Comments received in accordance with the Chair's proposal for the work plan for the period 2018-2021

Reproduced as received

16 March 2018

The present compilation was prepared in accordance with the Chair's Proposal for the 2018-2021 work plan 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 2018/47/(A)/DTA/OCB/CSS. The comments reproduced below were received by the Secretariat within the extended deadline of 14 March 2018. A total of fourteen contributions were received from the following Member States: Argentina, Armenia, Australia, Canada, China, France, Japan, Netherlands, Norway, Russian Federation, Singapore, Slovakia, United Kingdom and United States.

ARGENTINA

La República Argentina se encuentra tramitando la adhesión a la Convención de Budapest sobre Ciberdelicuencia. En efecto, dicho Acuerdo ya fue aprobado por el Congreso de la Nación Argentina y actualmente se encuentra en trámite el correspondiente instrumento de adhesión.

Dicha Convención, que fue firmada en Budapest el 23 de noviembre de 2001 en el ámbito del Consejo Europeo y entró en vigor el 1° de julio de 2004, es el primer instrumento internacional vinculante en materia de crímenes cometidos a través de internet. Su principal objetivo apunta a establecer una política criminal común destinada a proteger a la sociedad de los delitos cibernéticos, especialmente a través de la adopción de legislación adecuada y de promover la cooperación internacional.

Asimismo, el citado instrumento establece una política penal común ante la ciberdelincuencia, respetando los derechos y las libertades humanas y sugiere que los Estados partes deberán adoptar las medidas necesarias para tipificar como delito: los cometidos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informático, los relacionados con la falsificación y el fraude informático, las infracciones a la propiedad intelectual y la complicidad o tentativa de realizar cualquiera de los delitos mencionados, entre otros.

Por otro lado, cabe señalar que el 24 de junio de 2008 se sancionó en nuestro país la ley N° 26.388 por la cual se modificó al Código Penal Argentino. Dicha reforma incorporó un conjunto de delitos vinculados con la criminalidad informática teniendo en cuenta especialmente el modelo de normas penales promovido por la citada Convención. Posteriormente, se sancionó la ley 26.904 (B.O. 4 de diciembre de 2013) que incorporó como artículo 131 del Código Penal al siguiente: "Artículo 131: Será

[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

penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma".

ARMENIA

First of all we want to state that on November 24 of the 2017, during the European Union Western partnership 5th summit, EU-Armenia Comprehensive and enhanced partnership agreement was signed. It refers to political, civic, legal economic, energetic nature protection, educational cultural and other spheres regulations together with these fields reforms, their future enhancement and the necessity of development promotion.

As we mentioned earlier, as a result of constitutional improvements referendum, passed in Armenia, from upcoming April the governmental system will be replaced by that of parliament, and we hope that National Assembly adopts news legislation drafts on RA criminal and criminal-procedure which will ensure the international commitments meeting assigned by RA in criminal-legislative sphere, upon entering into force. It should be noted that RA Criminal Procedure Code was developed and sent to the National Assembly, while RA criminal new code draft is on the final stage of discussions after which it will be sent to the National Assembly too.

Except this the law draft on Mutual Legal assistance with criminal cases has already been developed about of which a number of meetings and discussions have been held. Regarding the stated law draft, in September of the current year a seminar entitled as "Support to development of the Law of Armenia on International Cooperation in Criminal Matters/Mutual Legal Assistance" with the participation of both various state bodies representatives and specialists invited from Europe, was held at the Ministry of Justice.

A training Mutual Legal Assistance Requests and Asset Forfeiture was held in corporation with USA Investigation Federal Bureau and Republic of Armenia investigative committee in September of this year. Practical issues regarding proceedings and other activities operative performance aimed at legal assistance ensuring were also discussed, including narrowing down inquiries making time frames by the USA legal bodies.

In October of 2017, in the scopes of Cybercrime@EAP III project, Cybercrime Programme Office of the Council of Europe held meetings with the aim of discussing various issues regarding public-private cooperation as well as to get acquainted with the legislation present state, particularly legislative barriers which occur during cybercrime investigation, which do not provide an opportunity or make the crimes disclosure in high tech sphere quite difficult.

Also, in October of 2017 The President of RA signed <<Concept on Information security policy and protection of Information security>> document, which includes article about developing strategy of information security. Now working group is developing strategy of Information security, which include Cybersecurity concept. Fight against Cybercrime would be a part of Cybersecurity concept.

AUSTRALIA

In anticipation of the 4th 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 3 (Legislation and Frameworks) and Chapter 4 (Criminalisation) of the Draft Comprehensive Study on Cybercrime.

Australia recognises the real threat that cybercrime poses internationally and has enacted a comprehensive framework for the criminalisation of cybercrime. At the Commonwealth level, Australia's principal cybercrime offences are contained in the Criminal Code Act 1995 (Cth) and the Telecommunications (Interception and Access) Act 1979 (Cth). Australia's legislative framework covers both criminal activities directed at computers and information communications technologies, as well as crimes where computers facilitate an existing offence, such as online fraud or online child sex offences.

These offence provisions are supported by a range of powers, which can be exercised by law enforcement and national security agencies in the detection, disruption and investigation of these offences. Commonwealth laws and frameworks are also complemented by laws at the State and Territory level. Critically, Australian States and Territories have primary responsibility for laws dealing with online versions of personal and property crimes, such as stalking, theft and fraud.

As the Draft Comprehensive Study notes, technological developments associated with cybercrime requires legislation to grapple with new concepts not traditionally addressed by criminal laws. There is also the ongoing challenge of ensuring that legislative frameworks keep in step with the evolving nature of technology and criminal methodologies.

Australia ratified the Budapest Convention on 30 November 2012 and considers it to be the best practice model in framing domestic and international responses to cybercrime. Consistent with Convention, Australia has framed its cybercrime offences in technologically-neutral terms to ensure they remain responsive to rapidly evolving technologies and patterns of usage. Australia also keeps its cybercrime laws under review, to ensure its legal frameworks take account of key developments. For example, Australia has a Bill before Parliament that will criminalise the provision of an electronic service to facilitate dealings with child abuse material online, such as websites, chat fora, hosting services and peer to peer sharing platforms. Australia is also pursuing legislative reforms to enable Australian law enforcement and security agencies to adapt to the challenges posed by anonymising technologies.

The Draft Study recognises the transnational nature of cybercrime and highlights the importance of international cooperation and harmonisation of laws. In this context, Australia notes the usefulness of the Budapest Convention as a guide for developing comprehensive legal frameworks at the domestic level, and for facilitating international cooperation in the investigation and prosecution of cybercrime offences. In addition, Australia notes the value of United Nations Convention against Transnational Organised Crime and the Protocols thereto, which provide useful mechanisms for international legal cooperation to combat transnational crime, including cybercrime. These existing international instruments provide a strong basis for international cooperation to investigate and prosecute cybercrimes.

Australia strongly supports actions to improve and facilitate effective cross border access to information, noting the increasing reliance on electronic material in a broad range of criminal investigations. Australia is actively involved in the work of the Budapest Conference of the Parties (T-CY), including the development of an Additional Protocol to the Convention. This work is focused on ensuring the Convention remains responsive to technological developments and operational challenges, and identifying opportunities for enhanced collaboration and improved international legal cooperation processes.

