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

Reproduced as received

28 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 after the extended deadline of 14 March 2018. A total of three contributions were received from the following Member States: Mexico, Philippines and Poland.

MEXICO

Insumos del Gobierno de México para la 4ª Reunión del Grupo de Expertos sobre Delito Cibernético sobre los temas de legislación y marcos y criminalización

Como marco general de referencia, el 14 de noviembre de 2017 se presentó en México la Estrategia Nacional de Cibserseguridad (ENCS), lo que representa un avance importante para alinear los esfuerzos de autoridades y otros sectores para promover un ciberespacio seguro, estable, libre y accesible. La ENCS establece la visión del Estado mexicano en la materia, a partir del reconocimiento de:

- La importancia de las tecnologías de la información y comunicación (TIC).
- El creciente número de Ciberdelitos.
- La concientización sobre la necesidad de tener una cultura de la Ciberseguridad.

Tiene su fundamento en el Plan Nacional de Desarrollo 2013-2018 y contribuye de manera importante al logro de los objetivos planteados por el Programa para un Gobierno Cercano y Moderno 2013-2018, el Programa Nacional para la Seguridad Pública 2014-2018, así como del Programa para la Seguridad Nacional 2014-2018.

Derivado de la complejidad y naturaleza transfronteriza de las dinámicas de la era digital, se advierte la necesidad de abordar la Ciberseguridad de forma integral, colaborativa, holística y transversal.

Por ello, la ENCS define los siguientes objetivos y principios rectores:

[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

Objetivos estratégicos:

1. Sociedad y derechos.
2. Economía e innovación.
3. Instituciones públicas.
4. Seguridad pública.
5. Seguridad nacional.

Principios rectores:

A. Perspectiva de derechos humanos.
B. Enfoque basado en gestión de riesgos.
C. Colaboración multidisciplinaria y de múltiples actores.

Cabe destacar, que el objetivo general de la Estrategia establece acciones en materia de Ciberseguridad aplicables a los ámbitos social, económico y político.

Dicho documento es resultado del trabajo intersecretarial y un ejemplo de buenas prácticas internacionales, ya que el borrador fue abierto a consulta pública, por lo que cuenta con las aportaciones sustantivas de expertos de la academia y la sociedad civil.

El Gobierno de México asumió un rol de facilitador concertando espacios de diálogo, discusión y aprendizaje mediante la celebración de foros y talleres realizados entre marzo y octubre de 2017.

Con el fin de alcanzar los objetivos estratégicos estipulados, se desarrolló a través de 8 ejes transversales que basan en los siguientes puntos:

1. Cultura de Ciberseguridad.
2. Desarrollo de capacidades.
3. Coordinación y colaboración.
4. Investigación, desarrollo e innovación TIC.
5. Estándares y criterios técnicos.
6. Infraestructuras críticas.
7. Marco jurídico y autorregulación.
8. Medición y seguimiento.

Igualmente, se prevé llevar a cabo diversas acciones que coadyuven al cumplimiento de dichos objetivos estratégicos, consistentes en:

- El desarrollo de capacidades de operadores jurídicos y tomadores de decisiones en instituciones públicas y privadas que permitan proponer modificaciones o armonización legislativa.
- Certeza jurídica para que las instancias de procuración de justicia incrementen su eficacia en la investigación, prevención y persecución de ciberdelitos y en la sanción a la ciberdelincuencia.
- Procedimientos de autorregulación que favorezcan la construcción de confianza entre individuos, sector público y organizaciones privadas en pleno cumplimiento de la ley.
- La homologación y armonización de códigos penales y leyes complementarias en torno a ciberdelitos.

La ENCS tiene como visión que para el año 2030 el Estado mexicano sea una nación resiliente ante los riesgos y amenazas en el ciberespacio.

Asimismo, y en consonancia con los esfuerzos institucionales que México realiza para afrontar el reto de consolidar la implementación y operación de su nuevo Sistema de Justicia Procesal Penal Adversarial (SJPA), así como los desafíos internacionales respecto a la necesidad de robustecer las respuestas jurídicas y de investigación de los delitos en el ciberespacio, el Gobierno Federal a través de la Procuraduría General de la República (PGR) ha optado por construir nuevas capacidades que permitan fortalecer las instituciones de seguridad y procuración de justicia, para enfrentar los retos, riesgos y amenazas que supone el avance hacia un mundo con sociedades interconectadas, a partir del acceso universal a Internet, considerando que el delito cibernético, informático, electrónico o virtual y quizá cualquier otro delito difícilmente pueda quedar exento de vinculación alguna con evidencia digital y pruebas electrónicas.

