Greetings!

It is with great pleasure to present the 2016-2017 Philippine Cybercrime Report by the Department of Justice – Office of Cybercrime, which accounts the current trends, challenges, and developments in the field of cybercrime, including future plans and programs in response thereto.

We have considered cyberspace a new dimension - an online dimension - along with land, air, water - where we have to regulate and extend our mandate. This is a sense of justice challenge and an accretion to our essential task to ensure a safer and secured online environment for all, especially our children.

We will continue shaping our strategic plans and initiatives, developing innovative capabilities based on international legal and technical regime, and removing clouds of uncertainty in enforcing Republic Act No. 10175, or the Cybercrime Prevention Act of 2012, and other cyber-related laws.

Each of us is responsible for establishing a justice system that suppresses both traditional and online crimes before it occurs, brings perpetrators to justice, and instills trust and confidence in the people to come forward and seek justice.

I wish to thank everyone in the criminal justice system who continuously supports the Department’s fight against cybercrimes. Rest assured that we will continue guarding the rights and safety of every Filipino in the cyber domain.

*Mabuhay at maraming salamat po!*
# CONTENTS

## I. Updates on the Department of Justice – Office of Cybercrime
- (a) Accession to the Budapest Convention on Cybercrime
- (b) Central Authority and 24/7 Point of Contact
- (c) National Center for Missing and Exploited Children Point-of-Contact

## II. Current Trends on Cybercrime
- (a) Core Cybercrimes
- (b) Computer-related Offenses
- (c) Content-related Offenses
- (d) All other crimes committed by, through and with the use of Information and Communications Technology

## III. Accomplishments
- (a) Issuances/Advisories
- (b) Operational Achievements
  - i. Cases
  - ii. Capacity Building
  - iii. International Cooperation

## IV. Authorities under the Cybercrime Prevention Act of 2012
- (a) Cybercrime Investigation and Coordinating Center
- (b) National Bureau of Investigation – Cybercrime Division
- (c) Philippine National Police – Anti-Cybercrime Group

## V. Inter-Agency Cooperation
- (a) Inter-Agency Council Against Child Pornography
- (b) Inter-Agency Council Against Trafficking
- (c) National Law Enforcement Coordinating Committee - Sub-Committee on Cybercrime

## VI. Public – Private Partnership

## VII. Future Plans and Programs
- (a) Cybercrime Prevention Act version 2.0
- (b) Rules of Procedure for Cybercrime and Cyber-Related Cases and Designation of Cybercrime Courts
- (c) National Computer Forensics Training Program
- (d) Victim Identification Program
CHAPTER 1

UPDATES
(a) Accession to the Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime\(^1\) is the first international treaty on crimes committed via the Internet and other computer networks, upon which Republic Act (R.A.) No. 10175 or the Cybercrime Prevention Act\(^2\) is patterned, which pursues a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate domestic legislation and fostering international cooperation through the establishment of 24/7 Points of Contact, Mutual Legal Assistance (MLA), and Extradition.

Upon DOJ’s initiative, the Committee of Ministers of the Council of Europe (COE), at the 1026th meeting of the Ministers’ Deputies on 15 May 2007, invited the Philippines to accede to the Convention on Cybercrime, provided that all the necessary implementing measures have been complied with. In a letter dated 15 June 2011, the COE Secretary General Thorbjorn Jagland formally invited the Philippines to accede to the Budapest Convention.

---

1. Treaty No. 185, 23 November 2011. Herein after referred to as the “Convention”.
2. Hereinafter referred to as the “Cybercrime Law”.
In 2012, the Department of Science and Technology (DOST), Department of the Interior and Local Government (DILG), and DOJ issued their respective Certificates of Concurrence (COCs) acceding to the Convention. However, due to the Constitutional challenge against the Cybercrime Law, the submission of the COCs to the Department of Foreign Affairs (DFA) was deferred.

Come 2015, R.A. No. 10844 or the Department of Information and Communications Technology (DICT) Act of 2015 was enacted. By virtue of the DICT Act, the Information and Communications Technology Office (ICTO) under DOST was abolished, and their powers and functions, applicable funds and appropriations, records, equipment, property, and personnel were transferred to DICT 3.

Because of this development, as well as the change brought about by the Duterte Administration, DFA required the issuance of updated COCs from DOJ, DICT, and DILG in 2016.

