EUnited against crime: Improving criminal justice in European Union cyberspace:

Tommaso De Zan
Junior researcher, International Affairs Institute (IAI)

Wednesday, 23rd November 2016

BACKGROUND

- In today's **ultra connected world**, much of our life occurs online (Can you imagine living without the internet for even one day?)

- We live in the so-called "**Information Society.**"

- Increased connectivity and more powerful processing tools have not only fostered social and cultural developments, however:
  - **Cybercrime** is on the rise;
  - **Terrorist organizations** are increasingly using ICT and cyberspace to advance their purposes;
  - Traditional **organized crime groups** are moving their operations on the web.

- The collection of **e-evidence is becoming crucial** to successfully prosecute all criminal offences.

RESEARCH QUESTIONS AND PRIMARY SCOPE

- In June 2016, the Council of the EU highlighted the importance of **improving criminal justice in cyberspace** (enhanced cooperation with service providers, reorganization of Mutual Legal Assistance (MLA) proceedings, and enforcing jurisdiction in cyberspace).

- The primary scope of this paper is to **feed some "suggestions" into the ongoing debate** within EU institutions on how to effectively prosecute crime in cyberspace.

- This report seeks to do so by answering **three main questions**:
  - What are the main challenges EU member states face today when collecting e-evidence?
  - How are they tackling these issues?
  - Can an EU framework provide a common solution?

Why are these questions important to answer?

- Law enforcement agencies should be **fully equipped to prosecute criminals and terrorists** using cyberspace.

- **International judicial cooperation should be consolidated** (at the moment it is quite disorganized: MLATs are reported to be slow and inefficient; jurisdiction is difficult to enforce because data are stored and/or move across jurisdictions; law enforcement agencies are unhappy about cooperation with service providers; service providers are unhappy about the incongruous system in place; countries are "unilaterally" taking aim at these problems).

- **Privacy should be protected** and government authorities should not indiscriminately access citizens' data.

Report Structure

- **Section 1**: Background, research questions and assumptions.
- **Section 2,3 4**: Three case studies, namely France, Germany and Italy. A set of common topics and questions was developed to allow for cross country comparison.
- **Section 5**: Details current legislative framework on criminal justice cooperation (Is the EU framework facilitating collaboration between member states and between member states and third countries?)
- **Section 6**: Analyses main member states' commonalities and differences in the context of the EU, and provides suggestions to improve EU criminal justice in cyberspace.
- **Conclusions**

Sections 2,3,4,5: Case Studies (France, Germany and Italy) + EU

- Only have 15 minutes, can't make it, sorry!

- You will find all the details you are craving for in the report (the report will be released tomorrow on IAI's website http://www.iai.it/it/pubblicazioni/lista/all/all ; in alternative, just send me an email t.dezan@iai.it).

Section 6: Improving Criminal Justice in EU Cyberspace (analysis)

Four macro elements are of major importance:

- Member states **empowered (or attempted to empower)** their law enforcement and intelligence agencies to effectively investigate crime and terrorism offences.
- They have **similar national legislative frameworks** (data protection codes, national criminal and criminal procedure codes, data retention policies and electronic communications code).
- **Judicial cooperation with the USA** is of primary importance because data are owned by US-based service providers.
- **EU as a common denominator**, but judicial cooperation still based on rather cumbersome MLATs processes.

Section 6: Improving Criminal Justice in EU Cyberspace (analysis)

At the Member State level, many seem to suggest that a **harmonized EU approach** might solve some of the issues delineated:

But what should this harmonization should look like?

Section 6: Improving Criminal Justice in EU Cyberspace (8 suggestions)

We provide 8 policy suggestions:

1) The **subject-oriented approach** should determine which country could be the "**investigating state.**"

However, the country of habitual residence of the person whose data is sought, is the country with the authority to send the production order for the disclosure of data to the relevant service provider.

Because it is offering its services in the country, the service provider should abide by the law of the country sending the production order.

(Please note that the service provider is not abiding by the order because it is merely offering its services in a country, but because the country which can legally send a production order has asked the provider to do so).

Section 6: Improving Criminal Justice in EU Cyberspace (8 suggestions)

2) A new EU common framework should provide clarity on definitions for the following:

- **Digital evidence**
- **Service provider** (definition also including "Information Society/Over-the-top" providers?)
- **Offering services** in the EU

Section 6: Improving Criminal Justice in EU Cyberspace (8 suggestions)

3) The principle of mutual recognition enshrined in the **European Investigation Order** (EIO) to e-evidence should be clearly applied.

(At the moment is not very clear whether it does. It may require amendment before being transposed into member states' legislation in May 2017).

Section 6: Improving Criminal Justice in EU Cyberspace (8 suggestions)

4) The EU should seek an **agreement on cross border data requests** with the USA.

   The Electronic Communications Privacy Act (**ECPA**) may need to be revised to allow service providers to disclose data to EU law enforcement agencies (the opposite should be made possible too);

   This seems plausible given recent legislative initiatives in the USA (International Communications Privacy Act – **ICPA**, May 2016) and recent international agreements with (exiting) EU member states (**US-UK cross border data requests**, July 2016).

Section 6: Improving Criminal Justice in EU Cyberspace (8 suggestions)

5) Specific mechanisms determining how service providers **handle production orders** and produce e-evidence (in case of dispute: third-party agency to decide upon most intractable cases?)

6) A new **data retention** regime, which should be aligned between the USA and the EU.

7) An enhanced role for **Eurojust** (suggestions on legal requirements depending on type of data?)

8) An enhanced role for **Europol** (dissemination hub in the field of digital forensics).

Conclusions

- The proposed policy suggestions do not offer all answers, but **might be a good place to start.**
- Once clear guidelines are established, every single actor in the game **must do his part** and play according to the same rules.
- Stakeholders should recognize that trust is **hard to build but easy to elapse**, and continuous revelations about opaque programs do not necessarily inspire such a sentiment.
- Snubbing the various stakeholders' needs will only exacerbate conflict and, instead of antagonizing imaginary "privacy vs. security" groups, **all actors should commit themselves to clear frameworks and collaborate to ensure their effective application.**