En este contexto, es importante destacar que en 2017 México enfrentó múltiples y complejos desafíos en el ámbito de la procuración de justicia, el principal fue la implementación del SJPA, que implica una nueva visión y forma de actuación policial.

A este gran reto interno, se suma la necesidad de considerar aquél que representa garantizar la seguridad de individuos, organizaciones privadas y entidades públicas de posibles incidentes cibernéticos maliciosos, y que ésta dependa de la habilidad para mantener la protección de las actividades cotidianas de todos los usuarios sucesos cibernéticos que amenacen la seguridad de los sistemas digitales.

Ante estos desafíos, la PGR inició un proceso de introspección, con la finalidad de identificar áreas de oportunidad y opciones de mejora inmediatas para diseñar una arquitectura institucional congruente con los fines y principios constitucionales del SJPA, que eventualmente pueda ser replicable a todas las instituciones de procuración de justicia del país.

Un primer paso se dio en febrero de 2017, cuando la PGR presentó al Senado el diagnóstico institucional "Hacia un nuevo modelo de justicia", cuyos principales hallazgos fueron:

1) Para la plena consolidación del SJPA se considera indispensable eliminar prácticas y procesos basados en una cultura penal inquisitiva que resultan incompatibles con el nuevo sistema penal y;
2) Visibilizar las condiciones que guarda la operación del sistema.

Este diagnóstico contempló la propuesta de realizar una amplia Consulta Nacional sobre el Modelo de Procuración de Justicia, en la que participaron prestigiadas instituciones académicas e instancias gubernamentales. El resultado de esa Consulta Nacional se plasmó en el Informe Ejecutivo de la Consulta Nacional sobre el Modelo de Procuración de Justicia 2017. Entre sus principales recomendaciones destaca la necesidad de que las fiscalías cuenten con capacidades para desarrollar investigaciones sólidas para: a) Garantizar el esclarecimiento de los hechos y b) Identificar y sancionar a los responsables de la comisión de delitos.

- Buenas Prácticas

a) Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas (UICOT)

En el contexto de transición hacia un nuevo Sistema de Justicia Penal, una acción determinante para aprovechar las oportunidades y opciones de mejora, que permitió impulsar los esfuerzos institucionales para contar con áreas de investigación especializadas fue la publicación el 5 de septiembre de 2017 del Acuerdo por el que se crea la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas (UICOT)[2], adscrita a la Agencia de Investigación Criminal (AIC), como instancia de inteligencia encargada de ejecutar y

[2] Acuerdo A/076/17 del Procurador General de la República.

supervisar acciones policiales de apoyo a investigaciones relacionadas con medios electrónicos y tecnológicos.

A través de los servicios técnico-especializados de esta nueva Unidad, se pretende fortalecer la investigación y el combate del delito cibernético, usando herramientas tecnológicas en apoyo al Ministerio Público, autoridades competentes y áreas sustantivas de la PGR en sus diferentes procesos de investigación.

Adicionalmente, con la creación de esta nueva Unidad, se busca garantizar la seguridad de la información institucional, a través del establecimiento de normas y directivas que, en coordinación con otras áreas de la Institución, definan y supervisen el Sistema de Gestión de Seguridad de la Información.

Con estas nuevas capacidades, la PGR podrá hacer frente a la creciente amenaza que plantean los ataques cibernéticos, así como aprovechar las oportunidades que presenta la nueva era digital y enfrentar los retos crecientes en el ámbito de la seguridad cibernética, particularmente, con la estructuración de esta nueva Unidad y sus 4 áreas de especialización, a través de las cuales brinda los siguientes servicios: Ciberseguridad, Investigación e Inteligencia Cibernética, Operaciones Tecnológicas y Tecnología para la Investigación.

Asimismo, contribuirá a establecer las normas y directivas de seguridad de la información institucional, comenzando con la elaboración del Reglamento para el uso de las tecnologías de la información, para fortalecer tanto la seguridad de la información como su confidencialidad, integridad y disponibilidad.en las labores que realiza la UICOT.

b) Equipo de Seguridad y Respuesta de Incidentes Cibernéticos (CSIRT)

Actualmente se realizan trabajos para la creación de un Equipo de Seguridad y Respuesta a Incidentes Cibernéticos (CSIRT) para la Agencia de Investigación Criminal (AIC) que se espera pueda extender su cobertura en el largo plazo para a toda la PGR, con el propósito de que controle y minimice cualquier tipo de daño tecnológico a la institución y su información, y de que cuente con capacidad para preservar evidencia y documentarla para conocer a fondo el contexto de cualquier incidente cibernético, determinar su origen y posibles consecuencias.

