IAP
International Association of Prosecutors

The Submission of the International Association of Prosecutors - Global Prosecutors E-Crime Network (GPEN) to the Parliamentary Joint Committee on Law Enforcement Enquiry into the New and Emerging Information and Communications Technology (ICT)

The International Association of Prosecutors (IAP) is the only world-wide association of prosecutors and has been in existence for over 22 years. It is a non- governmental, non-political organization. The need to establish such an organization was required by the rapid growth in transnational crime and thus the IAP was established in June 1995 at the United Nations offices in Vienna. The IAP has 172 organizational members from over 171 different countries, representing every continent, as well as many individual members.

The IAP is an international community of prosecutors committed to setting and raising standards of professional conduct and ethics for prosecutors worldwide; promoting the rule of law, fairness, impartiality and respect for human rights and improving international co-operation to combat crime.

Its mission is to be a world authority for prosecutors in the conduct of criminal prosecutions and associated matters and to operate as an organization of international repute and referral.

The IAP is based in The Hague and holds consultative status with The UN Social and Economic Council and works with the UNODC [United Nations Office of Crime and Drugs] which is based in Vienna. The IAP web site http://www.iap-association.org includes information of relevance to prosecutors with an interest in cross jurisdictional matters. The IAP holds Annual Conferences on topical themes as well as Regional Conferences with more of a training element for frontline prosecutors.

The Global Prosecutors E-Crime Network (GPEN) was launched as an IAP initiative at the IAP's 13th Annual Conference in Singapore in 2008. It was agreed at that conference that GPEN would in the area of Information and Communications Technology (ICT) be the IAP's main vehicle to promote training, heighten awareness, spread good practice and link with industry.

Prosecutors play an important role in the criminal justice system and they need to be trained to prosecute ICT cases and the use of electronic evidence. In order to enable the delivery of such training globally in a cost effective and sustainable manner GPEN supports and encourages regional ICT capacity building and has organized and sponsored regional training events for prosecutors, judges and law enforcement.

GPEN speeds up safe communication between specialists, enabling prosecutors to share best practice, knowledge and training, thereby raising standards and the chances of successfully prosecuting ICT cases across continents.

GPEN puts together extremely useful programs which start by raising the issues and obstacles that law enforcement globally faces such as the borderless nature of ICT crime, the multiplicity of jurisdictions involved, the challenges in detecting ICT crime and the difficulties in obtaining admissible evidence to support prosecutions owing to for example its temporary nature and volume and the need for

expertise and legislation in this field. We encourage delegates from different countries to learn from each other and share some of the solutions they have utilize to fight against ICT crimes: investigation strategies, international legal tools such as the Council of Europe Convention on Cybercrime and cooperative mechanisms. We have received feedback from delegates that the contacts that they make during such events and the network they establish is invaluable

ICT is constantly changing and is a crime without borders. Many jurisdictions around the world are woefully underprepared to investigate and prosecute cybercrime. ICT crime is the most fluid and hard to trace allowing criminals in most regions to stay far ahead of law enforcement. ICT crime is now a very topical subject and hardly a day goes by when there is not a story online or in the papers of an ICT crime being perpetrated somewhere in the world. Caution needs to be applied otherwise the general population will be of the view that cyberspace is basically unsafe, and that online crime is the norm and that cyber criminals are not brought to justice. With the speed of technological change, we can expect such innovations to be open to misuse by ICT criminals and therefore need to ensure that protection is factored in right from the beginning. The ability of governments to protect society against ICT crimes is of paramount importance.

We have highlighted below some of the challenges that prosecutors, judges and law enforcement personnel globally are dealing with arising from new and emerging ICT threats. We have also stated some of the solutions being used to address them.

Challenges:

The biggest challenge in the cybercrime investigation is firstly, to understand the criminal activity and secondly to prove it.

The anonymity of the technology involved makes it harder to trace people. The borderless nature of the internet makes it harder to track the defendant or obtain evidence quickly from other jurisdictions. The complexity of ICT crimes such as hacking, malware, ransomware, phishing, viruses, worms, Trojans, spyware, identity theft, distributed denial of service attacks (DDoS), social engineering, online stalking, harassment and child abuse images amongst others. Add to this the veracity of evidence and how it is obtained, and you can see how it can lead to lengthy arguments at court between expert witnesses. The volume of the evidence collected, and stored further creates implications for search and seizure procedures and the consequent duties of disclosure. In addition to this the legislation used to prosecute such offences often lags behind the technological developments.

There is the problem of detection of the crime, we are seeing now institutions acknowledging that they were hacked a few years ago but they have only recently detected the intrusion. The anonymity of the technology involved makes it harder to trace people, when you combine that with the problem that the evidence maybe encrypted it becomes even harder. With the borderless nature of the internet itself making it harder to track the offender or obtain evidence quickly from other jurisdictions. The involvement of organized crime and the surge in the sale of ICT criminal services has led to increasingly sophisticated ICT crimes.

With regard to the availability and accessibility of electronic evidence, the very fact that the Internet is borderless is the dominant challenge. This is especially true for cybercrime, where, for example phishing, ransomware and Distributed Denial of Service (DDoS) attacks allow a single criminal actor to have an almost immediate impact all over the world, thereby effectively turning the whole world into one big crime scene.