Australia firmly believes that the international community should prioritise the provision of capacity and technical assistance, especially for developing countries, to assist countries strengthen legal frameworks to combat cybercrime. Australia continues to support capacity building, including through the provision of technical assistance, both through key regional bodies and bilaterally. A priority for Australia is working with countries in the Pacific to strengthen their criminal justice frameworks to support both domestic and international cybercrime efforts.

CANADA

Canada is pleased to submit this reply to the United Nations Office on Drugs and Crime note verbale CU 2018/47/(A)/DTA/OCB/CSS and to provide information on its national efforts related to the substantive issues included in Chapter 3 (Legislation and Frameworks) and Chapter 4 (Criminalization) of the Draft Comprehensive Study on Cybercrime (Draft Study) produced by the United Nations Office on Drugs and Crime in preparation for the fourth meeting of the Intergovernmental Expert Group on cybercrime (IEG).

One of the objectives of Canada's efforts over the past fifteen years in the area of cybercrime has been to undertake a legislative review of its criminal legislation to ensure that it could address the realities of today's technologically advanced environment. A number of flaws have been identified through this review and, as a result, it was determined that there was a significant need to update some of those provisions in order for federal legislation to adequately deal with crimes committed with the assistance of a computer, whether that crime was committed with a computer as a tool, a target or a storage device. While most of the substantive provisions were drafted in a technology neutral manner, in considering Criminal Code provisions relating to child pornography, hate propaganda and obscenity, some areas were identified that reflected a 'paper' world and required updating in order to better address new forms of criminal offences that can occur using the Internet. However, the Criminal Code provisions pertaining to mischief to data, unauthorized use of a computer or possession of a device to obtain unauthorized use of a computer system or to commit mischief, which were introduced in 1985, have withstood the test of time and considered to apply to new developments in offending such as botnets. Canada will be pleased to talk about its experience in this regard at the meeting.

The main challenge pertaining to legislation 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. Although there were investigative powers in existing laws that could be used to fight many crimes, they were no longer the right tools to regularly perform complex investigations in the current environment, as some were out of date with technology. With the coming into force of the Protecting Canadians from Online Crime Act on March 10, 2015, law enforcement agencies were provided with new, specialized investigative powers to help them take action in criminal investigations involving electronic evidence, such as investigations relating to Internet child sexual exploitation, and on-line organized crime activity. These investigative powers 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. Except for data preservation powers to assist with the volatile nature of electronic evidence, such powers are not qualitatively new but rather update existing powers to respond to new technologies.

These amendments also allowed Canada to ratify the Budapest Convention on Cybercrime, an international solution in the fight against cybercrime which provides a range of international cooperation tools to deal effectively with the global nature of the Internet and criminal use of this medium. As communications can easily be – and frequently are – routed through many countries between their source and destination, communications must often be traced back through many countries, one after another, quickly enough so that electronic data, which could be information that is essential to an investigation, is not automatically erased before the tracing can be completed. Ratification of the Convention was considered as being a positive step towards this solution.

One interesting issue that may warrant some discussion at the upcoming meeting of the IEG is how Member States reach the delicate "balancing act" that is referred to in chapter 4 of the Draft Study when they develop legislation to address the challenges brought forward by new technologies. While law enforcement agencies require the proper investigative tools to combat crime in the 21st century, popular opposition to cybercrime legislation on the basis of privacy and human rights advocates who are concerned that law enforcement agencies are gaining increased powers can be challenging to address.

Canadian legislative initiatives in this area have been subjected to an important level of scrutiny by the media and privacy commissioners, and some proposals have been met with severe criticism, reflecting how difficult it can be to ensure law enforcement agencies' ability to lawfully access information and to investigate cybercrime, while protecting human rights and helping to increase the confidence of Canadians in electronic commerce. Along with the primary objective of the Protecting Canadians from Online Crime Act to ensure that the criminal justice system was able to keep pace with this new environment, as well as the changing nature of how criminals operate, the Canadian Government was attentive to the privacy-intrusive character of certain investigative techniques. While a police investigative tool, such as a search warrant or a production order, naturally impact upon a person's privacy, the Government explained that all amendments included in the Act were carefully crafted to balance the pressing need to provide police with effective investigative tools in the current environment with the constitutional imperative to protect the right of Canadians to be free from unreasonable search and seizure. The Government called this concept "privacy with precision". Throughout the legislative passage of the legislation, a number of examples were provided on how each investigative power had been carefully designed to strike the appropriate balance between providing for the safety and security of all Canadians, and ensuring that rights and liberties were respected. The Government of Canada is strongly committed to maintaining the rule of law through all of its legislation. It will continue to ensure that such authority will be exercised bearing in mind privacy interests and human rights protected in Canadian laws such as the Canadian Charter of Rights and Freedoms, the Privacy Act, and the Personal Information Protection and Electronic Documents Act.

CHINA

1. China has always been supporting the discussion process for promoting international cooperation in countering cybercrime under the framework of the United Nations. We welcome the UN Open-ended Inter-governmental Experts Group on cybercrime (IEG) to start its substantial discussion on international cooperation in countering cybercrime. With the joint effort of all parties, the IEG was granted with new mandate in 26th United Nations Commission on Crime Prevention and Criminal Justice (CCPCJ), and its Extended Bureau has successfully adopted Chair's Proposal of 2018-2021 Workplan of the IEG recently, thus sending a strong response to the international community's expectation on enhancing the United Nations' efforts in tackling cybercrime. China supports the adoption of the Chair's proposal of 2018-2021 Workplan by this Meeting, and would like to work together with all parties to fully implement the Workplan, with the aim to make the IEG an important platform for providing policy guidance,exchanging experience and sharing information for international cooperation on countering cybercrime for all parties.

I. Trends of Cybercrime and Overview of China's Policy and Legislation

2. With the advancement of informatization, cost for conducting cybercrime reduced greatly, patterns of its manifestation proliferated, scale of and damage caused by cybercrime dramatically increased. In addition, cybercrime in China represents a trend of complex combination of traditional crimes and the internet, and become more organized, industrialized, trans-national and trans-regional. According to statistics, in 2017, China's public security authorities have filed 537,000 cases in the single field of telecommunication and internet frauds, cracked 78,000 cases, punished 47,000 illegals and criminals, confiscated of illicit money and items of 1.36 billion RMB value .

3. In response to the growing threat of cybercrime, China has been continuously making efforts in improving overall cybersecurity policy and legal frameworks. It has made the combating of criminal and terrorist use of cyberspace an important strategic task in safeguarding national cybersecurity, and has established necessary policy and legal frameworks for promoting international cooperation. In recent years, China has published National Strategy for Cyberspace Security and International Strategy of Cooperation on Cyberspace, and promulgated some landmark laws such as National Security Law，

Anti-Terrorism Law and Cybersecurity Law. China also has actively engaged in improving cyber criminal legislation. Through amendments to the Criminal Law in 1997, 2009, and 2015, three categories of cybercrime has been established, i.e. the destruction of computer information systems and data security, the use of computer networks to commit crimes, and crimes related to computer content. In addition, the Supreme People's Court, Supreme People's Procuratorate and Ministry of Public Security have jointly issued relevant legal guidance on cybercrime, such as the Opinions of Several Issues on criminal procedure applying to the handling of cybercrime cases, and Provisions on Several Issues Concerning the Collection, Examination and Judgment of Electronic Data in Handling Criminal Cases. Those documents clarify procedural questions of law enforcement agencies and judicial authorities about applicable criminal procedures and electronic evidence issues when handling cybercrime cases. In addition, extra documents has been issued to clarify legal criteria on conviction and sentencing on certain cybercrime, such as Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Certain Issues Concerning Applicable Laws in Handling Criminal Cases Involving the Activities Endangering Computer Information System Security, Opinions of the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security on Certain Issues Related to the Application of Law in Trying Cases Involving Online Gambling Crimes, etc.

