

PHILIPPINE NATIONAL POLICE
ANTI-CYBERCRIME GROUP



Philippines

Scope of Presentation

- Philippine National Police
- PNP Anti-Cybercrime Group
 - Types of Cybercrimes
 - Statistics and trends of cybercrime
 - Legal System
 - Cooperation with private sector
 - Digital Forensics
 - Training for Officers
 - International Cooperation
 - Case Study



Cybercrime in the Philippines

- **The “I LOVE YOU” Computer Virus**
 - The virus was received in e-mail inboxes in Hong Kong on 4 May, 2000, with subject “I LOVE YOU” an attachment “LOVE-LETTER-FOR-YOU.TXT.vbs.”. It erases or blurs the graphics and data in the computer. The damage was about US\$ 5.5 billion.
- Congress Response : Passing of Republic Act 8792 Electronic Commerce Act of 2000
 - Section 33 of the law has two (2) provisions that enumerates and penalizes the following acts:*
 - *Computer hacking,*
 - *Introduction of computer virus, and*
 - *Copyright infringement*
- PNP Response :
 - The creation of Computer Crime Unit (CCU) under the Anti-Transnational Crime Division (ATCD) of the Criminal Investigation and Detection Group (CIDG)



RA 10175 ALSO KNOWN AS “CYBERCRIME PREVENTION ACT OF 2012”

CHAPTER IV ENFORCEMENT AND IMPLEMENTATION

Section 10. *Law Enforcement Authorities.* — The National Bureau of Investigation (NBI) and the Philippine National Police (PNP) shall be responsible for the efficient and effective law enforcement of the provisions of this Act. The NBI and the PNP shall organize a cybercrime unit or center manned by special investigators to exclusively handle cases involving violations of this Act.