In this regard, the DOJ-Office of Cybercrime (DOJ-OOC), as the designated Central Authority under the Cybercrime Law, spearheaded the collection of said COCs and submitted the same to DFA for collation in September 2016.

In October 2016, DFA, through the Office of Legal Affairs (OLA), transmitted the Accession Package to the Convention to the Office of the President for the Executive Secretary’s review and subsequent endorsement to President Rodrigo R. Duterte.

As of December 2016, the Instrument of Accession to the Convention was signed by President Rodrigo R. Duterte and the same was endorsed to the DFA-OLA, while the Accession Package was transmitted to the Senate for concurrence.

Once the Senate signifies its concurrence, the Senate Resolution providing for the same and the signed Instrument of Accession will be deposited by the DFA-OLA to the Secretary General of the COE.

(b) Central Authority and 24/7 Point of Contact

In relation to the immediately preceding subsection, DOJ-OOC, being the Central Authority as provided under the Cybercrime Prevention Act, has likewise been designated as the 24/7 Point of Contact in the Philippines, in accordance with the requirements of the Convention.

3 Section 15, Republic Act (R.A.) No. 10844.
It may be recalled that under Articles 24 and 27 of the Convention, a Party-State is required to designate a Central Authority, which is primarily responsible for making or receiving direct requests for extradition or mutual legal assistance to another Party-State. In addition, Article 35 of the Convention also mandates the establishment of 24/7 Point of Contact to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences.

Relatively, Section 23 of the Cybercrime law created the DOJ-OOC which shall act as the Central Authority in all matters related to international mutual assistance and extradition with regard to cybercrime and cyber-related cases.

A Note Verbale for this purpose has been executed by the DFA-OLA, which will be deposited to the Secretary General of the COE along with the Instrument of Accession and Senate Concurrence.

(c) National Center for Missing and Exploited Children Point of Contact

The National Center for Missing and Exploited Children (NCMEC) is a non-profit organization authorized by a United States (US) law\(^4\) to receive reports on online child abuse and sexual exploitation (OCASE) from electronic communication service providers such as internet service providers (ISPs) and electronic mail service providers (ESPs) operating in the US.

Pursuant to its mission and congressional authorization\(^5\), NCMEC operates the CyberTipline® and the Child Victim Identification Program to provide assistance to law enforcement and others in their efforts to identify and rescue victims of OCASE.

It may be recalled that in April 2014, DOJ-OOC was designated as the NCMEC Point-of-Contact in the Philippines. By virtue of said designation, DOJ-OOC is being notified, and is provided with access to NCMEC’s Virtual Private Network (VPN), every time it receives a report that has a Philippine nexus – either the offender or offended party is situated in the Philippines.

Numerous enforcement operations resulting in the arrest of the offender and rescue of victims were conducted on the basis of these reports. To date, the DOJ-OOC receives an average of one thousand five hundred (1,500) reports from NCMEC per month.

\(^4\) 18 U.S.C. § 2258A.
CURRENT TRENDS ON CYBERCRIME
Statistics show that from January to December 2016, the DOJ-OOC, National Bureau of Investigation – Cybercrime Division (NBI-CCD0, and Philippine National Police – Anti-Cybercrime Group (PNP-ACG), received a total of three thousand nine hundred and fifty-one (3,951) complaints for cybercrime and cyber-related offenses. This is 53.92% higher than the number of complaints received last year, which totaled to two thousand five hundred and sixty-seven (2,567).

**(a) Core Cybercrimes**

Out of the total number of complaints filed for cybercrime and cyber-related offenses in 2016, only three hundred twenty-two (322) pertains to offenses against the confidentiality, integrity and availability of computer data and system under Section 4 (a) of the Cybercrime Law.
(b) Computer-related Offenses

Eight hundred thirty (830) complaints received by the relative law enforcement agencies (LEAs) in 2016 pertain to computer-related offenses under Section 4 (b) of the Cybercrime Law. This category includes “E-mail Spoofing” and “Phishing”, which are considered as computer-related forgery and computer-related fraud, respectively.

(c) Content-related Offenses

Under Section 4 (c) of the Cybercrime Law, cybersex, child pornography, and libel are categorized as content-related offenses. In 2016, a total of six hundred forty (640) complaints were received by the respective LEAs, with libel as the most complained about offense.

