Comments received in accordance with the workplan of the Expert Group on Cybercrime for the period 2018-2020

Reproduced as received
Status: Tuesday, 12 March 2019

The present compilation was prepared in accordance with the workplan for 2018-2021 of the Open-ended intergovernmental expert group meeting on Cybercrime, based on Commission on Crime Prevention and Criminal Justice resolution 26/4,[1] approved by the extended Bureau of the expert group on at its meeting on 26 January 2018, which *inter alia* states that:

> Prior to each IEG meeting, the Secretariat will invite Member States to provide, in writing, comments, good practices, new information, national efforts as well as recommendations regarding the meeting's main topics. Observers will be invited to provide relevant information. The Secretariat will then compile and disseminate the information collected not later than three weeks prior to the meeting.

An invitation to provide such comments was transmitted through Note Verbale CU 2019/4(A)/DTA/OCB/CSS. The comments reproduced below were received by the Secretariat within the extended deadline of 11 March 2019. A total of seven contributions were received from the following Member States: Australia, Canada, Guatemala, Jordan, Norway, Portugal and the United Kingdom.

Australia

In anticipation of the 5th meeting of the Open-Ended Intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime (IEG), Australia welcomes the opportunity to provide written comments on the substantive content in Chapter 5 (Law Enforcement and Investigations) and Chapter 6 (Electronic Evidence and Criminal Justice) of the Draft Comprehensive Study on Cybercrime.

Australia recognises the importance of balancing law enforcement access to data that allows effective investigation and prosecution of cybercrime and other crime that relies on digital evidence against appropriate safeguards and thresholds. Australia is committed to robust privacy frameworks, including recent reform under the Notifiable Data Breaches scheme. These reforms seek to enhance transparency and accountability between regulated entities, affected individuals, and Australia's independent national privacy regulator. Australia also recently introduced measures to modernise industry assistance for telecommunications interception and enhance computer access powers. These measures allow law enforcement and national security agencies to adapt to the use of encryption without undermining the security of the emerging technology.

Australia recognises the importance of strong partnerships and cooperation, both internationally and with digital industry, to address shared challenges in preventing, investigating and prosecuting

[1] Available at http://www.unodc.org/unodc/en/organized-crime/open-ended-intergovernmental-expert-group-to-conduct-a-comprehensive-study-of-the-problem-of-cybercrime2018.html

cybercrime. Australia has implemented measures to increase the reporting of cybercrime through awareness raising, cooperation with digital industry and enhanced cybercrime reporting avenues. In addition to existing avenues, the Office of the eSafety Commissioner introduced an online portal to report image-based abuse, which also provides practical advice and resources for victims. The Office of the eSafety Commissioner can issue take-down notices, requiring providers to remove illegal online content in response to reports.

The establishment of the Australian Centre for Countering Child Exploitation demonstrates Australia's strong commitment to collaboration to combat online child sexual abuse. The Australian Centre for Countering Child Exploitation coordinates operational functions across federal, state and territory law enforcement partners relating to evaluation and referrals, victim identification, and covert online engagement.

Australia invests in building Australian law enforcement and criminal justice capability to properly collect, interpret and use e-evidence to prosecute cybercrime and firmly believes that the international community should prioritise the provision of capacity building and technical assistance, especially for developing countries, to assist countries to build capabilities to investigate and prosecute cybercrime.
Australia continues to support capacity building, including through the provision of technical assistance, both through key regional bodies and bilaterally. Australia prioritises working with States in the Pacific to strengthen their criminal justice frameworks, including capability to collect, interpret and use e-evidence to support both domestic and international cybercrime efforts. The Australian Centre for Countering Child Exploitation also maintains an active role in international efforts to counter child sexual exploitation, particularly in South East Asia, where it provides support, training, and financial assistance to international law enforcement agencies.

Australia strongly supports actions to improve and facilitate effective access to evidence across jurisdictions, noting the increasing reliance on electronic material in a broad range of criminal investigations. Australia continues to be actively involved in the work of the Budapest Conference of the Parties (T-CY), including the development of an Additional Protocol to promote the use and sharing of data and information across jurisdictions to combat cybercrime.