PNP Anti-Cybercrime Group



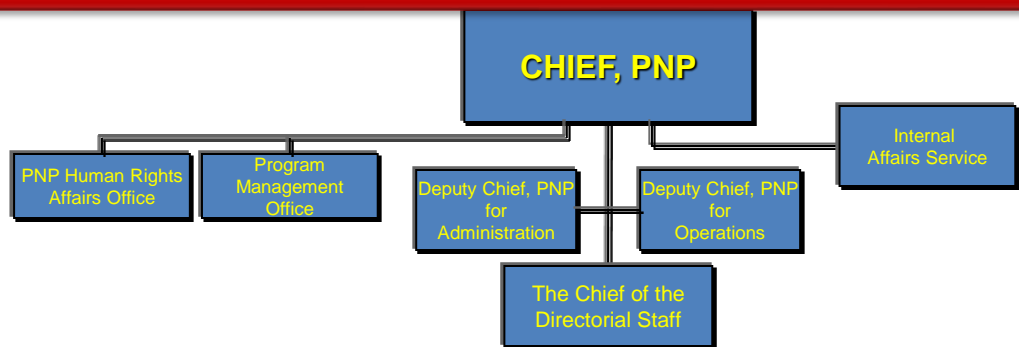
PHILIPPINE NATIONAL POLICE

ANTI-CYBERCRIME GROUP

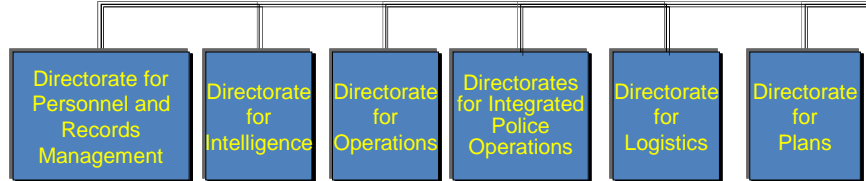


PNP Anti-Cybercrime Group

PNP Organizational Structure



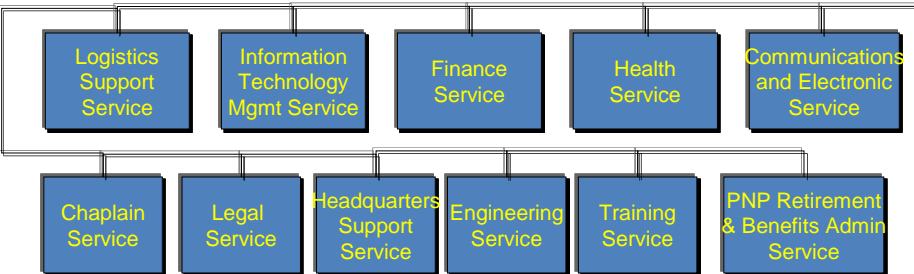
DIRECTORIAL



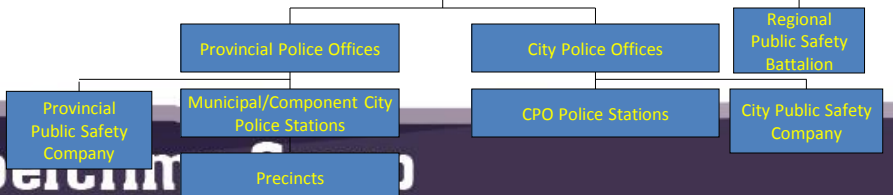
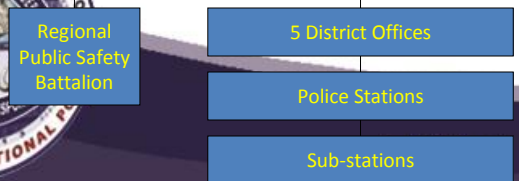
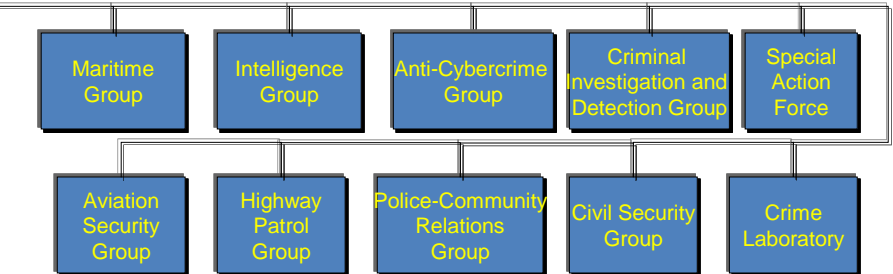
STAFF