Treated separately, but under the same category, are the NCMEC Reports concerning OCASE, which were received by the DOJ-OOC in 2016.
(d) Crimes Committed by, Through and with the Use of ICTs

The biggest chunk of complaints relating to cybercrime and cyber-related offenses are the cyber-enabled offenses or those conventional crimes committed by, through and with the use of ICTs under Section 6 or the Cybercrime Law.

<table>
<thead>
<tr>
<th>Crimes</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Qualified Theft</td>
<td>2</td>
<td>6</td>
<td>10</td>
</tr>
<tr>
<td>2 Theft</td>
<td>11</td>
<td>15</td>
<td>9</td>
</tr>
<tr>
<td>3 Grave Threats</td>
<td>110</td>
<td>184</td>
<td>345</td>
</tr>
<tr>
<td>4 Photo and Video Voyeurism (R.A. No. 9995)</td>
<td>116</td>
<td>111</td>
<td>329</td>
</tr>
<tr>
<td>5 Access Device (R.A. No. 8484)</td>
<td>14</td>
<td>47</td>
<td>39</td>
</tr>
<tr>
<td>6 Violence against Women and Children (R.A. No. 9262)</td>
<td>10</td>
<td>8</td>
<td>31</td>
</tr>
<tr>
<td>7 Passport Act (R.A. No. 8293)</td>
<td>6</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>8 E-Commerce Act (R.A. No. 8792)</td>
<td>4</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>9 Trafficking (R.A. No. 9208/10364)</td>
<td>0</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>10 Unjust Vexation</td>
<td>11</td>
<td>33</td>
<td>52</td>
</tr>
<tr>
<td>11 Online Fraud/Scam</td>
<td>277</td>
<td>523</td>
<td>607</td>
</tr>
<tr>
<td>12 Intellectual Property</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>13 Illegal Gambling (P.D. No. 1602)</td>
<td>1</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>14 Robbery/Extortion</td>
<td>42</td>
<td>54</td>
<td>70</td>
</tr>
<tr>
<td>15 Falsification</td>
<td>4</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>16 Child Abuse (R.A. No. 7610)</td>
<td>14</td>
<td>8</td>
<td>37</td>
</tr>
<tr>
<td>17 Illegal Recruitment</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>18 Others (Not specified)</td>
<td>2</td>
<td>0</td>
<td>20</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>628</strong></td>
<td><strong>1,007</strong></td>
<td><strong>1,578</strong></td>
</tr>
</tbody>
</table>
(a) Issuances/Advisories

i. Advisory on Online Shopping Fraud

Issued on 30 April 2015, the Advisory on Online Shopping Fraud was published to apprise online buyers of the risks involved in dealing online and, at the same time, to provide guidelines to the general public for a secure online shopping experience, in the promotion of consumer welfare.

Said advisory tackled relevant laws on the matter, such as R.A. No. 7394 or the Consumer Act of the Philippines, R.A. No. 8792 or the Electronic Commerce Act of 2000, R.A. No. 10173 or the Data Privacy Act of 2012, and the Cybercrime Law, and discussed what constitutes deceptive sales practices and other prohibited actions on the merchants’ part based on said laws.

Ultimately, the advisory enumerated tips on how online shoppers can protect themselves from online shopping fraud, misleading or deceptive product advertisements, unexpected customs dues, transaction costs, and surcharges, and complicated delivery procedures, among others.

This advisory can be downloaded from - http://www.doj.gov.ph/files/ADVISORY%20ON%20ONLINE%20SHOPPING%20FRAUD(1).pdf

ii. Advisory on Online Child Abuse

In light of the augmenting number of complaints and reports being received by the DOJ-OOC and other relevant law enforcement agencies with regard to online child abuse, and the categorization thereof as one of the DOJ-OOC’s priority areas, the Advisory on Online Child Abuse was issued on 28 August 2015.

With the view of protecting the Filipino children from all kinds of online abuse and in accordance with the Constitutional duty of the State to protect the physical, moral, spiritual, intellectual, and social well-being of the youth, the DOJ-OOC, through this advisory, appealed to the general public, specifically the parents, to be conscientious of their children’s activities in the cyberspace.