Also, it should be noted that particular forms of electronic evidence might no longer be found in possession of the ICT criminals themselves. Rather, that evidence can be found with the Internet Service Providers (ISPs), electronic communication providers and Cloud storage providers. These companies may not be incorporated or represented in the country where the crime is being investigated. And if they are, they may have stored the relevant data abroad or even distributed over multiple data storage facilities in a number of countries.

In a connected world more than ever criminal justice relies on access to digital evidence. Digital evidence may be the only way to link an act to a real person.

The issue of access to evidence in the cloud and related questions of jurisdiction must be resolved. This then brings to the fore the problem of jurisdiction and the borderless nature of the internet.

Nearly every cybercrime will involve more than one jurisdiction and therefore require some form of international cooperation. In cybercrime cases you can have parallel or competing jurisdictions. There is the need for clarity regarding jurisdiction some countries have domestic laws with extra-jurisdictional effect; and will limit the assistance they will give to another country on a matter if they have a jurisdictional claim or interest. If you look also at the different legal, investigative and prosecution systems and the fact that some countries will not extradite their own nationals. It can become very complicated and you can understand why countries require rules on negotiating jurisdiction.

In looking at international cooperation I have mention the Convention on Cybercrime of the Council of Europe (ETS 185), known as the Budapest Convention. The Budapest Convention is the only multilateral treaty dealing with cybercrime matters. It provides a global standard and it is already implemented in many countries (including Australia), and is being used as a guideline for drafting legislation on cybercrime by a number of countries. The Convention describes offences, outlines investigative and procedural requirements and mutual legal assistance imperatives. The Budapest Convention is the most obvious framework providing solutions to some of the challenges of ICT crime. The Budapest Convention sets out offences that criminalize ICT offending, and encourages effective international cooperation which is needed not only between Governments but also with industry.

Because of the borderless nature of cybercrime no one country can fully protect itself against ICT criminals but rather countries are dependent on the skills of law enforcement personnel in other countries to help protect cyberspace. ICT criminals typically hide in countries that are less developed, where the law enforcement personnel, prosecutors and judges are less efficient in the investigation and prosecution of ICT offences. All countries need law enforcement personnel, prosecutors and judges who understand the nature of the problem and cooperate together to investigate and prosecute these crimes in the most efficient manner.

Evidential problems

Digital evidence or electronic evidence is any information stored or transmitted in digital form that a party to a court case may use at trial.

Digital is like any other evidence, it must be: admissible, authentic and accurate. Each country has legal rules which determine whether potential evidence can be considered by a court for its probative value.

- Not obtained "illegally"
- Not excluded by statute
- Not excluded by judicial decision / discretion

Consideration needs to be given to questions such as:

- What links the person to the material recovered?
- What types of evidence are involved?
- Where is the evidence located?
- Has any data been generated by the investigators?
- Are any third parties involved and what role have they played?

In cases involving digital evidence you will generally require an expert to give evidence expert evidence usually consists not only of a description of scientific facts, observations and processes, but also of an opinion as to what these mean in the context of the case in question.

The first question that prosecutors need to ask is whether the subject matter of the opinion falls within the class of subjects upon which expert testimony is permissible.

The second question is whether the witness has acquired by study or experience sufficient knowledge of the subject to render his opinion of value in resolving the issues before the court.

Generally speaking, the justice system is not well placed to assess the expertise of a witness. As a result, these issues are normally resolved by the prosecution and defense calling their own experts to challenge the opinions provided by the opposite side.

The investigation and prosecution of crimes committed on the DarkNet

DarkNet (or Dark Net) is a network that can only be accessed with specific software (e.g. TOR), configurations, or authorization, it is not reachable through standard browsers and/ or search engines.

TOR is free software for enabling anonymous communication. The name is an acronym derived from the original software project name The Onion Router. Onion routing is implemented by encryption. Tor enables its users to surf the Internet, chat and send instant messages anonymously, and is used by a wide variety of people for both legal and illegal purposes. A number of DarkNet websites operate a criminal business model and illegally buy and sell stolen financial information and related items such as credit card deception, personal data, account takeovers, money laundering and hacking tutorials drugs, counterfeit currency, forged identity documents etc.... Virtual/crypto currencies and online money laundering which are topics in their own right are alleged to be rift on the DarkNet.

In spite of the many difficulties in trying to investigate crime on the DarkNet the United States and European law enforcement agencies in particular have had some success in disrupting activity on the DarkNet.

Other ICT topics to consider but not dealt with in detail above are:

- Virtual / crypto currency
- Online Money laundering.
- Mobile platforms as smart phones and tablets are no longer just used for communication.
- Radicalization on the Internet leading to terrorism has become a major problem.
- A major problem on the horizon is the Internet of things (IoT) this covers everything and anything with network connectivity allowing it to send and receive data. This includes connected cities, buildings, vehicles etc.
- Cyber warfare - Stuxnet is seen by some as the first detected instance of cyber warfare. It was specifically designed to work with specific hardware and software of nuclear power plants. The recent wave of politically motivated cyber offensives e.g. attacks on the White House and the US Department of Homeland Security show the need for a country to protect its critical national infrastructure.

Yours sincerely,

Han Moraal

Secretary-General of the IAP