IGF 2017 Reporting Template

- Session Title: **Legal challenges in cloud forensics and cross-border criminal and counterterrorism investigations**

- Date: **20/12/2017**

- Time: **0900**

- Session Organizer: **Frank Pace**

- Chair/Moderator: **Frank Pace**

- Rapporteur/Notetaker: **Oskar Gstrein**

- List of Speakers and their institutional affiliations:

Jan Ellerman: EUROPOL
Markus Hartmann: Prosecutor's Office of Cologne, Germany
Christopher Kelly: Office of the Attorney General for the State of Massachusetts, USA
Ken Pennington: Policing Service of Northern Ireland
Maria Angela Biasiotti: Institute of Legal Information Theory and Techniques (ITTIG), Italian National Research Council
Patrick Curry: British Business Federation Authority (BBFA)

- Key Issues raised (1 sentence per issue):

Security & Freedom:

Law enforcement isn't facing an issue of Security vs. Freedom, but one of ensuring Security and Freedom is attenable and maintained in civilised society.

Scope of cybercrime:

There is no such thing as a "local" case in large scale incidents of cybercrime, all have an international nexus.

Pending legislation:

Cases pending in the United States Supreme Court are focused on the requirement for US law enforcement to meet a "search warrant" standard for probable cause, and a decision solely focused on the language contained in the Stored Communications Act of 1986.

Human rights:

Today's challenges in accessing and using remotely stored electronic evidence often presents issues of rights vs. rights, the approach by law enforcement must be proportionate, minimally invasive and with common legal authority.

International cooperation:

Cooperation between Academia, Industry and Law Enforcement is the key to creating viable solutions to the challenges faced in accessing remotely stored electronic data.

- If there were presentations during the session, please provide a 1-paragraph summary for each presentation:

Jan Ellerman from EUROPOL presented the efforts EUROPOL undertakes in regards to removing terrorist propaganda and darknet markets that promote illicit goods and services from the Internet. Jan explained that their success is only through the participation of individuals and other organizations that bring attention to sources in question. Importantly, he reiterated that EUROPOL, supports law enforcement with no enforcement powers itself, only providing notification to Internet Service Providers of the questionable material that they discover. This reinforces the need for cooperation and trust between the public and the law enforcement agencies that support them.

Markus Hartmann from the Cologne Germany Prosecutors Office, presented the current challenges faced by his office regarding the investigation and prosecution of cybercrime. As an example, Mr. Hartmann provided an overview of a ransomware case involving a Ukrainian software company that provides tax service software globally. The impact of the intrusion was a violation not only of the company on German soil, but that of the many victims throughout the world that used its product and services. This brought up the issue of a need for increased expediency, efficiency and international cooperation that does not currently exist. Mr. Hartmann highlighted the redundancy of multi-jurisdictional investigations of the same incident and a proposal for standards development and prosecution “clusters” that could alleviate the inefficient use of resources.

Maria Angela Biasiotti from the Institute of Legal Information Theory and Techniques (ITTIG), Italian National Research Council, presented on the challenges faced by law enforcement accessing remotely stored cloud data. Ms. Biasiotti highlighted the efforts of research projects such as the EVIDENCE project (European Informatics Data Exchange Framework for Courts and Evidence), which points to the need for increased collaboration between academia, industry and law enforcement and focused three main areas; Realities, Perspectives and Proposals for a path forward. She offered that the current patchwork of solutions, lack of standards and outdated capability of current Mutual Legal Assistance Treaty (MLAT) procedures has resulted in “creative” solutions that become the focus legal challenges and reinforce the need for solutions that address cross-border access to remotely stored data.

- Please describe the Discussions that took place during the workshop session (3 paragraphs):

The discussion following the session presentations was focused on themes surrounding current efforts at the United Nations and at EUROPOL in removing extremist content online; Mr. Kelly’s comments on pending legislation in the United States; and existing Cyber laws in Germany. Questions were received asking why remove terrorist info that may be of investigative value; how the US would respond in a hypothetical example in which the US Supreme Court rules against Microsoft and; clarification on what specifically German law enforcement can (and cannot do) in regard to removing hate speech online.

On efforts the United Nations is taking, Mr. Curry advised that the UN has several initiatives that work in cooperation with various governments, industry and NGO’s that aim to support the efforts of companies such as Google and Facebook. Mr. Ellerman clarified that EUROPOL submits requests for removal to providers that clearly promote violence or otherwise support criminal activity (such as with darknet markets) and that are in violation of the Terrorism Directive under EU law. Any examples of propaganda (i.e. displaying the of IS flag) are almost never submitted due to the overwhelming volume of more clearly questionable material that most likely violates terms of use and/or national laws. Mr. Kelly, was asked for his view on a hypothetical situation in which the US Supreme Court rules in favor of the Department of Justice in the Microsoft case, thus setting precedence for extraterritoriality. In this scenario, a request for data on a US citizen, originating from a Belgian court, is made to a US based provider that does not meet the US standard for probable cause. Mr. Kelly responded that this was a difficult area of the Stored Communications Act -which in this case- will only address the components of a request in which all parties involved are based in the US, but without regard to where the data itself is stored. Stating further, that this will ultimately be an issue that must be addressed by Congress, with the cooperation of industry and other nations. Mr. Hartmann added that solutions can only be found through the continued dependence upon and modification of the Mutual Legal Assistance Treaty (MLAT) system, addressing the underequipped and understaffed agencies responsible for investigation and prosecution.

Regarding efforts addressing the new law against hate speech, Mr. Hartmann explained that the hate speech legislation in Germany, is consistent with international norms and submitted as an example, that approximately 85-90% of submitted violations to his office, may be offensive, but are deemed not to be criminal acts. When asked if Germany should focus on the providers being in violation of the law, Mr. Hartmann explained that NGOs take the potential violations to the providers to act on. For their part, the prosecutors are working on efforts to streamline the process by which providers are notified, and subsequently, act on violations to their terms of service.

- Please describe any Participant suggestions regarding the way forward/ potential next steps /key takeaways (3 paragraphs):

The prominent theme leaving the session surrounded the need for updates to current legislation in both the United States and Europe. As with pending cases before both the United States Supreme Court and in various EU member states, resulting decisions are certain to have an impact on various facets of Internet Governance, to include cross-border access to electronic evidence.

Participants elaborated on the need for more transparency, trust and collaboration. Governments and legislative efforts are often slow, and in contrast to the speed of technological development. This reality, further supports the need to for industry, law enforcement and NGOs to increase their combined efforts to address the myriad of issues ranging from the removal of online hate speech and terrorist propaganda, to increasing investigative efforts against criminal market places on the darknet.

Contributions from members of civil society highlighted the challenges, and implications, that judicial and political decisions regarding internet governance have beyond the borders of any one nation. The dialogue included interventions that specifically call on policy makers to bring both national laws, and international treaties, in line with the 21st century challenges posed to society's increasing footprint, and vulnerability, within cyberspace.

Gender Reporting

- Estimate the overall number of the participants present at the session: 25-40

- Estimate the overall number of women present at the session: 5-10

- To what extent did the session discuss gender equality and/or women's empowerment? N/A

- If the session addressed issues related to gender equality and/or women's empowerment, please provide a brief summary of the discussion: N/A