Through this advisory, the general public was informed of the types of child abuse committed online, its critical impact on a child-victim, types of offenders in the cyberspace, and ways and means on how and to whom to report incidents of online child abuse.


iii. Securing All Filipino children from Exposure to harmful online contents (SAFE)

In July 2016, the DOJ-OOC issued the advocacy material entitled “Securing All Filipino children from Exposure to harmful online contents” or SAFE, in order to provide the public, the parents in particular, with an easy step-by-step procedure on how to keep their mobile phones, be it iOS or Android, from displaying explicitly unsuitable materials and mobile applications for the Filipino children.

This material is available at - http://doj.gov.ph/files/cybercrime_office/Safer%20use%20of%20Smartphones-01.pdf
(b) Operational Achievements

i. Cases

1) "Oplan Fountain"

In November 2016, the DOJ-OOC, together with the Bureau of Immigration (BI) – Fugitive Search Unit (FSU) and the PNP – Special Action Force (SAF), conducted verification, investigation, and law enforcement operations against Chinese nationals situated in Clark, Pampanga, whose acts constitute violation of immigration and employment laws, rules and regulations.

During the course of the operation, the operatives were able to apprehend one thousand three hundred (1,300) Chinese nationals, more or less, who were allegedly engaged in illegal online gambling, for lack of permit and/or license to operate.

To date, forty-three (43) Chinese nationals were charged with violation of Section 1 of P.D. No. 1602, Prescribing Stiffer Penalties on Illegal Gambling, in relation to Section 6 of the Cybercrime Law before the DOJ National Prosecution Service.

In the same case, the DOJ-OOC was able to secure a Search Warrant and authority to conduct forensic examination and analysis over the digital equipment utilized by the Chinese nationals engaged in gambling operations such as computer monitors, CPU (Central Processing Unit) towers, laptop computers, modems, network routers, hub/ethernet port switches, uninterrupted power supply (UPS), removable storage media (compact discs, DVD discs, flash drives, compact flash cards), removable hard drives, and cellular phones, among others.

2) Commission on Elections Data Breach Incident

On 27 March 2016, COMELEC’s website was defaced and the site was replaced with contents pertaining to the hacktivist group Anonymous Philippines. On even date, another group named LulzsecPilipinas claimed that it was able to access and obtain COMELEC’s database which contains personal identifiable information (PII), including passport information and fingerprints data, of at least seventy (70) million registered Filipino voters. Said database was made available online through the website -https://wehaveyourdata.com.
Pursuant to the orders of the President sometime in April 2016, DOJ-OOC investigated and conducted technical surveillance on the matter. Through mutual legal assistance and international cooperation, the DOJ-OOC was able to shut down the website containing the leaked PII and prevented it from further circulation.

Two of the three (3) members of Anonymous Philippines who were responsible for the hacking incident were arrested and are currently on trial for violation of the Cybercrime Law.

3) Online Child Abuse Cases

Numerous enforcement operations resulting in the arrest of the offender and rescue of victims were conducted on the basis of the NCMEC Cybertipline Reports. Several reports contain information regarding travelling child sex offenders visiting the Philippines for child sex tourism. These reports are shared with the BI which resulted in the denial of entry of the sex offenders to the Philippines to prevent access to children in the country.

Recent arrests involving online child abuse and/or child sex tourism with American targets include the case of Calvin BERNDHART who was recently convicted in the United States (US) as a result of the excellent cooperation between DOJ-OOC and US Homeland Security Investigations.

Another significant operation which was successfully conducted by the DOJ-OOC concerns the Australian Gholamreza Farhani POUR, who frequently travelled in the Philippines from 2015-2016 to commit child sexual abuse and exploitation, and is thus charged with violation of R.A. No. 9775 or the Anti-Child Pornography Act of 2009 and R.A. No. 10364 or the Expanded Anti-Trafficking in Persons Act of 2012.