II. Progress since 2017

4. Legislation. In May 2017, the Supreme People's Court and the Supreme People's Procuratorate jointly issued Interpretation on Several Issues Concerning Applicable Laws in handling Criminal Cases of Infringing Citizens' Personal Information, which provides detailed guidance on application of crime of infringing personal information provided in Criminal Law. In December 2017, China Information Security Standardization Technical Committee published the national standard of "Information Security Technology: Personal Information Security Specification" (GB/T 35273-2017), which sets standards for conduct of enterprises on personal information. Based on the above,the Chinese legislative has been actively doing research on formulation of personal information protection legislation. Furthermore, the in drafting International Judicial Assistance Law on Criminal matters will provide detailed rules for international judicial cooperation against cybercrime.

5. Criminalization. In October 2017, given the fast development and extensive application of cloud computing, the Supreme People's Court and the Supreme People's Procuratorate jointly published the Reply to the Issues of Conviction and Sentencing of the Activities of Using Online Cloud Disks to Produce, Reproduce,and Sell and Disseminate Obscene Electronic Information for Profit-making , which provides guidance on legal criteria for Conviction and sentencing to relevant crime activities. In June 2017, the Supreme People's Procuratorate published minutes of Symposium on Issues Related to Handling Internet Financial Crime Cases, which elaborates basic requirements for handling Internet financial crime cases.

6. Practices. From February 2018, Ministry of Public Security launched a special operation "Online Cleanup 2018", which focuses on cracking down criminal activities of infringing citizens' personal information, hacking attacks, and eliminating illegal criminal chains and sources. From July to December 2017, the National Copyright Administration and other relevant authorities launched an online campaign "Sword Internet 2017" on combating infringement activities against film, TV and broadcast products,and protect copyright on e-commerce platform and APP platform. In August 2017, relevant State Council agencies launched an one-month nationwide awareness-raising activity on countering new types of telecommunication and internet crimes, in order to enhancing public awareness in fighting fraud crimes. On promoting international cooperation, the Ministry of Foreign Affairs held the first International Forum against Cybercrime during the Fourth World Internet Conference in December 2017, Secretary-General of Asian-African Legal Consultative Organization (AALCO), Chairman of the IEG, and other more than 80 participants from the UN systems, Russia, Brazil, South Africa, etc., attended the forum. All parties agreed that the role of the UN on cybercrime should be

further strengthened, and international cooperation against cybercrime should be further enhanced by joint efforts through multi-channels.

III. Suggestions

7. As the only platform dedicated to promoting international cooperation against cybercrime in the UN framework, the IEG should commit itself to implementing relevant resolutions of the General Assembly and the CCPCJ, and fufilling its mandates given by the 2010 Salvador Declaration and the 2015 Doha Declaration. The IEG shall assist its Member States in deepening exchange of experience, building consensus and exploring an internationally applicable legal framework for international cooperation in the spirit of mutual trust, pragmatism and solidarity. Member States should firmly support the work of IEG, actively participate in discussions and submit relevant written comments and information. The Secretariat should also give its full support to the work of the IEG.

8. Based on the previous three meetings and also the Draft Comprehensive study on Cybercrime, the IEG may focus its work on the study of new developments of internet technologies such as cloud computing, Internet of Things, big data, cryptocurrency and dark network,as well as their implication to the criminal justice response to cybercrime, including organizing in-depth discussions on challenges and opportunities brought by those developments, such as legislation and legal framework, criminalization and international cooperation, in order to facilitate reaching international consensus in this regard.

9. With the assistance of the Secretariat, the IEG shall summarize suggestions and best practices shared by countries on legislation and legal frameworks, criminalization, and international cooperation and put them as a part of outcome of each meeting. They could serve as useful information or reference for relevant work of every country. It may also be necessary for the IEG to reach some consensus on some core types of cybercrime that are of universal concern, and explore new approaches of strengthening international cooperation in this regard.

FRANCE

En réponse à la note verbale CU 2018/47/(A)/DTA/OCB/CSS et à l'invitation du secrétariat de l'ONUDC de soumettre des commentaires jusqu'au 14 mars 2018, la France souhaite communiquer les éléments suivants.

La quatrième réunion du groupe intergouvernemental, à composition non limitée, chargé de réaliser une étude approfondie sur le problème de la cybercriminalité abordera les questions de législation, de cadre et de criminalisation de la cybercriminalité, conformément au plan de travail proposé par la présidence pour la période 2018-2021.

La France dispose depuis 2011 d'une stratégie nationale de défense et de sécurité des systèmes d'information. L'Agence Nationale de Sécurité des Systèmes d'information (ANSSI) rattachée au Premier Ministre, est l'autorité nationale en matière de sécurité et de défense des systèmes d'information. Elle assure la protection des systèmes informatiques de l'Etat et des opérateurs d'importance vitale.

Le dispositif législatif français a été étoffé par la loi du 13 novembre 2014 qui prévoit notamment la possibilité, pour l'autorité administrative, de demander le blocage des sites Internet provoquant ou faisant l'apologie du terrorisme ainsi que le « déréférencement » à partir d'un moteur de recherche ou annuaire.

Enfin, le décret n° 2017-58 du 23 janvier 2017 institue, auprès du ministre de l'Intérieur, un délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces. Il a succédé au cyber préfet et est chargé de coordonner l'action du ministère en matière de lutte contre les cyberattaques et d'un département chargé de la lutte contre la cybercriminalité. Il dispose en outre de plusieurs structures opérationnelles.

Afin de mieux appréhender la cybercriminalité, il paraît essentiel de mobiliser tous les acteurs concernés. Ainsi, le citoyen peut être un acteur important de la détection. C'est la raison pour laquelle la France a mis en place une plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS). L'internaute confronté à des contenus ou des comportements illicites sur Internet a la possibilité d'envoyer un signalement sur le portail du ministère de l'Intérieur français (www.internet-signalement.gouv.fr). La plateforme Pharos a enregistré 153 000 signalements pour contenus illicites en 2017.
La France a par ailleurs ratifié la Convention de Budapest du Conseil de l'Europe depuis 2006. C'est un outil précieux qui permet une coopération internationale efficace.

La Convention de Budapest offre une base juridique pour lutter contre la cybercriminalité, pour établir les différentes infractions dans les législations nationales, pour coopérer entre Etats pour les investigations. Elle permet notamment de faire geler les données numériques en urgence et de faciliter la conservation des preuves numériques grâce à un réseau international de points de contact fonctionnant 24/7. Ainsi, grâce à ce réseau de points de contacts, La France a reçu 115 demandes de gel et en a émises 101 pendant l'année 2017. Enfin, elle permet de mettre en place l'entraide judiciaire internationale.

La France participe également au groupe de travail chargé de rédiger un protocole additionnel à la Convention de Budapest. Ce protocole additionnel permettra d'améliorer la coopération opérationnelle, d'accélérer le partage d'information et d'améliorer le cadre du régime traditionnel d'entraide judiciaire.

JAPAN

The criminal law in Japan was revised in 2011 and a crime of electromagnetic records by illegal command, a so-called computer virus creation crime, was newly established along with the accession of the Budapest Convention. As a result, it became possible to arrest the suspect at the stage of creating, offering, serving, acquiring, and storing computer virus before the damage such as nauthorized access, fraud, or destruction of property was caused.

