ecrime

The Economic Impacts of Cyber Crime

Newsletter: Policy Brief – Recommendations for Regulatory Innovations to Deter Cyber Crime

Number: 10 – 15 March 2017

As part of the work undertaken in the final year of the ECRIME project, colleagues at Rijksuniversiteit Groningen led an investigation into the existing regulatory and legal frameworks within the cybersecurity field.

It is well understood that cybercrime in the European Union (EU) is constantly evolving along multiple dimensions, which in turn creates ongoing, dynamic challenges. This is reflected by new policies and regulatory measures being taken and implemented by EU and Member States' authorities to tackle growing cybercrimes in non-ICT sectors. This dynamic between the evolving EU cybercrime 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.

Top level European experts from several scientific domains and different industrial sectors have started to investigate the economic impacts of cyber crime in Europe

The key objectives of **E-CRIME** are:

1. To measure the economic impact of cyber crime on non-ICT sectors
2. To analyse the criminal structures and economies behind such crimes
3. To develop concrete measures to deter such crimes

http://ecrime-project.eu/

FOLLOW US ON

@ECrimeproject

E-CRIME project has received funding from the European Union's Seventh Framework Programme for Security under grant agreement no 607775