At present, another US citizen in the person of Gordon Cregeir SCHUCHARDT is detained with the PNP, and facing the same charges as POUR.

ii. Capacity Building


A two (2)-day training for DOJ Prosecutors, State Counsels, Public Attorneys, and Investigators from NBI and PNP, which discusses the role of ICTs in every stage of investigation, laws affecting ICTs, rules in the collection of evidence, appropriate procedure on investigation and prosecution, its presentation in court, up to the process for international cooperation.
To date, twelve (12) “Investigating and Prosecuting Cybercrimes: Focus on Electronic Evidence” Trainings were already conducted in the following Regions:

1. National Capital Region (NCR) on 02-03 July 2014 (Manila City);
2. NCR on 31 July-01 August 2014 (Manila City);
3. NCR on 18-19 September 2014 (Manila City);
4. NCR on 13-14 November 2014 (Manila City);
5. Region V on 16-17 December 2014 (Bicol);
6. Region VII on 28-29 January 2015 (Cebu City);
7. Region I on 17-18 February 2015 (La Union);
8. Cordillera Autonomous Region on 28-29 April 2015 (Baguio City);
9. Region X on 21-22 May 2015 (Cagayan De Oro);
10. Region IX on 24-25 June 2015 (Zamboanga);
11. Region XI on 15-16 September 2015 (Davao); and

2) First Responders for Cybercrime - Training of Trainers

The DOJ-OOC, in partnership with the COE under the Global Action on Cybercrime (GLACY) Project, has rolled out this training to establish a cadre of trainers in cyber incident response who will be able to cascade and instruct their colleagues on the proper approach to a crime scene containing electronic evidence and to process such in ways that will preserve its integrity and value.

Relatively, the training covers procedures on cyber incident response, proper handling of electronic and digital evidence, and development of training skills.

To date, the OOC has conducted three (3) First Responders for Cybercrime - Training of Trainers for the following law enforcers:

1. NBI, PNP, Philippine Drug Enforcement Agency (PDEA), then ICTO, Anti-Money Laundering Council (AMLC), Office of the Ombudsman (OMB) on 13-17 July 2015 (Clark, Pampanga);
2. Region VII NBI and PNP on 20-23 October 2015 (Cebu City); and
3. Region X NBI and PNP on 28-30 March 2016 (Cagayan de Oro City).

3) Basic and Advanced Judicial Trainings

The objective of the basic course is to train judges on how to appreciate electronic evidence presented before their respective courts, as well as to familiarize them with laws affecting ICTs and the Convention, in order for them to be enlightened in applying the same when resolving cases.
On the other hand, the advanced training is intended to reinforce the knowledge previously gained and to provide a greater insight into the challenges and methodologies involved in developing an air-tight case involving cybercrime and/or electronic evidence. The advance course is intended for judges who have successfully completed the basic course.

To date, five (5) Basic Judicial Trainings have been rolled-out for Judges in the NCR, Regions 3, 4, and 7; while an Advance Judicial Training was conducted for selected NCR, Regions 3, and 4 judges.

4) Basic and Advanced Digital Forensics Training

Both the basic and the advanced courses on Digital Forensics Trainings were participated in by the investigators from the NBI-CCD and the PNP-ACG, prosecutors, public attorneys, state counsels from the DOJ Legal Staff, and the personnel of the DOJ-OOC.

The aim of this training is to support the law enforcement agencies in the Philippines that are specialized in dealing with cybercrime and electronic evidence to get familiarized with both basic (stored data and computer systems forensics) and advanced (live data forensics) digital forensics skills and capabilities necessary for criminal intelligence and proper handling of electronic evidence in cybercrime cases.

iii. International Cooperation

As the designated Central Authority under the Cybercrime Law, the DOJ-OOC has facilitated twenty (20) international requests for assistance in 2016. This figure includes both legal and technical requests coming from, and to, the Philippines.

A significant number of requests received by the DOJ-OOC come from other law enforcement agencies and foreign counterparts. This include NBI-PNP, PNP-ACG, USDOJ, Turkish National Police Cybercrime Department, and Office of the Public Prosecutor General, Germany, among others.

These international requests involve preservation of data, provision of subscriber information of users, collection of computer and business data, as well as the seizure of domain names.
(a) **Cybercrime Investigation and Coordinating Center**

An inter-agency body under the administrative supervision of the Office of the President for policy coordination among concerned agencies and for the formulation and enforcement of the national cybersecurity plan is created under the Cybercrime Law, that is, the Cybercrime Investigation and Coordinating Center (CICC).

CICC is composed of an Executive Director as its Chairperson, with the Director of the NBI as Vice Chairperson, the Chief of the PNP, Head of the DOJ-OOC, and one (1) representative from the private sector and academe, as members.