A través del CSIRT se pretenden coordinar las actividades nacionales e internacionales para una recuperación rápida y eficiente de las actividades que pudieran ser afectadas, de manera tal que la institución pueda operar con normalidad en el menor tiempo posible y con el menor impacto tolerable. Lo anterior, con la finalidad de prevenir eventos que puedan ocurrir en el futuro y tener la capacidad de erradicar las causas de raíz de los incidentes potenciales.

Con la creación de este equipo profesional especializado en prevenir, identificar, erradicar e investigar delitos cibernéticos se proveerá a la PGR de personal, mecanismos, manuales, protocolos y procedimientos de ciberseguridad robustos que impidan ser blanco de actividades intrusivas (*hackeo)* dirigidas a vulnerar la infraestructura tecnológica y la información contenida en ella.

Este equipo altamente especializado permitirá generar una base de conocimientos que registre las lecciones aprendidas de estos sucesos, con el objetivo de evitar que se repitan y de suceder, se cuente con un antecedente de las posibles soluciones.

Adicionalmente, este equipo de respuesta será un punto de contacto para compartir información (*cooperación operativa*) relacionada con incidentes de seguridad con otros CSIRT, con fines de difusión y mitigación del impacto de nuevas amenazas, vulnerabilidades o incidentes.

- **Medidas a nivel nacional**

a) Proyecto de Código Penal Nacional

Actualmente, la Procuraduría participa activamente en la discusión del Proyecto de Código Penal Nacional, emitiendo comentarios y aportaciones respecto a los temas de su competencia, en dos aspectos fundamentales:

1. Modificar la sintaxis de la redacción utilizada para dar estructura lógica a la conducta que se requiere tipificar, evitando de esa manera repeticiones ociosas e infructuosas que dificulten la aplicación y la interpretación de los operadores jurídicos al momento de aplicar la norma.

2. Establecer una semántica marco/tipo para los ciberdelitos (delitos informáticos), a fin de no dejar margen la interpretación de los operadores jurídicos sobre los tecnicismos en la materia.

b) UICOT

A poco tiempo que esta nueva unidad especializada inició operaciones, se han detectado los siguientes impactos directos en investigaciones y operaciones:

- La detección, clasificación y erradicación de diferentes amenazas cibernéticas dentro de infraestructura cibernética en el territorio mexicano: *defacement*, *phishing* y la distribución de código malicioso (*malware*).
- Emisión de boletines o alertas derivada de investigaciones cibernéticas de diferentes amenazas detectadas en instituciones gubernamentales, así como de acciones de intrusión y ataques de negación de servicios (*DDoS*).
- Documentación, investigación y respuesta a distintos incidentes cibernéticos tanto en instituciones gubernamentales, como en empresas del sector privado.

c) Colaboración a través de INTERPOL

En coordinación con INTERPOL y a través de su Centro de Ciber Fusión, se participó activamente en la Operación Internacional *Ciber Surge*, la cual tuvo como objetivo fortalecer las capacidades de países miembros para prevenir, detectar y responder a ciberamenazas.

- **Recomendaciones**

Ante la tendencia internacional y el surgimiento de innovaciones delictivas de los ciberdelincuentes, se considera pertinente explorar y profundizar el conocimiento, experiencias y buenas prácticas sobre la necesidad de incluir en los marcos regulatorios nuevos ámbitos, tales como: medidas o técnicas de investigación, jurisdicción (*datos extraterritoriales*), evidencia electrónica (*volatilidad y admisibilidad*) y cooperación internacional (*convenios multilaterales inclusivos*).

De igual manera, se estima esencial considerar la posibilidad de establecer una semántica marco para el tema del ciberdelito, lo suficientemente amplia como para abordar las diversas manifestaciones de este fenómeno y, a su vez, lo suficientemente concisa para cerrar los márgenes de interpretación de los operadores jurídicos sobre los tecnicismos en la materia.

PHILIPPINES

I. Accession to the Budapest Convention on Cybercrime

The Convention on Cybercrime, also known as the Budapest Convention (Convention), is an international treaty which seeks to address computer and internet crimes by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. Specifically, the Convention aims to protect society against cybercrime "by providing for the criminalization of such conduct and the adoption of powers sufficient for effectively combating such criminal offenses, by facilitating their detection, investigation and prosecution at both domestic and international levels and by providing arrangements for fact and reliable international cooperation."

On 19 February 2019, the Republic of the Philippines (Republic) obtained the required Senate Concurrence in the Accession to the Convention, which was previously signed by the President Rodrigo Roa Duterte on 9 December 2016.

It maybe be recalled that even pending accession, the Convention has earlier provided the Philippines with the necessary legal framework in adopting appropriate legislation which paved the way for the enactment of the first comprehensive domestic legislation on cybercrime and cyber-related offenses, that is, Republic Act (R.A.) No. 10175 or the Cybercrime Prevention Act of 2012.