Administrative Support Units



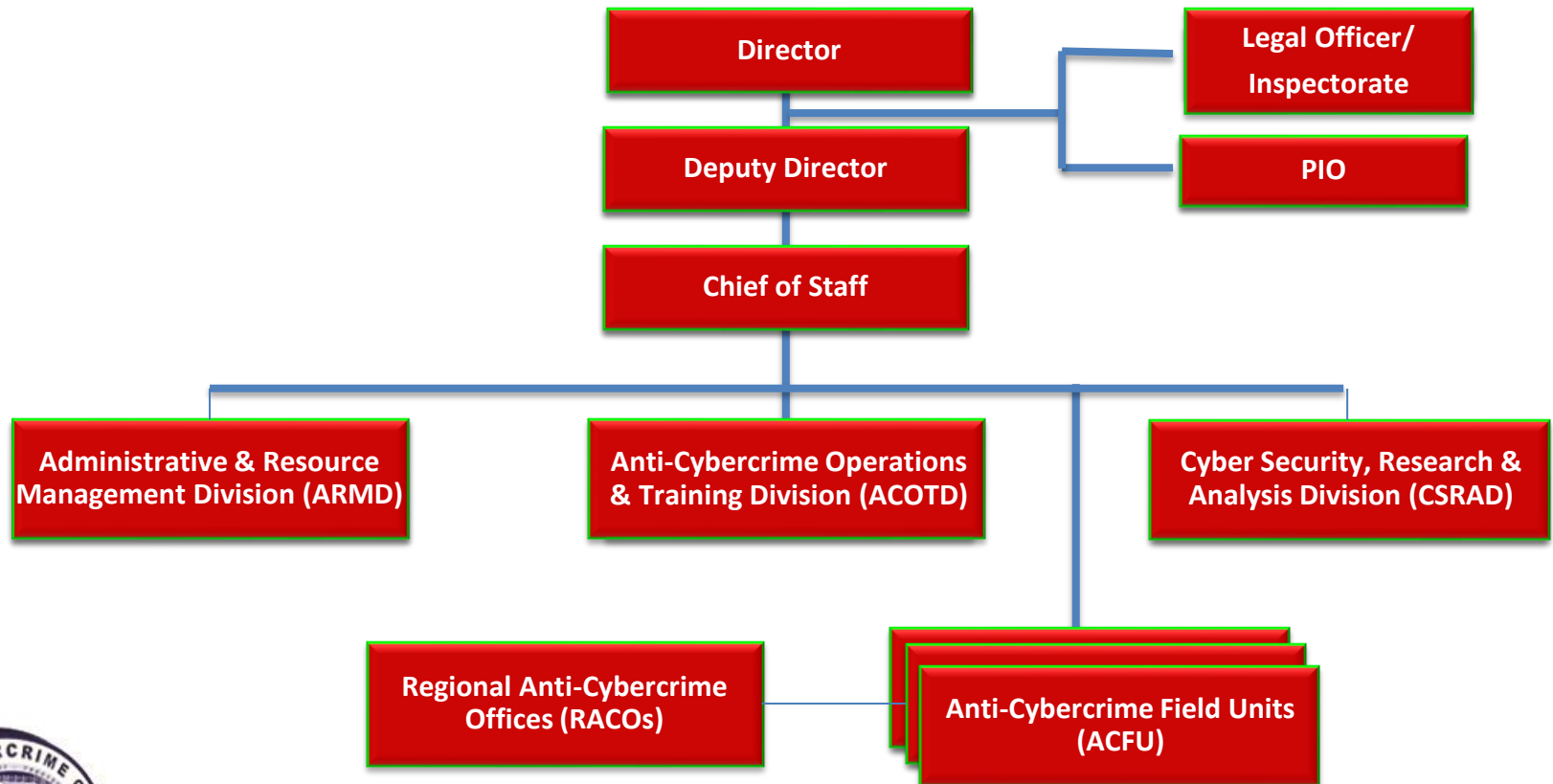
Operational Support Units



Anti-Cybercrime Center

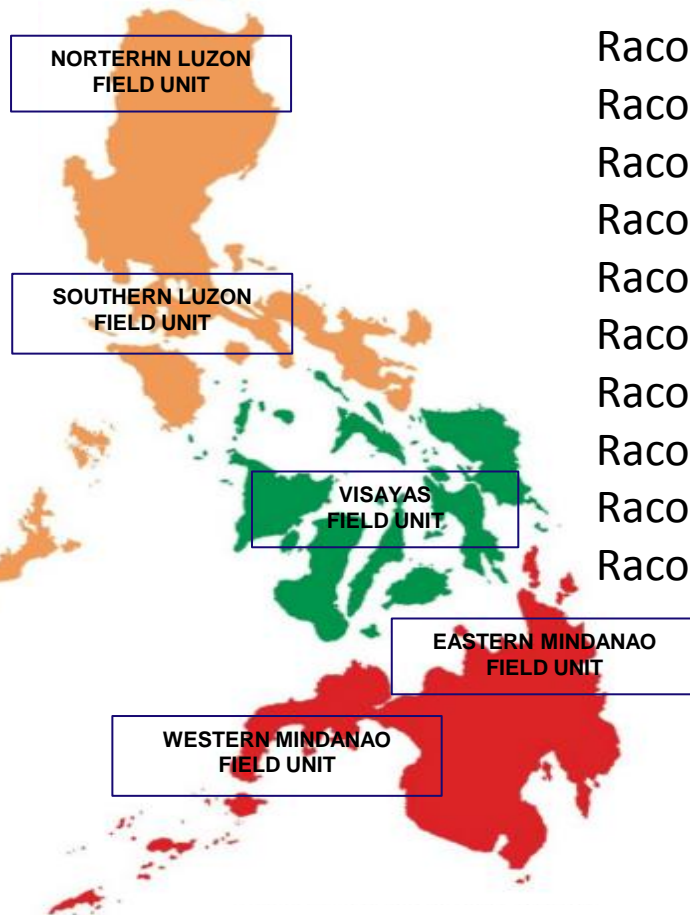
Anti-Cybercrime Group

Organizational Structure



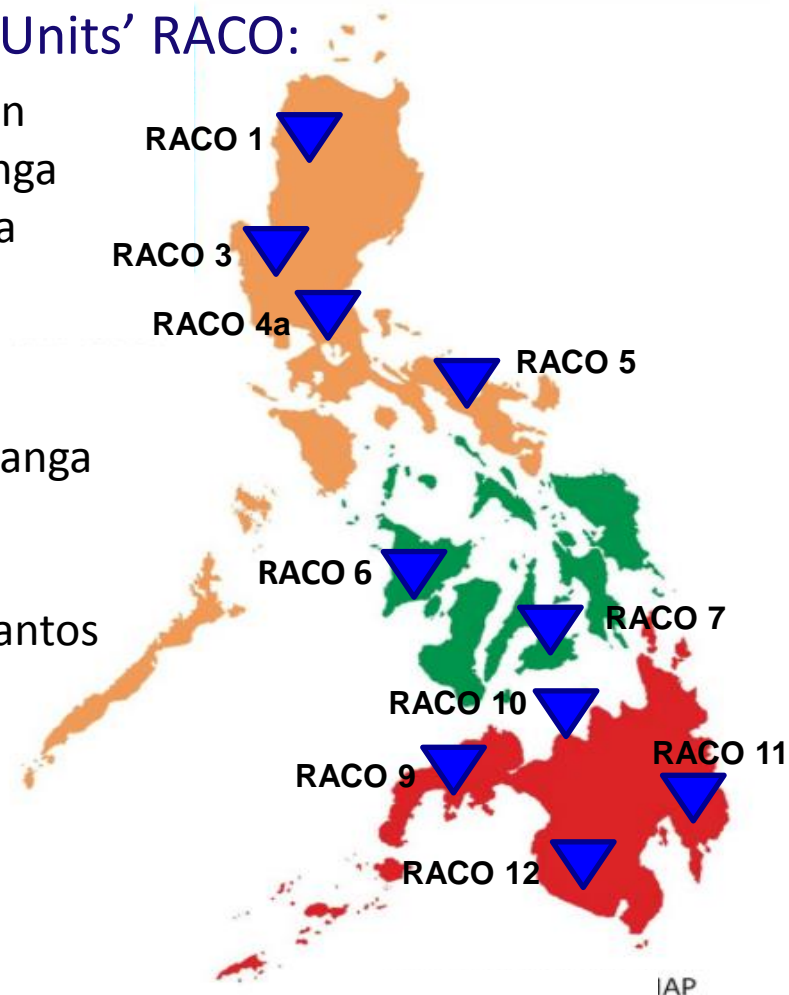
Field Units and Regional Anti-Cybercrime Offices (RACOs)

- PNP ACG Field Units:



- Field Units' RACO:

- Raco1 – La Union
- Raco3 – Pampanga
- Raco4a – Laguna
- Raco5 – Bicol
- Raco6 – Iloilo
- Raco7- Cebu
- Raco9 – Zamboanga
- Raco10 – CDO
- Raco11 - Davao
- Raco12 – Gen Santos



IAP



Cybercrime Statistics and Trends



PNP Anti-Cybercrime Group

CYBERCRIME STATISTICS

NATURE OF CASES	2013	2014	2015	2016	TOTAL
Art. 315 RPC Swindling/Estafa (Online Scam)	42	154	334	511	1,041
Sec. 4 (c) 4 R.A. 10175 (Online Libel)	22	112	311	498	943
Light/Grave Threats (Online Threat)	29	56	106	208	399
Sec. 4 (b) 3 R.A 10175 (Computer Related Identity Theft)	23	61	101	175	360
Hacking	12	41	57	116	226
R.A. 9995 (Anti Photo and Video Voyeurism)	10	43	52	196	301
Unjust Vexation	1	10	33	46	90
Robbery/Extortion (Sextortion)	3	11	30	40	84
R.A. 8484 (Atm/Credit Card Fraud)	1	1	30	31	63
R.A 9775 (Child Pornography)	2	10	12	25	49
R.A. 7610 (Child Abuse)	-	14	8	30	52