Canada

Canada is pleased to reply to the United Nations Office on Drugs and Crime note verbale of January 18, 2019 (CU 2019/4(A)/DTA/OCB/CSS) regarding the organization of the fifth meeting of the Open-Ended Intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime (Expert Group), and to provide information on its national efforts related to the substantive issues included in Chapter 5 (Law Enforcement and Investigations) and Chapter 6 (Electronic Evidence and Criminal Justice) of the Draft Comprehensive Study on Cybercrime (Draft Study) produced by the UN Office on Drugs and Crime (UNODC) for further consideration by the Expert Group.

There is little doubt that emerging and evolving communications technologies clearly benefit all societies, however their use for illicit purposes creates significant public safety challenges. Many of today's crimes involve criminals using mobile cell phones or computers to send messages through the

Internet using new telecommunications capabilities. Unlike physical forensic evidence localized at a murder scene, digital forensic evidence can be scattered across dozens of devices that have accessed a multitude of Internet-based services which could be located in several jurisdictions. Further, this digital evidence does not only exist for cyber-crimes but for almost every type of crime because the use of webmail, texting services and social media by victims and perpetrators alike. Moreover, electronic data can exist along an entire spectrum of permanence, from being very volatile and transient to being stored on long term storage media. Consequently, investigative tools need to possess the agility to address a variety of scenarios.

It should also be noted that the 2013 Draft Study surveyed countries in the 2010-12 timeframe, so it is based on data that is about a decade old. In that time, the global roll-out of high speed Internet and mobile access has created the potential for every person, no matter where they are located in the world, to become a data producer. However, the consolidation of data holder jurisdictions, where much of that data is controlled and often located, is still primarily limited to a small number of countries. Accessing this digital evidence in a manner which is respectful of sovereignty and international law, will be one of the most pressing problem for law enforcement and prosecutors in the years to come. The discussions on Chapter 7 of the Draft Study at the meeting of the IEG next year will have to examine these issues.

Although there are investigative powers in existing laws that can be used to fight many crimes, they are in some cases no longer the right tools for complex investigations in the current environment, as they can become outdated with the evolution of technology. As pointed out in chapter 5 of the Draft Study, investigative powers that are tailored for obtaining evidence in the new telecommunications environment permit investigators, prosecutors and judges to realize new efficiencies that benefit the administration of the criminal justice system by being less cumbersome, more precise and also constrained to impair human rights as minimally as possible. Such powers may not be qualitatively new but rather an update of existing powers to respond to new technologies.

One of the objectives of Canada's efforts over the past years in the area of cybercrime has been to review its criminal legislation to ensure that it could address the realities of today's technologically advanced environment. The main challenge for Canada has been to ensure that national authorities have the procedural powers they need to conduct domestic investigations and prosecutions in relation to cybercrime and other crimes involving electronic evidence. With the coming into force of the *Protecting Canadians from Online Crime Act* on March 10, 2015, law enforcement agencies were provided with new tools, including an updated warrant and a new production order to obtain transmission data (i.e., data that relates to the routing of communications either by telephone or the Internet).

Another important tool that is now available to Canadian law enforcement officials is the preservation demand and the preservation order. This demand and this order can be used to require a telecommunication service provider (TSP) to preserve for a certain period of time specific data related to a specific communication or a subscriber, which the TSP already has in its possession or control and to protect the data from change or deterioration, if that data could assist in the investigation of an offence. Complementing Canada's legislation in this regard, a practical means to handle international requests for preservation was also introduced. Canada has developed a new centralized mechanism through the 24/7 Point of Contact to optimize requests for electronic evidence, including the

preservation of electronic data, in a manner that enhances its ability to address deconfliction when multiple agencies may be requesting the same data and to reduce the risk of unnecessary data destruction. The Royal Canadian Mounted Police's (RCMP) National Operations Centre (NOC) is the 24/7 point of contact.

