial resources to be distributed to ensure better implementation and compliance. We suggest, however, that such regulatory measures (policies) of a soft law nature should be made via the proper channels of self-regulation or co-regulation that is supported or assisted by state regulatory authority.

Our second strategic recommendations is that ***cybercrime prevention should be the main focus of EU regulators, especially of Member State regulators***. In view of the present cybercrime landscape, Member States should take more active steps to implement preventive measures in all sectors that depend on Critical Information Infrastructures. This includes: cybersecurity education and establishing mandatory operation procedures to reduce human errors; establishing security roles and responsibilities; deployment of qualified digital devices and security programs; updating security software; information and best practices sharing inter-and-intra sector; incident reporting and alerts; cyber (security) exercises; and better access controls.

Member States should shoulder the most responsibilities by making short-term strategic plans based on their domestic circumstances. EU competent authorities may step in to provide cooperation platforms for mutual support and financial assistance to member states that may lack needed resources and technologies. Private sectors should make specific progress in the following fields: cybersecurity education programs; active participation in platforms or organizations for information and best practice sharing regarding cybersecurity; and adopting multiple measures to improve cybersecurity (i.e., adopting preventive measures, organizing cybersecurity exercises, making security updates and patch ups, hiring security staff, etc.).

A third strategic recommendation for law and policy makers is that fighting cybercrime requires ***systematic, collaborative efforts of both the ICT sector and the non-ICT sector*** to create much safer cyber eco-systems. First, the use of many low-cost but unsafe digital devices will create the weakest point on a service infrastructure that potentially can be compromised/abused for criminal ends when connected to larger networks. Thus, the ICT sector shall take more systematic initiatives to improve product safety such as creating and implementing minimum, mandatory security standards. Another efficient countermeasure is the establishment of professional certification/labelling mechanisms, so that consumers become educated in the security levels of digital devices they are purchasing. ***Thus, it is suggested that the selected non-ICT sectors should only choose products with sufficient security certificates within their supply chains. EU regulators shall encourage and support similar activities by providing technical and financial services*** across the EU to create a better cyber security environment.

Our fourth strategic recommendation is that ***to improve systematic cybersecurity requires imposing more accountability and responsibility on the players in the EU's cyber ecosystems***. Manufacturers should be held accountable and punished accordingly if they install/produce negligent security measures that lead to security breaches causing serious harms, even if they may be located outside the EU. Consequently, future IoT producers may pay more attention to the security features and security maintenances of their products during their whole life-cycles. ***Legislators, regulators and prosecutors should consider multiple liabilities of both service providers and device manufacturers whose negligence to meet pre-prescribed security criteria can be attributed in case of cybercrime***.

The fifth strategic recommendation is that national state authorities should take a major role in securing Critical Information Infrastructures by: assisting with the establishment of ***mandatory industrial standards***, providing multiple platforms for information, expertise and best practice sharing, building up cross-EU expert groups, monitoring law implementation, etc. For non-critical infrastructures and services, Member States and EU authorities shall only provide non-mandatory guidelines and financial support for cybersecurity training programs, without interfering with SME's daily operations. SMEs in non-critical sectors must able to decide which security standards they may meet and how much they spend on cybersecurity.

Recommendations for EU and MS Law and Policy Makers

Following on from these five reflections, E-CRIME makes the following recommendations for future regulatory strategies for EU and Member State law and policy makers:

a) **To make hard law hard and soft law really soft; and to make much less hard law, but more soft laws as non-mandatory guidelines at the EU level.**

b) **To strictly implement the "security by design and by default" requirements for ICT product producers and service providers;**

c) **To extend legal liability to device and service providers that take no effort to meet mandatory law standards or minimum industrial standards in case of cybercrime that is certain to occur;**

d) **To directly supervise and monitor the cybersecurity development in critical services (both in ICT and non-ICT sectors);**

e) **To support preventive measures by information sharing, expertise building and best practice promoting;**

f) **To cooperate with cybersecurity experts and teams in the private sector, better offering a clear role for the private sector, so that they do not operate in a grey area;**

g) **To develop effective means and capacities to tackle the abuse of the Darknet and virtual currencies for criminal purposes.**

Recommendations for Private (non-ICT) Sectors

For private (non-ICT) sectors, risk management and cybercrime prevention are the priorities. Our recommendations here are as follows:

a) **We recommend that genuine focus should be on law compliance and implementation at both EU and Member State levels.**

b) **We recommend the following issues to be tackled by means of more soft law measures:**

- Differentiate the legal status of critical service sectors and none-critical ones in implementing cybersecurity measures;
- Mandate key cybersecurity measures/procedures for critical infrastructure operators, including stricter control on access to networks, security training for employees and operators, establishing security procedures and policies, setting up emergency procedures and back up plans to reduce loss, clarify security duties among employees using secured devices, active participation in information sharing platforms, a cooperation plan with LEAs in cybercrime investigation and detection, etc.
- Encouraging and supporting non-critical infrastructure sectors to take multiple cyber security measures to prevent cyber incidents, by providing free, public platforms for information and best practice sharing, security consultancy, legal and technical aids, free training, introducing safe, cost-efficient devices and services, etc.;
- Encouraging or mandating cyber (security) insurance development with multiple means to mitigate potential losses, including more empirical data input, providing a state-supported re-insuring program, etc.,
- Drafting specific cybersecurity strategic plans to support SMEs that lack sufficient budget and personnel who focus on cybersecurity.

This policy brief is drawn from the work undertaken in D8.3, led by the team at Rijksuniversiteit Groningen