R.A. No. 10175 was adopted in conformity with the Convention's principal parts: (1) the first part identifies the substantive cybercrime offenses which each ratifying State is obliged to adopt in its domestic law, (2) the second part deals with investigative procedures that States must implement, and (3) the third part relates to mechanism that will enhance international cooperation.

II. Adoption of ASEAN Declaration to prevent and combat cybercrime

During the last quarter of 2016, the Philippines, through the Department of Justice initiated the crafting of ASEAN Declaration to Prevent and Combat Cybercrime (Declaration) in line with the integration of cybercrime as one of the transitional crimes under the purview of the ASEAN Plan of Action to Combat Transnational Organized Crime, which was adopted during the 2nd AMMTC on 23 June 1999 in Yangon, Myanmar, in relation to the 3rd AMMTC on 11 October 2001 in Singapore.

Among others, the Declaration envisions a united ASEAN committed to battling cyber-criminals who pervade the cyberspace, in conformity with one of its purposes, that is, "*to respond effectively, in accordance with the principle of comprehensive security, to all forms of threats, transnational crimes and transboundary challenges.*"

In particular, the Heads of State/Government of the ASEAN, on 14 November 2017, have resolved to strengthen the commitment of ASEAN Member States to cooperate at the regional level in preventing and combating cybercrime by "acknowledging the importance of harmonization of laws related to cybercrime and electronic evidence" and "encouraging ASEAN Member States to explore the feasibility of acceding to existing regional and international instruments in combating cybercrime."

III. Amendment on domestic legislation on cybercrime

In line with the Philippines' efforts to further strengthen the law and in order to level the playing field with its foreign counterparts in pursuing a common criminal policy aims at the protection of society against cybercrimes, the Department of Justice initiated the drafting of the amendatory bill to its domestic

cybercrime law, R.A. No. 10175, which is one of the legislative priority measures of the present administration.

The proposed amendatory bill integrates the concept of cybercrime investigation wherein investigating prosecutors will be assigned to supervise the investigation being conducted by the law enforcements authorities as early as the case build up state. Under this set-up, law enforcers shall take guidance from the investigating prosecutors in the process of conducting investigations, especially when the former needs advice/assistance with matters concerning laws and rules of procedure and evidence-gathering. It is envisioned that this proposition will ensure the success of cybercrime investigation and prosecution.

In addition, the proposed amendatory bill likewise seeks to remove the crime of cyber libel or committed by, through and with the use of information and communications technologies from its scope, as it is a mere for of publication which is already covered by the Republic's Criminal Code.

POLAND

The Ministry of the Interior and Administration – remarks for the Expert Group on Cybercrime meeting – April 2018

In view of the forthcoming 4th session of the intergovernmental Expert Group on Cybercrime (3-4 April, 2018) Poland would like to draw attention to the following issues which require international consultation and action. The transborder character of cybercrime require cooperation on international fora, including regulatory solutions.

- an unequal validity of telecom data retention period - an attempt in view of harmonization of the regulations in this area, would improve the process of acquiring data for operational purposes. In Poland, according to the Telecommunication Law of 16 July 2014, para 180 a section 1.1, the data retention time is 12 months.

- searching cloud computing in domains (Gmail, iCloud, Onedrive etc.) during the implementation of procedural activities. At present, there are discrepancies in legal interpretations as to the validity of such actions, in relation to both servers in the EU countries, or outside the UE.

- implementation of telecommunications and internet arrangements, in the so-called NAT (Network Address Translation) services. Based on the Police actions (based on Chief Police Officer Decision no 98, of April 1, 2016, on obtaining and processing of telecommunications, postal and internet data by the Police) the functioning of IP addresses belonging to the group assigned dynamically to subscribers in the conditions of telecommunications overload of network and transmission devices, which can be used by many users at the same time, has been identified. In order to clearly establish the user who is in the Police's interest, it is necessary to provide - in addition to the IP address - also the network port number of the terminal device initiating the call, which is once insufficient and prevents the performance of operational activities by the officers of the Polish Police.

- methods and forms of exchanging information concerning (in relation to the competence of the police division concerned) inter alia the end-user data to which IP addresses, data of internet domain owners or data of persons to whom the individual MSISDN (called the Mobile Station International Subscriber Directory Number) were assigned at given dates. An exchange of this information should be based on a bilateral agreement between Poland and another country requesting the operational data. As example, there is a bilateral agreement between Poland and Germany, of May 15, 2014, concerning cooperation between Police, Border and Customs Authorities , which relates as well to exchange of information on "subscribers

and users of telecommunications and teleinformation networks" and "data from information systems, registers and other data sets kept in accordance with the internal law of a given Party".