An updated tracking warrant was also enacted to better recognize the expectations of privacy that people have in relation to themselves or objects. Issues around privacy were key in this work as the government understood the necessity of striking the balance between strengthening public safety and respecting the human rights and freedoms guaranteed to Canadians. As pointed out throughout the Draft Study, the ability to improve access to data for law enforcement needs to effectively protect human rights, and address public concerns about privacy at a time when increasing volumes of data are moving rapidly across borders.

The above-mentioned legislative amendments were required to meet Canada's domestic imperatives. However, they also allowed Canada to ratify the Council of Europe Convention on Cybercrime, better known as the Budapest Convention in 2015. Not only does the Convention deal effectively with the global nature of the Internet and criminal use of this medium, but it also provides an international solution in the fight against cybercrime. There are now 62 States Parties to the Convention, including a significant and growing number of non-European states. As evidenced by the issuance of Guidance Notes to help States Parties to apply existing provisions to new phenomena of cybercrime, the 24/7 network and the capacity building programme, the Convention is adaptable to emerging challenges. This is further demonstrated by the ongoing negotiation of a 2nd Additional Protocol to enhance international cooperation and access to evidence in the cloud as criminal investigations increasingly require access to information stored in other jurisdictions. The Convention has proven its usefulness in confronting cybercrime, and its on-going work on transborder access to data will continue to ensure its utility to States Parties into the future. Canada encourages UN Member States to consider joining the Budapest Convention or using it as a model for domestic cybercrime legislation.

The challenges to capacity and human and financial resources are well articulated in chapter 6 of the Draft Study. The rapidly evolving cybercrime landscape means that countries must continuously adapt their investigative methods, update their legal frameworks and cooperate internationally. While this poses a challenge for developed countries where many of the major private sector entities are located, it is a much greater challenge for developing countries, in which even basic legal and telecommunications infrastructure may be weak or absent. Cyber capacity building aims to help developing nations increase their access to, and ability to fully benefit from, the Internet and other elements of cyberspace by, for example, protecting Internet users and information networks, and supporting the development of capabilities of investigation and forensic analysis.

Since April 2015, the Anti-Crime and Counter-Terrorism Capacity Building Programs (ACCBP/CTCBP) of Global Affairs Canada (GAC) have disbursed $4.3M towards cyber capacity building projects in the Americas, with an additional $6.4M planned to be disbursed over the next two years. Canada's current international cyber security programming is provided through several international partners, including the United Nations, the Organization of American States (OAS) and INTERPOL. GAC is also working with the Royal Canadian Mounted Police (RCMP) to deliver Internet child exploitation investigative techniques training to law enforcement authorities and prosecutors.

Guatemala

El 20 de junio de 2018, el Viceministro de Tecnologías de la Información y las Comunicaciones, presentó la primera Estrategia Nacional de Seguridad Cibernética, la cual contempla entre sus ejes de trabajo la creación de un marco regulatorio, al igual que la creación de un Equipo de Respuesta a Incidentes (CERT por sus siglas en inglés).

En ese marco, se ha trabajado para apoyar al Congreso de Guatemala en el desarrollo de una Iniciativa de Ley contra la Ciberdelincuencia, la cual se presentó inicialmente el 8 de marzo de 2017; sin embargo, debido a observaciones de la Comisión de Derechos Humanos de la Organización de Estados Americanos, es necesario realizar ajustes a la redacción para adecuarla a estándares internacionales de aplicación de Derecho Informático y pruebas digitales. Por tales motivos se solicitó al Consejo de Europa el apoyo para la revisión de dicha iniciativa de Ley. El Consejo de Europa en el marco del proyecto GLACY+ envió una misión consultiva de expertos para realizar una revisión general, esta misión dio como resultado una propuesta bastante madura de esta iniciativa de ley, alineada a los requerimientos para poder adherir a Guatemala al Convenio de Budapest. Esta última versión se presentará al Pleno del Congreso en marzo de 2019.