Here is a recent example of cases of arrest by this crime. The suspects uploaded a remote control computer virus pretending to be a cheat tool in a free online storage service and infected computers of the people who downloaded the virus. Nine suspects who infected the computers with the virus were arrested for this crime in 2016.

Japan utilizes the Budapest Convention's mutual legal assistance effectively in order to respond to new types of cybercrime quickly and efficiently. For instance, in the case of obstruction of business by DDoS (Distributed Denial of Service) attack in 2016, the National Police Agency made a request for mutual legal assistance, and necessary information was provided by other states parties accordingly. Also, Japan would like to share some experience on prosecuting new and emerging forms of cybercrime involving crypto-currencies and copyright infringement by rigorously applying already existing laws. There are two cases in relation to crypto-currency related cybercrime. The first is an internationally high profile case concerning the creation and use of false electromagnetic records and embezzlement of vast amounts of money by the CEO of a Bitcoin exchange company called Mt. Gox.

In this case, the CEO of Mt. Gox, with intent to distort the operations of the company, accessed the company's Bitcoin exchange system set up in a computer system server in the United States. The CEO then illegally uploaded electromagnetic records which contained false information that a total of five

million US dollars was remitted into his account. Later, the CEO illegally 2 transferred a total of approximately 340 million yen from the company's bank accounts to pay for his personal and business related expenses. The CEO was prosecuted for the offences of unauthorized creation and use of electromagnetic records and embezzlement. The second case relates to another Bitcoin exchange company. In this case, the offenders created a sham account by uploading false ID information and data of falsified ID cards onto the server computer of a Bitcoin exchange company. The offenders then unlawfully purchased Bitcoin by uploading illegally obtained credit card details as method of payment. The offenders were prosecuted for several offences including the unauthorized creation and use of electromagnetic records and computer fraud. Japan has also prosecuted members of a criminal group who operated a publicly accessible internet website that illegally uploaded copyright materials. In this case, there were additional accomplices who, in conspiracy with the criminal groups, operated an internet website that provided a link to the illegal website. These two cases are examples of how Japan has been able to apply already existing laws to combat new and emerging form of cybercrime involving crypto-currencies and copyright infringement.

NETHERLANDS

General remarks

The substantive parts of the 2013 draft Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector may serve very well as the point of departure for the 2018 – 2021 discussions on various themes, starting with "legislation and frameworks" and "criminalization". Of course it must be kept in mind that the 2013 draft study presents a snapshot of the situation described by governments, and by civil society, businesses and academia reflecting on the year 2012 and earlier.

The nowadays "problem of cybercrime" is to be described taking into account major changes since 2012 in ICT's and cyberspace. Changes such as human behavior in cyberspace, the evolvement of criminality constituted by and/or enabled by and/or recorded, as well as in the technological developments over the last years. Cyberspace has become more and more borderless. Information flows freely between countries providing citizens and organizations almost unlimited access to information and digital services. Information is everywhere; the physical location of the servers on which it is stored is often not known and deemed irrelevant to users. Information can be stored, changed and deleted, and internet services can be used from anywhere in the world. Cyberspace has grown into an essential element of modern life. People often simultaneously use various ICT devices – predominantly smartphones, as well as tablets and laptops – to communicate and access data stored in clouds or via so called "always on" applications like Whatsapp. Many of these applications use by default encryption tools. Other techniques make it easy to "go dark" and be anonymous on the internet. Many people nowadays shop online, connecting businesses and people as never before, but we have also witnessed a huge rise of so-called illegal marketplaces used to trade and transfer illegal goods and services.

Even more than in 2012, governments are in need of – and do adopt – more comprehensive policies to address cybercrime and to enhance cyber security. Next to improving legal frameworks on criminalization, enhancing procedural powers for law enforcement and strengthening international cooperation, effective policies now also target prevention, victim support and recidivism. For an overview of the Netherlands recent policies on cyber security and cybercrime: https://www.ncsc.nl/english/current-topics/national-cyber-securitystrategy.html. Reference is also made to recurrent threat assessments on cyber security (https://www.ncsc.nl/english/currenttopics/Cyber+Security+Assessment+Netherlands). The coalition agreement of the new government of the Netherlands mentions that a new cyber security agenda will be formulated.

Legislation and frameworks

The Netherlands

As did many States at the end of the 20th century, The Netherlands first penalized in the Dutch Criminal Code (DCC) actions in which computer resources were used against other computer resources and thereby threatening the confidentiality, integrity and availability of electronic data. It concerned acts like illegal access, system interference and DDOS-attacks.

Because of the inherent borderless nature of the internet The Netherlands soon realized that an effective approach to cybercrime needs international cooperation next to an adequate national criminal law. For this reason more international harmonization is a prerequisite. To this end the Netherlands actively joined the debate to come to a cybercrime convention. The Netherlands signed the Cybercrime Convention on 23 November 2001 and ratified it on 16 November 2006.

During the ratification process, triggered from debates and the concluded articles in the convention and because of national legal debates, the Netherlands have amended the DCC and the Dutch Criminal Code of Procedure (DCCP). Search and seizure of electronic data, production orders directed at internet service providers and preservation orders were regulated. Also a 24/7 point of contact was established. All the substantive criminal acts of the convention are enacted in Dutch law.

Having a national framework that was compatible to internationally agreed standards proved to be an important asset in the fight against cyber crimes and greatly facilitated cooperation with other States in order to address specific criminal acts that targeted The Netherlands, or were performed from or via the infrastructure of The Netherlands. Working in a commonly accepted framework also facilitates international technical assistance and capacity building projects, developed in the various projects of the Council of Europe and the European Union.

In the field of online sexual abuse of children the Netherlands DCC was even further amended with respect to grooming and the distant accessing of child sexual abuse images in line with the Lanzarote Convention and later the EU Directive on combating the sexual exploitation of children online and child pornography (2011/EU/92).

The Netherlands positively evaluates the possibilities for law enforcement on the basis of the national legal framework which is in line with the Cybercrime Convention and the 2012 EU Directive on Attacks Against Information Systems (2013/40/EU). However to keep pace with the recent developments as described above The Netherlands are in a process of amending the national law (both DCC and DCCP) and is supporting ongoing legislative amendment processes within the Council of Europe and the EU.

A “third Computer Crimes law” is currently in process in the Senate of the parliament of The Netherlands. The bill addresses shortcomings in current law enforcement powers to have access to electronic data for investigation purposes and to gather electronic evidence. For severe criminal acts, the bill will allow direct and online access to data where there is an overriding necessity and no other possibility to obtain the data. This investigative power is subject to strict procedural safeguards, like prior judicial authorization. Next to this procedural power, the bill will introduce specific criminalization of so-called electronic marketplace frauds and the “fencing” of illegally acquired data of third parties.

The Netherlands support the ongoing debate and drafting processes in the Council of Europe and in the EU on investigation in cyberspace and on e-evidence. Enhanced regulated options and modalities to swiftly access and acquire electronic evidence, possibly located in another and sometimes unknown territory are much needed to uphold the rule of law in cyberspace. In order to be able to start up investigations, subscriber data, including data related to accounts or devices accessed, are most needed

as they form the initial start of investigations and provide leads to further criminal investigations or proceedings. Next to this, however relatively less in quantity, access to traffic or metadata and content data may be needed, especially in further stages of an investigation or prosecution.