Under the Cybercrime Law, the CICC have the following powers and functions to: (a) formulate a national cybersecurity plan and extend immediate assistance for the suppression of real-time commission of cybercrime offenses through a Computer Emergency Response Team (CERT); (b) coordinate the preparation of appropriate and effective measures to prevent and suppress cybercrime activities as provided for in the Cybercrime Law; (c) monitor cybercrime cases being bandied by participating law enforcement and prosecution agencies; (d) facilitate international cooperation on intelligence, investigations, training and capacity building related to cybercrime prevention, suppression and prosecution; (e) coordinate the support and participation of the business sector, local government units and nongovernment organizations in cybercrime prevention programs and other related projects; (f) recommend the enactment of appropriate laws, issuances, measures and policies; (g) call upon any government agency to render assistance in the accomplishment of the CICC’s mandated tasks and functions; and (h) perform all other matters related to cybercrime prevention and suppression, including capacity building and such other functions and duties as may be necessary for the proper implementation of the Cybercrime Law.

In the interim, Executive Order (E.O.) No. 189, Series of 2015, was issued by then President Benigno S. Aquino III creating the National Cybersecurity Inter-Agency Committee (NCIAC). By virtue of this E.O., the administrative and policy supervision over CICC was transferred from the Office of the President to NCIAC. Thereafter, R.A. No. 10844 or the DICT Act of 2015 was enacted mandating the attachment of CICC, for policy and program coordination, to DICT.

In line with this development, CICC has started formulating the National Cybersecurity Plan 2022 (NCSP), which identified key strategic imperatives that will combine efforts in order to achieve a resilient, safe, and secure cyber domain in the Philippines. CICC formally launched the NCSP in December 2016.

---

7. Section 25, R.A. No. 10175.  
8. Section 26, R.A. No. 10175.  
10. Section 15 (b)(3), R.A. No. 10844.
(b) National Bureau of Investigation – Cybercrime Division

In 2016, the NBI-CCD moved for its reorganization to achieve organizational development in the current structure of the office with the primary purpose of effectively improving its cyber response, digital forensic, and cyber security capability as mandated by the Cybercrime Law.

Said reorganization resulted in the creation of three (3) NBI Cybercrime Regional Centers in the Field Offices in Baguio for Luzon, Cebu for Visayas, and Davao for Mindanao, in line with the NBI’s policy in clustering its Field Offices.

For its laboratory, NBI-CCD was able to acquire new and updated forensic tools and software with the corresponding training for its digital examiners. It also operationalized a Mobile Digital Forensic Laboratory in 2016.

Relatively in May 2016, the DOJ-OOC loaned its digital forensic equipment to the NBI-CCD which shall be used primarily for investigations of cases involving child sexual abuse and exploitation and child pornography, in general.

(c) Philippine National Police – Anti-Cybercrime Group

Since its institution in 2013, PNP-ACG has established nine (9) Regional Anti-Cybercrime Office (RACO) in the entire country. In particular, there are RACOs for Regions I (Ilocos Region), III (Central Luzon), IV-A (CALABARZON), V (Bicol Region), VII (Central Visayas), IX (Zamboanga Peninsula), X (Northern Mindanao), XI (Davao Region), and XII (SOCCSKSARGEN).

With regard to capacity building, PNP-ACG developed four (4) specialized anti-cybercrime courses which are required to be completed by policemen who desire to be qualifies as “Cyber Cops”. These courses are: (1) Introduction to Cybercrime Investigation (ICIC); (2) Identification and Seizure of Digital Evidence (ISDE); (3) Introduction to Digital Forensic Investigation (IDFI); and (4) Proactive Internet Investigation Course (PIIC).

To date, PNP-ACG is composed of at least one hundred twenty (120) uniformed and non-uniformed personnel all over the administrative regions.
Section 20 of R.A. No. 9775 or the Anti-Child Pornography Act of 2009 established the Inter-Agency Council against Child Pornography (IACACP) to be chaired by the Secretary of the Department of Social Welfare and Development (DSWD) and composed of, as members, other relative government agencies\(^{11}\) and children’s non-governmental organizations.

From its inception, the DOJ-OOC has been an active member of the IACACP, in the performance of its functions relating to the formulation of comprehensive and integrated plans and programs to prevent and suppress any form of child pornography and in filing of cases against individuals, agencies, institutions or establishments that violate the provisions of R.A. No. 9775, among others. In the same vein, DOJ-OOC serves as the focal agency for cases concerning online child pornography.