Por otra parte, durante los años anteriores, el Ministerio de Gobernación ha trabajado en el desarrollo del GT-CERT, el cual es un equipo de expertos que analizan y responden ante incidentes informáticos, Se ha formado, como parte de este equipo, una Unidad de Informática Forense la cual está conformada por un equipo de peritos expertos en el manejo de evidencia digital basados en estándares ISO 27034 e ISO 27017.

Norway

We hereby provide updated information concerning activities – measures and initiatives against cyber crime, following the invitation in January 2019 from The Secretary General of the United Nations to the Permanent Representative of Norway to the United Nations (Vienna). We would like to apologise for the delay of our response.

The Norwegian Ministry of Justice and Public Security is pleased to have the opportunity to contribute to the compilation of good practices, new information, national efforts as well as recommendations. From the Norwegian context we would like to share the following:

In January 2019 the Norwegian Government launched a National Cyber Security Strategy for Norway. The developments in relation to previous national strategies are based on the need to reinforce public-private, civilian-military and international cooperations. Preventing and combating cyber crime is an explicit part of the strategy. The overall strategic objective is that the police have strengthened their ability to prevent and combat cyber crime. Police tasks are the same in cyberspace as in the physical world, with responsibilities to protect society and prevent, detect, investigate and prosecute crime. The police are faced with new demands in their work due to the current threats, e.g. regarding access to new technology, need for specialist skills and collaboration with other actors. The authorities will

improve the conditions for the police to carry out their tasks in line with technological developments and crime trends.

The strategy is accompanied by a list of measures:

https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/list-ofmeasures--national-cyber-security-strategy-for-norway.pdf

Some initiatives/measures are of particular relevance for cyber crime:

- *National cyber crime centre - NC3*

The National Police Directorate (POD) initiated in 2018 the establishment of a national cyber crime centre (NC3) under the National Criminal Investigation Service (NCIS/Kripos), following the example of many other countries. NC3 will serve as an expert body designed to improve the ability of the police to prevent and combat cyber crime. NC3 – formally established in January 2019 is currently staffed with about 80 people, with an aim to increase the number of staff to 200 people by 2022. The current units include digital forensics, internet-related investigation support, cyber crime investigations and investigations of online sexual abuse. NC3 will also assist the police districts and other units in the Norwegian police, as well as being a point of contact for international cooperation.

- *National cyber security centre*

The Norwegian National Security Authority (NSM) will establish a National cyber security centre, building on previously decided and established measures, basing its framework on a structure similar to those used in other influential countries with equivalent centres. The establishment is a key measure to increase private-public partnership in the area of cyber security. In order to ensure clear division of roles and responsibilities, it is important to establish good cooperation between the National cyber security centre and the national cyber crime centre (NC3) for the best possible utilisation of cyber security resources.

- *White Paper on future challenges - police capacity and competence*

The government will publish a white paper on changes in the crime landscape and the consequences of this for police assignments and services. The report will review and discuss current and developing crime trends and their consequences for police capacity and competence.

- *The Norwegian Police Security Service (PST)*

For 2019, funding for PST work on hybrid- and cyber threats was increased by 25 million NOK, ensuring PST has the personnel and technology necessary to improve capacity in cyberspace to detect, prevent, handle and investigate the most serious attempts at espionage, sabotage, influencing operations and compound (hybrid) threats.

- *International cooperation on cyber crime*

The Ministry of Justice and Public Security will promote international cooperation and participate in relevant international fora concerning Norwegian efforts to prevent and combat cyber crime. This includes cooperation within, for instance, the United Nations, the Council of Europe and the European Union.

- *Norwegian support to UN efforts to combat cyber crime at global level*

In 2018-2021, Norway contributes 35 million NOK to fight cybercrime through the UNODC's Global Programme on Cybercrime to the United Nations Office on Drugs and Crime. Norway's support will focus on developing countries, in particular in West Africa, the Middle East and North Africa as well as South East Asia, to build capacities to investigate, prosecute, convict and prevent cyber crime. The objective is to make a tangible contribution to save lives and apprehend criminals, locally as well as in cases across jurisdictions.