Relevant elements are:

- Practical improvements in the current MLA procedures;
- Elaborating on current voluntary direct contacts with service providers;
- Acceptance of new (to be developed) legislative measures to enhance cross-border access to electronic evidence beyond current national production orders, MLA regulations and voluntary cooperation with private industry: Legislating international production requests/orders in order to enable authorities in one state to request ("production request") or to compel ("production order") service providers, possibly seated in another state and offering their services in the investigating State, to respond voluntarily or mandatory and disclose data.
- Legislative solutions to facilitate direct access to data, like extending network searches or using legally acquired credentials.

The Council of Europe and the European Union

The Netherlands view the Cybercrime Convention as the key international instrument that has fundamentally affected legislation, practice and international cooperation on cyber crimes in a large number of states around the world. Since 2012 the significance of the Cybercrime Convention expanded further.

- At the moment 56 States have ratified or acceded to the Convention and 4 States have signed, though not ratified. A further 11 States are currently in the process of accession. This sums up to a total of 71 States. From the experiences in the technical assistance and capacity buildings programs there is testimony to the fact that over 20 other States have (draft) laws largely in line with the Convention. Beyond this, many more States draw on the Cybercrime Convention for legislation.
- Among the State Parties, the currently acceding states and the States that have been inspired by the Convention many are not from the European region. Participating States come from all regions in the world.
- The quality of the implementation of the Convention is safeguarded by thematic studies and assessments on the implementation of the Cybercrime Convention, such as the assessment of the functioning of mutual legal assistance , on the functioning of 24/7 points of contact and on the preservation provisions in the Convention.
- The Netherlands, and other State Parties, have been able to elaborate and improve their implementation of the Convention by making use of Guidance Notes accepted by the State Parties. They cover various cyber crime activities (e.g. Botnets) and various investigatory powers (e.g. production orders on ISP's offering their services on the territory of State Parties). Thus, the convention and its implementation are kept up to date. This is further driven by the ongoing process of drafting a second additional protocol to the Convention, mainly for the much needed quick and effective access to electronic data which are very often stored anywhere abroad.

The Netherlands also would like to draw attention to efforts by the European Union to strengthen the international legislative framework. The above mentioned directives on attacks against information systems and on combating the sexual exploitation of children online and child pornography subscribe to the Cybercrime Convention as the base level, regulating for EU countries on some specific areas a higher level of regulated conditions to effectively address cyber crimes and child sexual exploitation online. Recently, the EU Commission has proposed a new Directive aimed at updating current EU framework decisions, removing obstacles to operational cooperation and enhancing prevention and

victims' assistance, to make law enforcement action against fraud and counterfeiting of non-cash means of payment more effective.

Expected is an EU Commission legislative proposal to the Council of EU Minsters of Justice and Home Affairs. This proposal will be the result of an exhaustive expert process as a follow up to the June 2016 EU JHA Council's conclusion on criminal law in cyberspace. The Council acknowledged the need - as a matter of priority - to find ways to secure and obtain e-evidence more quickly and effectively. The ministers asked the EU commission to come forward with possible practical and legislative measures to address the obstacles faced in criminal investigations in relation to access to e-evidence that is often stored outside the investigating country or handled by a foreign service provider.

Criminalization

The Netherlands subscribes to the view that there is much common understanding on the criminalization of the 14 cybercrime acts contained in the draft comprehensive study. It must be noted that the draft comprehensive study also reports on offences that are not widely criminalized. However, referring to the remarks above, within the Cybercrime Convention, it's Guidance notes and the UN, Council of Europe and EU regulations on child sexual exploitation, the negative picture in 2012 has changed regarding spam, computer misuse tools, racism, xenophobia and online harassment, and the grooming of children.

The Netherlands agrees there is a certain baseline consensus on culpable cybercrime conduct.

Little common agreement is seen on crimes connected to issuing opinions, images and videos, and posting these on the internet. The Cybercrime Convention is limiting content-offences to child pornography, while xenophobia and racism are covered in a separate Protocol since not all States are prepared to sign up to this. It would be useful to learn more about the meaning and level of acceptance of concepts and provisions such as "violation of public morals" or "undermining the state", "obscenity" or safeguards to ensure the protection of human rights and rule of law which can be found in various other instruments, some of them mentioned in the draft comprehensive study.

The Netherlands recall the importance of human rights law, in particular the freedom of expression and the right to privacy. The same fundamental rights that people have offline must also be protected online, including the right to privacy. Interferences with these fundamental rights, enshrined in several UN and other instruments, have to meet all conditions laid down in the relevant provisions, which entails inter alia demonstrating that the measures serve a legitimate aim, are proportionate, appropriate and necessary.

As stated earlier criminalization is also found in other international instruments, such as the UN Convention on Transnational Organised Crime (UNTOC). The relevant legislative framework for law enforcement in cyberspace is also strengthened by the UN Convention on the Rights of the Child, and especially by the second Protocol to that Convention. The Council of Europe elaborated on this in the so-called Lanzarote Treaty (Ets. 201).

NORWAY

Legislation & frameworks; Criminalization

Norway ratified the Council of Europe Convention on cybercrime (CETS No. 185, the Budapest Convention) in 2006. As a part of the ratification process, Norway amended some provisions in the

General Civil Penal Code and in the Criminal Procedure Act, to comply with the Convention[2]. Regarding criminalisation, some provisions in the Penal Code may apply both to cybercrime and to other types of crime (for example Section 351, Vandalism), while other provisions are specifically addressing crimes against computer systems and information (Section 201 to 205 in the Penal Code[3]).

Some smaller changes in the Penal Code and in the Criminal Procedure Act have been made since then.

In 2017, the Norwegian Parliament approved an amendment of Section 199a in the Criminal Procedure Act to clarify search and seizure of computer systems protected by biometric authentication systems, such as fingerprint readers. Below is an unofficial translation of the current provision, with the new parts underlined:

When conducting a search of a data-processing system, the police may order everyone who is dealing with the said system to provide the information necessary for gaining access to the system or to open it by use of biometric authentication.

If someone refuses to comply with an order of biometric authentication as mentioned in the first subsection, the police may perform the authentication by use of force.

Decision regarding use of force in accordance with the second subsection, is done by the prosecuting authority. In case of urgency, the decision may be done by a police officer at the scene. The decision shall promptly be reported to the prosecuting authority.

This article also applies to search of computer systems seized after Chapter 16.

The Norwegian Parliament's Justice Committee will March 6 present a Bill to amend the current provisions regarding distribution of private images without consent (including so called "revenge porn"). Some of the members in the Committee will propose a new provision in the Penal Code, while others will prose that the Ministry of Justice conducts a review of this legal issue.[4]

In November 2016, the Norwegian Supreme Court convicted a man for illegal distribution of private photos, via BitTorrent networks. From the summary of the case:

The punishment for violation of Section 317, subsection 1 and section 162, subsection 1 of the Penal Code (1902) was set at a term of imprisonment of five months. The offence concerned downloading and file sharing using so-called torrent technology of a large number of files containing private images of young women, mainly nude images, without the women's consent. The images were obtained from social media, where most of them were originally posted by the women themselves in the belief that they could not or would not be distributed further. The images were sorted using a file-sharing tool so that many of the women could be easily identified. Emphasis was placed on considerations of general deterrence. The punishment for receiving stolen property was set at a term of imprisonment of 120 days.