One of the issues faced by the IACACP in 2016 was the internet service providers’ (ISPs) failure to comply with their filtering and blocking functions under Section 9\(^{12}\) of said law. In response thereto, the DOJ-OOC initiated the issuance of the Legal Opinion, dated 20 May 2016, reiterating that R.A. No. 9775 is presumed valid and constitutional until or unless otherwise ruled by the Supreme Court.

In this regard, the DOJ-OOC also spearheaded the drafting of Guidelines to Ensure Compliance of the ISPs with, and Implementation of, Section 9 said law, inclusive of steps which are to be strictly followed by the stakeholders to guarantee a child pornography-free cyberspace.

\(^{11}\) Secretary of the Department of Justice; (b) Secretary of the Department of Labor and Employment; (c) Secretary of the Department of Science and Technology; (d) Chief of the Philippine National Police; (e) Chairperson of the Commission on Information and Communications Technology; (g) Commissioner of the National Telecommunications Commission; (h) Executive Director of the Council for the Welfare of Children; (i) Executive Director of the Philippine Center for Transnational Crimes; (j) Executive Director of the Optical Media Board; and (k) Director of the National Bureau of Investigation.

\(^{12}\) Section 9. Duties of an Internet Service Provider (ISP). - All internet service providers (ISPs) shall notify the Philippine National Police (PNP) or the National Bureau of Investigation (NBI) within seven (7) days from obtaining facts and circumstances that any form of child pornography is being committed using its server or facility. Nothing in this section may be construed to require an ISP to engage in the monitoring of any user, subscriber or customer, or the content of any communication of any such person: Provided, That no ISP shall be held civilly liable for damages on account of any notice given in good faith in compliance with this section. Furthermore, an ISP shall preserve such evidence for purpose of investigation and prosecution by relevant authorities. An ISP shall, upon the request of proper authorities, furnish the particulars of users who gained or attempted to gain access to an internet address which contains any form of child pornography. All ISPs shall install available technology, program or software to ensure that access to or transmittal of any form of child pornography will be blocked or filtered. An ISP who shall knowingly, willfully and intentionally violate this provision shall be subject to the penalty provided under Section 15(k) of this Act. The National Telecommunications Commission (NTC) shall promulgate within ninety (90) days from the effectivity of this Act the necessary rules and regulations for the implementation of this provision which shall include, among others, the installation of filtering software that will block access to or transmission of any form of the child pornography.
(b) Inter-Agency Council against Trafficking

Similar with IACACP is the Inter-Agency Committee against Trafficking (IACAT) which is chaired by the Secretary of Justice\textsuperscript{13}. One of its primary functions is the promulgation of rules and regulations as may be necessary for the effective implementation of R.A. No. 9208, or the Anti-Trafficking in Persons Act of 2003, as amended by R.A. No. 10364 or the Expanded Anti-Trafficking in Persons Act of 2012.

Taking into consideration the part being played by ICTs in the commission of trafficking in persons, the DOJ-OOC has been designated as the Cyber-trafficking Unit of the IACAT early in 2016.

As such, DOJ-OOC works intimately with the IACAT for program and project coordination to effectively address the issues and problems attendant to trafficking in persons. It also recommends measures to enhance mutual assistance among foreign countries, through bilateral and/or multilateral arrangements, to prevent and suppress international trafficking in persons.

(c) National Law Enforcement Coordinating Committee – Sub-Committee on Cybercrime

For the effective and efficient enforcement of the Cybercrime Law, DOJ-OOC has joined the National Law Enforcement Coordinating Committee (NALECC) in 2015, and thus, NALECC – Sub-Committee on Cybercrime (SOCY) was created.

By virtue of its creation, NALECC-SOCY aims to strengthen inter-agency coordination with the primary purpose of combatting cybercrime and other cybercrime related activities by providing assistance in the anti-cybercrime campaign of other government, such as facilitating information sharing and arrest of personalities involved in cybercrime.

DOJ-OOC currently serves as the Chair of the NALECC-SOCY.

\textsuperscript{13} Section 20, R.A. No. 9208.
Public - Private PARTNERSHIP
In 2016, the government, through the DOJ-OOC and DSWD, with the assistance of various children’s non-governmental organizations such as UNICEF and Stairway Foundation, Inc., thought of countless ways on how to engage the private sector, specifically the ISPs, in keeping the cyberspace safe for the Filipino children.