- *National electronic proof of identity (eID)*

The national ID cards are scheduled to be introduced in 2020 and will contain electronic proof of identity (eID). With this, the security level for electronic identification will be the same as for passports. A person can only have one national eID and the eID will be made available to both Norwegian citizens and foreign citizens who qualify for the national ID card. With the introduction of this scheme, ICT services that require the same level of security as passport identification can start using the national eID, thus reducing the risk of crime through fraud/misuse. It will be possible to use the national eID for both public and private sector services, and it is intended to serve as a supplement to other eID schemes available in the market. The security level for public services is defined in the "Framework and authentication and non-repudiation in public communication".

- *The Police's citizen survey*

The National Police Directorate initiates an annual citizen survey indicating the public's level of confidence in the police force. The survey provides valuable information about the public perception of safety and the impression they have concerning the capacity of the police to handle cyber crime.

Portugal

Portugal and the fight against Cybercrime

The fight against cybercrime is a matter of strategic concern to Portugal, that is strongly committed at this respect. Since 1991, Portugal adopted a law on computer crime (Law 109/1991), revised in 2009 (Law 109/2009 – The Cybercrime Law). In 2015, a National Strategy on Security in the Cyberspace was adopted, which is currently in the final stage of revision. A new National Strategy is expected to be published in the coming months. Both the *old* strategy and the *new* draft strategy consider cybercrime as one of the most important issues to face.

The international commitment

Portugal ratified the Budapest Convention on Cybercrime in 2009 and considers this international instrument crucial at this respect, since it provides a very good framework to allow to investigate and cooperate internationally. Even if it is an international treaty born in Europe, it became truly global, with 63 Parties in all the continents (more countries, from outside Europe, are expected to join the Convention soon). It is in force and effectively in place, allowing countries to cooperate with each other and providing the proper environment to develop common efforts against cybercrime.

In previous meetings of the IEG, the importance of the Budapest Convention was emphasised. A number of the members of the Group come from countries that are Parties of the Convention. In general, even beyond those who are Parties to the Convention, this treaty is recognised as a source of

inspiration in many jurisdictions, and also the main reference to capacity building programmes. Thus, the Budapest Convention is broadly recognised as a good treaty, and as a source of inspiration to national laws.

Portugal encourages all the countries that did not do it yet to join the Budapest Convention.

The work of the Intergovernmental Expert Group

Portugal attended all the previous meetings of the Group, actively taking part in the discussions, since considers that the IEG is the adequate forum, at the UN level, to discuss all the cybercrime related issues. Portugal contributed to workshops and debates, in a constructive approach, in view of reaching consensus and add value to the global fight against cybercrime.

The Agenda of the Fifth Meeting

As a result of the third meeting of the Expert Group, in April 2017, it was proposed to the Commission on Crime Prevention and Criminal Justice that IEG continued its work, holding periodic meetings, functioning as the platform for further discussion on substantive issues concerning cybercrime, keeping pace with its evolving trends, and in line with the Salvador Declaration and the Doha Declaration. The Commission approved this approach and decided that the Expert Group should exchange information on national legislation, best practices, technical assistance and international cooperation.

Portugal is prepared to share with the other members of the Group its law and practical experience at this respect, namely regarding the topics of "Law enforcement and investigations" and "Electronic evidence and criminal justice".

Internally, as mentioned before, a law on cybercrime was adopted, including procedural measures, fully in line with the provisions of the Budapest Convention. This is a very important point: there is a need, in each country, to have a proper domestic legal framework at this respect. Law enforcement agencies cannot investigate if the domestic law does not provide for proper procedural tools and powers, with respect of the safeguards of the suspect and the victims.

Also at this respect the Budapest Convention is a very useful instrument, as it describes a number of specific procedural tools that each country must adopt, domestically, in view of properly gather evidence related to cybercrime and also digital evidence related to all other types of crimes.

On the other hand, Portugal developed specialization on the law enforcement side: within the Prosecution, a Cybercrime Office was created in 2011 and at the police level, a special unit on cybercrime was also established, at the Judiciary Police. Both operate and coordinate at the national level. This specialization is considered a very important added value, as it brings efficiency in the concrete investigations. On the other hand, it ensures an holistic and consistent approach to the phenomenon and international coordination.