Distribution of private photos (including so called "revenge porn") is a violation of the current Norwegian Penal Code, but the upcoming proposals from the Parliamentary Justice Committee, indicates a political interest in this area, as well as an interest in possibly increasing penalties and widen the scope of the current provisions. Any changes in the Penal Code for this type of crime, such as increased penalties, may also open for use of new investigative measures for this type of crime, as several of the provisions in the Criminal Procedure Act requires a possibility of a certain maximum penalty.

[2] https://www.regjeringen.no/contentassets/4deac3823b2f48cc9d7b2d5a2d9091f3/no/pdfs/otp200420050040000dddpdfs.pdf
[3] Link to the English translation of the Norwegian Penal Code, https://lovdata.no/dokument/NLE/lov/2005-05-20-28/*#*
[4] https://www.nrk.no/norge/vil-ha-strengere-straffer-for-a-spre-nakenbilder-pa-nett-1.13929188

In 2012 the Norwegian Government presented the Cyber Security Strategy for Norway[5]

In 2017, the Norwegian Government launched an international cyber strategy[6]. Regarding cybercrime, the strategy document pointed out:

4.5 Safeguard society's ability to prevent, detect and investigate cyber crime
(…)

Selected areas of focus include:

- All stakeholders must take initiative to help prevent and mitigate losses or damage resulting from cybercrime and identity theft and abuse.
- The police must have sufficient expertise and capacity to detect, identify and deal with cybercrime.
- Police must be present on the Internet, both openly and covertly, in order to prevent, avert and, when necessary, investigate and try to bring this type of crime to justice.
- There must be clear procedures for collaboration and sharing knowledge both within the police, and between the police, government agencies and key security environments.

In 2015, the Ministry of Justice and Public Security presented a strategy document[7] regarding ICT crime. The strategy includes national and international cooperation, and having good and updated legal regulation and provisions. The stragegy documents includes and action plan with 15 points, including centralised statistical reporting regarding ICT crime, a research stragegy to prevent and fight cybercrime, increased national cooperation and strengthened international cooperation, and consider the need for changes in the Penal Code and other criminal laws.

In a report on ICT security to the Norwegian Parliament[8] of June 9, 2017, the Ministry of Justice and Public Security presented findings and proposals to improve the general ICT security in Norway.

RUSSIAN FEDERATION

Информационно-справочные материалы относительно международно-правовой базы сотрудничества в сфере информационной безопасности, а также национального законодательства, регламентирующего вопросы борьбы с преступлениями в сфере компьютерной информации

l. В настоящее время конвенции универсального характера, основным предметом регулирования которых являлась бы международная информационная безопасность, отсутствуют.
На региональном и двустороннем уровнях подписаны и действуют следующие международные договоры:
Конвенция о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года;
Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20 ноября 2013 года;
Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 года;

[5] https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/cyber_security_strategy_norway.pdf
[6] https://www.regjeringen.no/en/aktuelt/cyberstrategy/id2573036/
[7] https://www.regjeringen.no/contentassets/8de0db6aff3e4dd79c92519057af690f/strategi_ikt-kriminalitet.pdf
[8] https://www.regjeringen.no/contentassets/39c6a2fe89974d0dae95cd5af0808052/no/pdfs/stm201620170038000dddpdfs.pdf

Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от
8 мая 2015 года;
Соглашение между Правительством Российской Федерации и Правительством Республики Куба о сотрудничестве в области обеспечения международной информационной безопасности от 11 июля 2014 года;
Соглашение между Правительством Российской Федерации и правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности от 25 декабря 2013 года.
МВД России завершена работа по подготовке к подписанию Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий, направленного на создание современных правовых механизмов практического взаимодействия правоохранительных органов государств-участников СНГ в борьбе с преступлениями в указанной сфере. Разработка данного международного договора проводилась во исполнение пункта 1.1.1.2 Межгосударственной программы совместных мер борьбы с преступностью на 2014-2018 годы.
Проект Соглашения одобрен распоряжением Президента Российской Федерации от 26 августа 2017 года № 297-рп. Подписание Соглашения планируется осуществить в 2018 году в ходе очередного заседания Совета глав государств СНГ.
Вопросы противодействия преступлениям в сфере информационных технологий входят в число направлений взаимодействия, предусмотренных двусторонними межправительственными договорами в области борьбы с преступностью, а также соглашениями о сотрудничестве между Министерством внутренних дел Российской Федерации и компетентным органом иностранного государства.

2. Приоритеты Российской Федерации в информационной сфере сформулированы в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 (далее - Доктрина).
Согласно пункту 29 Доктрины к основным направлениям обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства, в том числе относятся: защита суверенитета Российской Федерации в информационном пространстве; участие в формировании системы международной информационной безопасности и создание международно-правовых механизмов, учитывающих специфику информационных технологий, в целях предотвращения и урегулирования межгосударственных конфликтов в информационном пространстве.
Уголовная ответственность за преступления в сфере компьютерной закреплена главой 28 (Преступления в сфере компьютерной информации) Уголовного кодекса Российской Федерации (далее – УК), содержащей статьи 272 (Неправомерный доступ к компьютерной информации), 273 (Создание, использование и распространение вредоносных компьютерных программ),
274 (Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей) и 2741 (Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации) УК.
Также в УК установлена ответственность за мошенничество с использованием платежных карт (статья 1593), мошенничество в сфере компьютерной информации (статья 1596), неправомерный оборот средств платежей (статья 187).
Предварительное расследование уголовных дел о преступлениях, предусмотренных частями первыми статьей 1593 и 1596 УК, отнесено к компетенции дознавателей органов внутренних дел Российской Федерации, а частями вторыми - четвертыми указанных статьей, а также статьи l87 УК – к полномочиям следователей органов внутренних дел Российской Федерации (пункт 1 части третьей статьи 150 и пункт 3 части второй статьи l51 Уголовно-процессуального кодекса Российской Федерации).

Для дополнения российских комментариев к заседанию IV Межправительственной группы экспертов по киберпреступности

На сегодняшний день результатом «регионализации» международно-правовых инструментов по борьбе с информационной преступностью стала фрагментация позиций на международном уровне, препятствующая выработке общего понимания ключевых аспектов противодействия незаконным действиям в информационной сфере.

Одновременно существующие механизмы двустороннего сотрудничества не являются панацеей от проблемы киберпреступности. Государства могут отказывать в представлении необходимой информации, ссылаясь на особенности национального законодательства в плане трансграничного обмена данными, либо необоснованно затягивать сроки ответа.

Очевидно, что при существующих региональных инструментов по борьбе с киберпреступностью и беспрецедентном росте преступлений, совершаемых с использованием информационно-коммуникационных технологий, давно назрела необходимость в разработке уголовно-правовой конвенции под эгидой ООН в данной сфере, которая учитывала бы современные реалии и принципы суверенного равенства и невмешательства во внутренние дела государств. В этой связи российскими экспертами подготовлен проект универсальной конвенции ООН о сотрудничестве в сфере противодействия информационной преступности, который мог бы лечь в основу международной дискуссии по этой теме.