One of which is the development of a curriculum by UNICEF, in coordination with the relative government agencies, which will be used to train ISPs to activate their roles in the government’s fight against online child sexual abuse and exploitation. The training is intended to be conducted during the first quarter of 2017.

Sometime in October 2016, the DOJ-OOC initiated a meeting with the Philippine Chamber of Telecommunication Operators (PCTO) in order to reinforce the government’s relationship with the private sectors, specifically with ISPs, regarding the latter’s compliance with the mandate of R.A. No. 9775 or the Anti-Child Pornography Act of 2009.

The government also supported the launch of the joint project of The Asia Foundation (TAF), the Australian Embassy, and DAKILA, entitled AlamBaU.ph, which is intended to be an online hub which educates, supports, and connects people together to advocate the protection of children from online sexual abuse and exploitation in September 2016. This is akin to the #StopChildPornPH Web Portal Project of the DSWD, which is one of the components of the National Online Prevention and Protection against Child Pornography, in addition to organization and capacity-building of child online protection advocates and the establishment of an online reporting and referral system for child pornography cases.
FUTURE PLANS AND PROGRAMS
(a) Cybercrime Prevention Act version 2.0

In its effort to strengthen the law, the DOJ-OOC is currently drafting version 2 of the Cybercrime Law which takes into consideration legislations in other jurisdictions, in order to level the playing field between the Philippines and its foreign counterparts in pursuing a common criminal policy aimed at the protection of society against cybercrimes.

(b) Rules of Procedure for Cybercrime and Cyber-Related Cases and Designation of Cybercrime Courts

Corollary to the Judicial Conference on Cybercrime held on 23 - 24 June 2016, where gaps between the Cybercrime Law and the Rules of Court were identified, the DOJ Technical Working Group\textsuperscript{14} drafted the Rules of Procedure for Cybercrime and Cyber-related Cases aimed at answering and filling up the technological requirements of cybercrime prosecution and adjudication in line with existing laws, rules, and jurisprudence.

In addition, said draft Rules also mentioned the designation of Cybercrime Courts in the Philippines as required under Section 21 of the Cybercrime Law.

In November 2016, the draft Rules was formally endorsed to Hon. Associate Justice Diosdado M. Peralta, Chairman of the Committee on the Revision of the Rules of Court, through the Office of the Court Administrator, for the said Committee’s consideration and review.

(c) National Computer Forensics Training Program

A National Computer Forensics Training Program (NCFTP) will be launched to train and capacitate our law enforcers in computer forensics jointly. The main purpose is to have a consolidated training for all law enforcement agencies in computer forensics and provide them with a structured procedures and guidelines consistent with international best practices.

In this regard, the OOC organized the CompTIA A+ Training and Examination in October 2016 to provide participants with basic fundamentals in computing technology that are essential for the effective and efficient handling, investigation, and prosecution of cybercrime incidents.

\textsuperscript{14} Department Order No. 539, s. 2016, creating the DOJ Technical Working in drafting special rules on Cybercrime and Cyber-Related Cases
The OOC also intends to incorporate the establishment of the NCFTP in version 2 of Republic Act (R.A.) No. 10175 or the Cybercrime Prevention Act of 2012 (Cybercrime Law) to ensure its institutionalization and appropriate funding.

(d) Victim Identification Program

In mid-2016, DOJ-OOC endeavored to put up a centralized database system that would store all known child pornographic materials gathered through investigations (including those from PNP and NBI), and intelligence gathering. A hash list of this database will be shared to all ISPs to serve as their reference for “filtering and blocking” child pornographic materials passing through their systems in line with their duty under R.A. No. 9775 or the Anti-Child Pornography Act of 2009.

This system will be integrated in the upcoming National Justice Information System (NJIS) and to other international systems such as the NCMEC and Interpol’s International Child Sex Exploitation (ICSE) database to maximize the law enforcers’ capacity to identify victims of child pornography. This will dramatically shorten the investigation process and it will surely make the prosecution more efficient.

This will be operationalized by Hubstream which is an intelligence analytics tool that will relate data intelligently. In 2016, Hubstream provided one (1) month proof of concept to DOJ-OOC for its investigation agents to have a feel and familiarize themselves with the said tool.