Along with the conclusions of previous meetings of the IEG, Portugal believes that efforts need to be made building capacities all over the globe, at this respect. On one hand, revisiting the national legal frameworks, in view of the international standards (namely the Budapest Convention) and also in view of supporting national authorities to develop special units on cybercrime.

Around this issue, there is an important topic to be discussed during the meeting: cross-border access to evidence. It is recognised, each day more, that all the investigations regarding crimes committed on the networks or with the use of networks, are potentially international. However, formal and traditional international cooperation (via the so-called MLA process) cannot correspond to these

growing needs of obtaining evidence. On the other side, digital evidence requires expeditiousness, since it is fragile and volatile. Finally, there is need of certainty at this respect, since there are no comprehensive international regulations in place and national frameworks state diverse solutions.

These issues are currently being discussed among the Parties to the Budapest Convention, who aim drafting an additional protocol to the Convention, exactly at this respect. Such legal instrument would have the benefit of providing guidance and legal clarity to law enforcement, when accessing to data cross-border. On the other hand, it is expected that such a protocol may improve informal cooperation, information sharing and also, last but not the least, improve in practice the functioning of traditional mutual legal assistance, while fully respecting fundamental rights and freedoms.

Portugal encourages Members of the IEG to follow the works around the drafting of this future Second Additional Protocol to the Budapest Convention.

United Kingdom

When considering topics related to the fifth intergovernmental Expert Group on Cybercrime, it is necessary to set out relevant definitions adopted by the UK in relation to tackling this threat. The National Cyber Security Strategy, 2016-2021, makes a distinction between two interrelated concepts in relation to cyber crime:

- Cyber-dependent crimes – crimes that can be committed only through the use of Information and Communications Technology (ICT) devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g. developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity); and
- cyber-enabled crimes – traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT (such as cyber-enabled fraud and data theft).

Recognising the response to these threats will often require common building blocks, the UK has developed programmes to enhance the general capabilities of law enforcement in order to adapt to the increasing prevalence of electronic evidence and/or a requirement for digital forensics skills in routine investigations. However, the UK also recognises that cyber crimes of all types are becoming increasingly ‘specialised’, warranting different strategies and approaches to tackle variances in offender profiles, behaviours, motivations and methodologies. The overall approach to tackling both cyber-dependent and serious cyber-enabled crimes is set out in the Serious and Organised Crime Strategy, published in November 2018. The National Cyber Security Strategy (NCSS) then focuses on the UK’s efforts to reduce the threat and harm from cyber-dependent (usually financially motivated) crime specifically.

Law Enforcement and Investigations

As set out above, the NCSS sets out the UK's transformational programme to improve law enforcement capabilities to tackle cyber-dependent crime. This is supported by a National Cyber Security Programme of £1.9 billion of transformational investment across all cyber threats, including cyber crime. The UK Government has invested over £100 million under the 2010-2015 Parliament to bolster the law enforcement response to cyber crime, and has invested over £80 million to bolster the law enforcement response since 2015. Work to improve law enforcement's ability to investigate cyber dependent crime includes:

- Boosting the capabilities of the National Crime Agency's National Cyber Crime Unit (NCCU) by increasing their ability to investigate the most serious cyber crime.
- Continuing to invest in the cyber teams within each of the Regional Organised Crime Units (ROCUs) across England and Wales in order to bolster the national and local response.
- Providing funding for the build of dedicated specialist cyber crime unit in all 43 Police Forces in England and Wales. This will ensure that local forces are able to provide an effective victim experience, an investigative response, targeted local cyber crime prevention messaging and undertake work to identify and divert young people vulnerable to going down the path to cyber crime.