SINGAPORE

Computer Misuse and Cybersecurity Act (CMCA) and 2017 Amendments

Singapore recognises that cyberspace presents a new challenge to law enforcement agencies. In Singapore, the Computer Misuse Act (CMA) provides the necessary provisions to protect computer materials against unauthorised access and modification. The Act also allows law enforcement agencies to deal with the threat of cyber-attacks on systems that may endanger Singapore’s national security, essential services, defence or foreign relations. In November 2012, a Bill was put forward in Parliament to amend Section 15A of the Computer Misuse Act to allow for effective and timely measures against cyber threats that may endanger national interests or national security. The key amendment will enable the Minister for Home Affairs to direct Singapore's national critical information infrastructure (CII) owners to take effective and timely measures against cyber threats. National Critical Information Infrastructure (CII) refers to the various essential information systems and assets, such as telecommunication networks, banking infrastructure, water, electricity, gas and public transportation systems. On 13 March 2013, the Act was enacted and renamed to Computer Misuse and Cybersecurity Act (CMCA).

In April 2017, changes to the CMCA were passed in Parliament to help strengthen our response to cybercrime. The CMCA Amendment Bill includes the following four key changes:

a) Criminalise the act of dealing in personal information obtained via an act in contravention of the CMCA;
b) Criminalise the act of dealing in items capable of being used to commit a CMCA offence;
c) Extraterritorial application of CMCA offences with “serious harm” to Singapore; and
d) Amalgamate charges for CMCA offences.

National Cybercrime Action Plan

On 20 July 2016, Mr K Shanmugam, Minister for Home Affairs and Minister for Law, announced the National Cybercrime Action Plan (NCAP) at the RSA Conference Asia-Pacific & Japan. The NCAP sets out the Government's strategies in combatting cybercrime. It details the Government's ongoing efforts, as well as future plans, to effectively deal with cybercrime. SPF will implement, in collaboration with local and external stakeholders (e.g. in the public and private sectors including International Organisations such as Interpol/Interpol Global Complex for Innovation), 5 strategic thrusts, to enhance capabilities and capacities to fight cybercrime and to support the NCAP:

a) Operationalise a SPF CyberCrime Command (CCC) with cybercrime integrated investigation, forensic and policy-planning capabilities;
b) Investing more in Prevention through Public Education;
c) Review of Legislation;
d) Strengthening Partnerships in R&D in e.g. Malware Analysis; and
e) Furthering International Cooperation through Joint Operations and Training.

SLOVAKIA

Act on cyber security and on the amendment of certain acts

On 30 January 2018, National Council of the Slovak Republic adopted Act on cyber security and on the amendment of certain acts. The Act was signed by the President of Slovak Republic on 22 February 2018.

The aim of the Act is to create a functional legislative framework that will allow effective implementation of key measures that are important for the security of the national cyberspace and at the same time transposes into the Slovak national law the priorities and requirements of the European Network and Information Security Directive (NIS Directive).

The main areas of the Act are:

- The organization and competence of public authorities in cyber security,
- National cyber security strategy,
- A unified cyber security information system,
- The status and responsibilities of operators of essential services and to digital service providers
- Organization and competence of Computer Security Incident Response Team (CSIRT) units,
- A system for ensuring cyber-security and minimum requirements for ensuring cyber security,
- Building security awareness;
- Control and audit.

The content of the law also includes other requirements of the NIS directive, such as compliance with notification obligations, reporting of cyber security incidents (including voluntary reporting), and through its provisions it supports research and education, including awareness raising in cybersecurity.

UNITED KINGDOM

The United Kingdom welcomes the opportunity to provide written comments, examples of best practice and recommendations related to the main topics of the meeting (legislation and frameworks, and criminalization), in accordance with the Chair's proposal for the work plan for the period 2018-2021.

The United Kingdom has long-established legislation and legal frameworks related to cyber crime and its criminalisation. The Computer Misuse Act (CMA) was established in 1990 to address the challenge

of intrusion and modification or impairment of computer systems for criminal purposes (typically referred to as cyber-dependent crime). This law serves as the principle domestic legislation in defining offences and sanctions and has stood up well to the rapidly evolving challenge of cyber crime, owing to its technology-neutral language and focus on the nature of the offence - unauthorised intrusion and impairment - rather than the technical means to commit the offence. The CMA is additionally supported by a range of other laws which address the online element of 'traditional' crimes - such as fraud, child sexual exploitation (CSE) and malicious communications. This provides the UK legal framework to tackle both the principle means of facilitating cyber criminality, in conjunction with appropriate other laws which recognise the different ways in which cyber crime manifests and the resulting harm faced by victims.

The CMA has been updated on several occasions since 1990, the most recent being in 2015. The changes ensured that the UK was compliant with EU Directive 2013/40/EU on Attacks against Information Systems, as well as bringing in a new offence of unauthorised acts causing serious damage which carries a maximum life sentence and making other clarifying changes.

The United Kingdom has also been a ratifying member of the Budapest Convention since 2011. For the UK and our key partners, the Convention offers a vital framework in which the UK can progress international cooperation on cyber crimes, by ensuring mutual recognition of offences amongst its members and providing the basis for international cooperation to tackle them. This is vitally important given the international and transborder nature of these types of crimes, meaning the international partnerships the Convention facilitates are often essential to successfully pursuing a law enforcement investigation and bringing offenders to justice. Practical measures set out by the Convention, such as the requirement for a 24/7 Point of Contact to enable the timely sharing of evidence and preservation requests, has proven highly effective in enabling UK law enforcement cooperation with international partners and has in turn produced real-world operational benefits in prosecuting cyber criminality. Using communication channels established through the Budapest Convention (and the G7), the UK's National Crime Agency dealt with 440 preservation requests during 2017. In some cases, this allowed investigators to identify crucial links with crimes being pursued by overseas partners, including a series of threats using email addresses being investigated by another Party, and a ransomware campaign – in turn, prompting the establishment of joint investigative teams and further evidence sharing.

The United Kingdom is supporting work under the Council of Europe to develop an additional protocol to the Budapest Convention in order to further deepen and enhance the operational cooperation this provides to its members. This includes provisions currently being considered to hasten the speed and effectiveness of information sharing and tackling some of the lengthy time periods associated to international criminal investigations under the traditional Mutual Legal Assistance (MLA) regimes.

The Budapest Convention has offered a vital foundation for international cooperation on cyber crime since 2001 and has developed a mature process though the Cybercrime Convention Committee (T-CY) to facilitate dialogue amongst members and consider improvements to the Convention, ensuring it remains relevant and responsive to evolutions in cyber crime. It is the UK's recommendation that we build further upon this framework by enhancing its provisions and deepening the cooperation it offers. The UK also reaffirms its commitment to encouraging new members to consider joining the Convention, and recognises its applicability as a gold standard for countries working to improve their efforts to tackle cyber crime.

UNITED STATES OF AMERICA

The Permanent Mission of the United States of America is pleased to respond to note verbale CU 2018/57/(A)/DTA/OCB/CSS regarding the organization of the fourth meeting of the Open-Ended Intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime (Expert Group), and to provide written comments on the main topics under consideration at this meeting. In this context, the United States submits the following comments regarding the substantive content contained in Chapter 3 (Legislation and Frameworks) and Chapter 4 (Criminalization) 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.

General Comments

There are specific and basic requirements for effective law enforcement anti-cybercrime efforts at the national and international levels. These requirements contribute to a national cybercrime strategy which must also involve participation by private industry and end users as stakeholders in the strategy. Focusing in particular on law enforcement needs, effective anti-cybercrime efforts include the following elements:

First, each country requires adequate legislation which criminalizes conduct and provides procedural legal authority that permits law enforcement to investigate alleged crimes consistent with due process guarantees, privacy interests, civil liberties and human rights. Gaps may exist in current criminal statutes which permit culpable conduct to escape prosecution. In addition, each country needs a modern legal evidence framework which permits the admission of electronic evidence in criminal investigations and prosecutions, including sharing electronic evidence with law enforcement partners internationally.