A number of challenges remain to tackling this threat. Recognising that cyber crime is a borderless phenomenon, where victims and perpetrators can transcend regional and international boundaries, the UK has sought to ensure a joined up approach across law enforcement agencies tackling this threat. We have created the National Cyber Crime Unit which, as part of the NCA, has brought together law enforcement experts into a single elite unit. We also established a network of Regional Organised Crime Units (ROCUs) which include cyber crime units, to provide access to specialist capabilities at a regional level. The law enforcement response to cyber crime across England and Wales has therefore changed so that it operates as one nationally networked resource, able to react to any given situation and based on the best available intelligence.

Ensuring sufficient law enforcement officers are trained and retained to tackle cyber dependent crime also remains a challenge. The College of Policing are working on behalf of the Home Office to create the Cyber Digital Career Pathways (CDCP) project. This project recognises that non-traditional policing skills are valuable within the digital age, and different career pathways are needed to equip the modern workforce. The CDCP project will create a Cyber Digital Investigation Profession across all of law enforcement, providing a career pathway and professional certification for Cyber Digital Investigation Professionals who are defined as 'A person at the core of cyber digital investigations, who may have to present evidence at court of their cyber digital investigation skills'. The Career Pathway will create 'multi agency' standards within which Cyber/Digital Investigation Professionals are recruited, retained and developed. This will enable interoperability between police forces, wider law enforcement and partners, with the ultimate goal of setting the industry standard 'profession' of Cyber Digital Investigation/Security Professional.

In terms of tackling broader cyber-enabled crime, driving up cyber knowledge at the local policing level is also very important. In September 2016, the College of Policing launched the second phase of its Mainstream Cyber Crime Training course for police forces. This is a modular course consisting of a series of self-teach and interactive modules accessible to all police officers and staff, and which gives an introduction to how to recognise and investigate cyber crimes. This consists of two courses: 'Cyber

Awareness,' for all staff; and 'Cyber for Investigators', for officers and staff carrying out investigations. Currently in excess of 100,000 officers/staff have completed the cyber awareness modules. Finally, digital awareness for all front line staff and officers is a specific project of the Digital Investigation and Intelligence (DII) programme. This will upskill all staff from call handler/front counter staff through to response officers and local CID investigation teams. This is currently being scoped and will use findings from a 3 force pilot Project CRYSTALLISE on the best operating model to support the development of digital capabilities at local level.

Electronic Evidence and Criminal Justice

The UK recognises some of the major challenges regarding territoriality and access to data overseas in relation to tackling cyber crime. Increasingly, criminals are using global communications services to facilitate their criminal activities. This makes the data generated by those applications a vital source of evidence for the prosecution of criminal offences. Law enforcement agencies and prosecution authorities are clear on the value of obtaining the evidence that they need for their investigations and prosecutions as swiftly as possible, even when that data is held overseas. The majority of this relevant electronic data is controlled by service providers outside of the UK.

Currently when the required stored electronic data is controlled by a company based outside the UK, *Mutual Legal Assistance (MLA)* channels are used. MLA is a form of judicial cooperation between States that allows law enforcement officers and prosecutors to obtain data for evidence purposes from a foreign jurisdiction via relevant authorities in that jurisdiction. However, the MLA process can take time and, in some cases, may result in delayed or abandoned investigations or prosecutions. It can also delay people from being eliminated from a criminal investigation.

A new Act – the Crime (Overseas Production Orders) Act – has been established to overcome some of the delays associated to accessing evidence overseas. This provides UK law enforcement officers and prosecutors with the power to apply to courts for overseas production orders. These UK court approved orders will be capable of being served in a foreign jurisdiction where a designated international cooperation agreement exists between that country and the UK. These overseas production orders will allow appropriate UK law enforcement officers and prosecutors agencies (as set out in the Act and any subsequent additions made by regulation) to seek stored electronic evidence, mainly content data including messages, files, pictures, directly from overseas service providers for the purposes of investigation and prosecution of serious criminal offences only, including terrorism. This is likely to result in quicker access to this data to support domestic investigations and prosecutions of serious crime to secure criminal convictions.

Each application for an overseas production order will be robustly scrutinised by a UK court and subject to stringent tests set out in the Act. The provisions in the Act reflect our existing high levels of privacy protection, respect for freedom of speech and international human rights law in our similar UK process for applying for a domestic production order.