The Draft Study demonstrates broad interest by Member States in the foundations of effective and comprehensive anti-cybercrime efforts. Many countries already have in place appropriate legislation, harmonized with existing international instruments, which reflects a consensus view on the range of culpable criminal conduct through computer networks. Similarly, many countries have both police investigative and prosecutorial resources to address cybercrime.

Detailed Comments

Legislation and Frameworks

In 2013, less than half of responding countries believed that their substantive and procedural national laws were sufficient to address cybercrime. Of these countries, only half planned to address the shortcomings in national law. This suggests that many countries still do not appropriately prioritize cybercrime or may need assistance in raising the awareness of decision makers to cybercrime risks to economic development and national security. The Draft Study notes that, while differences in the scope of domestic legislation may exist, many regional instruments and national legislation share certain "core" provisions. These include: the criminalization of acts against the confidentiality, integrity, and availability of computer data or systems; procedural powers, including search, seizure, orders for computer data, real-time collection of computer data, and preservation of data; and general obligations to cooperate in the investigation of cybercrime criminal matters.

The Draft Study note that countries vary widely in their views of the adequacy of their domestic legislation. There appears to be a broadly shared view among Member States in Africa and the Americas that their domestic legislation is inadequate to address cybercrime. However, for countries with adequate legislation, the majority of respondents appear to agree on which types of conduct should be criminalized, either by a specific cybercrime statute or a general statute. Similarly, countries which have passed appropriate laws also agree on the essential procedural authorizations for law enforcement

investigations. Consensus on these questions reflects the finite examples of culpable conduct that constitute cybercrime and the commonly accepted techniques and procedural tools used to combat cybercrime.

According to the Study, there are 19 multilateral instruments relevant to cybercrime which show a base level of common core provisions of 14 categories of cybercrime. In addition, a "significant amount of cross-fertilization" exists among all instruments, which reflects for most regional instruments a common source in the Budapest Convention. Furthermore, no region of the globe is excluded from the reach of at least one regional instrument. Accordingly, countries have numerous examples of substantive law in both multilateral instruments and the national laws of their regional partners which illustrate the types of behavior that should be criminalized in national legislation on cybercrime. Importantly, the Draft Study notes that membership in a multilateral cybercrime instrument results in increased sufficiency of national criminal law, and that current multilateral provisions are considered effective by the countries that have joined an existing instrument.

The Draft Study also notes that one country in western Africa cited the "development of cybercrime groups that are more and more organized and possessing a transnational dimension." This finding comports with the experience of the United States. The Draft Study further notes that cybercrime has transformed from a low volume crime to a common high volume crime that is "organized and industrial-like." As highlighted in the Draft Study, the great majority of cybercrime is committed by organized groups, and the UN Convention against Transnational Organized Crime (UNTOC) can facilitate information and evidence sharing for cybercrime investigation in these cases. Based on requests that the United States has received to date, an increasing number of countries recognize the applicability of the UNTOC to cybercrime and/or criminal matters involving electronic evidence. To this end, it seems clear that States which are interested in combating cybercrime should consider ways to join or apply existing instruments like the Budapest Convention and UNTOC, and to ensure that national authorities are aware of their ability to engage in international cooperation and to investigate and prosecute cybercrime using these instruments.

Criminalization

Countries generally agree on core conduct that should be criminalized by specific cybercrime statutes. Other culpable conduct such as child pornography, identity offenses, and racism and xenophobia (where such claims are cognizable) are covered by general statutes because usually there is nothing peculiar or unique to cybercrime in this conduct. Similarly, countries generally agree on the general procedural tools for investigating cybercrime, including search and seizure, preservation orders, and real-time interception of traffic data or content.

Updated cyber-specific statutes are likely required because criminal laws are construed strictly, and traditional laws which cover familiar concepts like theft are probably insufficient to apply to cybercrime. Similarly, new harms such as damage to computers or data will require new statutes because traditional criminal statutes generally do not cover these concepts which are unique to the information age. The Study also raises the interesting possibility that some minor infringements could be addressed by civil or administrative regulations.

Countries continue to have different approaches to other tangential but substantive offenses, such as computer misuse tools, racist and xenophobic expression, and solicitation of children. Importantly, these divergences derive from underlying legal and constitutional differences, including differing conceptions of rights and privacy, and not from differing conceptions of typical, substantive cybercrimes. For example, some responding countries reported limitations to free expression. Other "socio-cultural" elements of some limitations are reflected in national law, and in regional instruments

to which the country may be a party. However, these differences generally do not prevent cooperation internationally.

In this context, exact "harmonization," replicating the exact law in every country, is not necessary. International cooperation on criminal matters does not depend on a precise match among the diverse criminal laws among countries. In fact, international cooperation against many forms of crime would be impossible if this were the actual standard. Instead, cooperation is premised on the adoption of criminal laws which, though tailored to fit within national legal frameworks, nonetheless sanction the same or similar underlying illicit activity. Satisfying this dual criminality requirement becomes insurmountable if countries must name offenses identically and include identical elements. As a result, treaties omit exact harmonization requirements, and instead focus on acts. The Draft Study itself notes that "[a] key factor in establishing dual criminality is the substantive underlying conduct, and not the technical terms or definitions of the crime in national laws." This approach leaves countries free to implement their obligations in differing ways consistent with their legal systems.

Countries vary more broadly with respect to investigative measures authorized by domestic law. While there is no practical difference between "cyber-specific" and general investigative powers, the Draft Study notes that countries with specific cybercrime legislation will also have sufficient laws authorizing investigative powers such as production orders to providers, search and seizure of data, and preservation schema.

A majority of countries admit electronic evidence, with standard evidentiary safeguards, in criminal prosecutions. However, a substantial number of countries (a little more than 20 percent) do not allow electronic evidence in criminal prosecutions – an impossibility when investigating cybercrime. This is most likely due to insufficient legislation or a court system approach to handling electronic evidence that requires updating. Moreover, over 80 percent of countries (and in some regions like Africa and the Americas, 100 percent) distinguish between domestic evidence and evidence obtained from foreign partners when considering its admissibility in a criminal trial. The ready admissibility of evidence received from foreign partners is a key element in international cooperation. Countries should revise domestic law, in accordance with local evidence codes, to permit the admissibility of foreign-obtained evidence. Harking back to earlier responses, 100 percent of African respondents report that they have insufficient resources to handle and analyze electronic evidence. As a result, it is also unlikely that these countries can be effective international partners when responding to foreign requests without receiving capacity building assistance. For this reason, technical assistance for law enforcement and criminal justice authorities is an urgent concern that should be addressed as a matter of priority.

Furthermore, the Draft Study notes that existing "gaps" in procedural investigative powers, in particular a lack of any domestic scheme to preserve electronic data expeditiously, remains a challenge for a number of countries. These gaps can easily be resolved through national legislation. Moreover, jurisdictional issues generally do not prevent prosecution or cooperation. As the Draft Study itself notes, it is likely that at least one, if not more, countries can assert jurisdiction over online criminal conduct as well as jurisdiction over the defendant. Thus, it is not necessary or appropriate to consider a new legal instrument as proposed in the Draft Study, as the challenges detailed above can and should be addressed through robust legislative assistance, capacity-building, and active dialogue between law enforcement agencies through networks.