Discussions are also taking place amongst Parties to the Cybercrime (Budapest) Convention on drafting an additional protocol to enhance the provisions on sharing cyber crime evidence across jurisdictions. It aims to tackle systemic problems related to four key issues:

- lengthy delays in cross-border evidence-sharing on cybercrime cases;
- a lack of consistency in processes for sharing evidence across jurisdictions;

- the need for faster processes to access evidential data from communication service providers across jurisdictions; and
- the lack of legal clarity on law enforcement cross-border access to data.

The second Additional Protocol is an important element supporting the wider Budapest Convention framework, which includes its valuable role as a facilitator of joint discussion and international cooperation in tackling evolving international cybercrime. The UK are supportive of this work and believe it has the potential to offer a crucial building block to overcoming issues related to jurisdiction and evidence in the 'cloud' amongst Parties to the Convention.

Recommendations

The UK makes the following recommendations pertaining to Law Enforcement and Investigations, and Electronic Evidence and Criminal Justice:

- The UK encourages States to take practical measures to share best practice and provide assistance, where appropriate, to support the development of technical law enforcement capabilities required to tackle cyber crime. Where possible, States should also consider making voluntary contributions to organisations recognised for providing technical capacity building in this field (such as Council of Europe, UNODC and European Union, amongst others).
- The UK encourages States to develop appropriate cyber crime investigative capabilities within law enforcement. This should include embedding the investigation of such crimes within law enforcement organisations, as well as within national government and/or law enforcement strategies and priorities. Moreover, States should ensure that efforts to tackle cyber crime are mainstreamed within the criminal justice system, accompanied by appropriate human rights safeguards and oversight regimes for lawful use of investigative powers, rather than relying predominantly or exclusively on national security organisations and powers to address these crimes.
- Recognising its status as a global standard in addressing cyber crime, and its leading role in exploring solutions to improving e-evidence exchange, the UK encourages non-signatories to consider accession to the Cybercrime ('Budapest') Convention. Existing Parties should also participate to the fullest possible extent in discussions to develop the Second Additional Protocol to the Convention.
- States should explore national strategies and plans to develop appropriate cyber investigation skills, including the development of schemes intended to incentivise the retention of such skills within law enforcement.

Jordan

Please see below

الاجراءات المتخذة من وزارة الداخليه حيال الامن السيبراني:

١- تحديد البيانات الموجودة وتصنيفها حتى نتمكن من حمايتها فليس كل المعلومات ذات درجة اهمية وحساسية واحدة.
٢- القيام بتشفير البيانات ذات الحساسية العالية حيث ان التشفير من الممكن ان يوقف الهجمات عندما تفشل عناصر الحماية الاخرى الموجودة لهذه الغاية.
٣- تصنيف المعلومات وتقييد حرية الوصول وتطبيق احد مبادىء الامن السيبراني على المعلومات.
٤- تدريب العاملين على المحافظة على امنهم الخاص واعطائهم الاساسيات في الامن ابتداءا من كلمات المرور التي يستخدمونها في المحافظة على ملفاتهم الشخصية حتى نصل الى تأمين البيانات كاملة ومن خلاله نحدد مصدر التهديد الداخلي.
٥- الاستفادة من التجارب السابقة بخصوص الهجمات الالكترونية وذلك لبيان نقاط القوة والضعف في اجراءات الامان المتبعة.
٦- فصل عمليات وصول الموظفين للانظمة الحرجة عن وصولهم للانترنت.
٧- فصل الشبكات وعدم تداخلها حتى نضمن عزل تأثير الانظمة المعرضة للاختراق عن غيرها.
٨- توفير الاجهزة والبرمجيات اللازمة لمراقبة وتحذير وكشف الاختراق الالكتروني وتوظيفها بشكل فعال في عمليات المراقبة وكشف الاختراق.
٩- تحديث انظمة التشغيل والبرمجيات المثبتة على الاجهزة والخوادم الخاصة بالانظمة الحرجة بشكل دوري ومستمر.