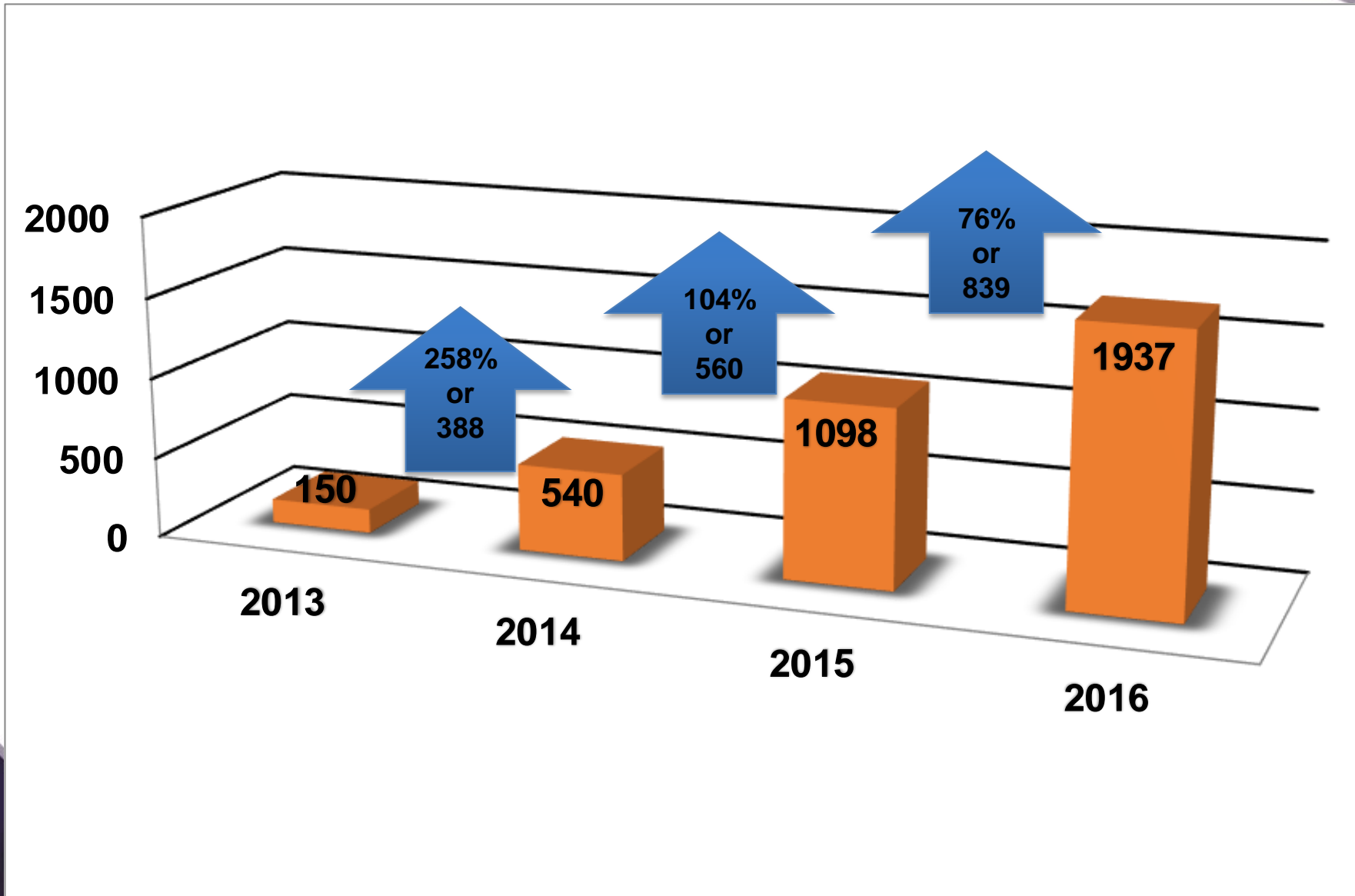


CYBERCRIME STATISTICS

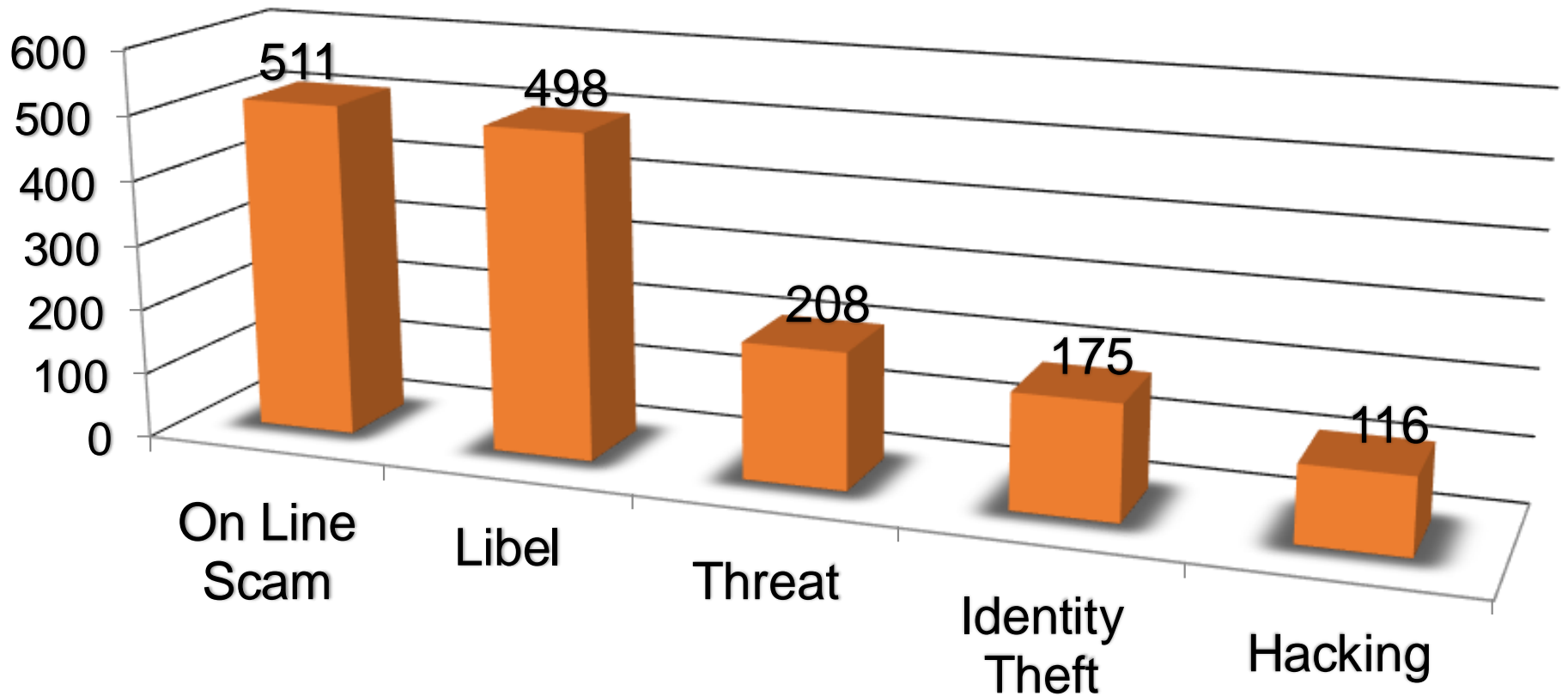
R.A. 9262 (VAWC)	-	5	5	16	26
Sec. 4 (a) 1 R.A. 10175 (illegal access)	-	-	5	26	31
Cyber Bullying	-	2	3	16	8
Sec. 4 (a) 6 (Cyber Squatting)	-	4	2	1	7
E-mail Spoofing	1	6	2	6	15
Phishing	-	-	2	1	3
R.A. 10364 (Anti Trafficking in Persons Act)	3	-	2	5	10
Online Piracy	-	2	1	0	3
Online Illegal Recruitment	-	1	1	0	2
Sec. 4 (a) 3 R.A. 10175 (Data Interference)	-	5	1	3	9
Missing Person	-	2	-	0	2
TOTAL	150	540	1,098	1,937	3,725



CYBERCRIME TREND



2016 MOST PREVAILING CYBERCRIME INCIDENTS



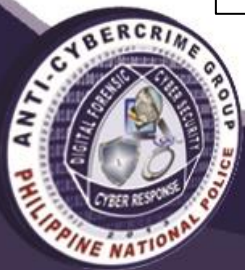
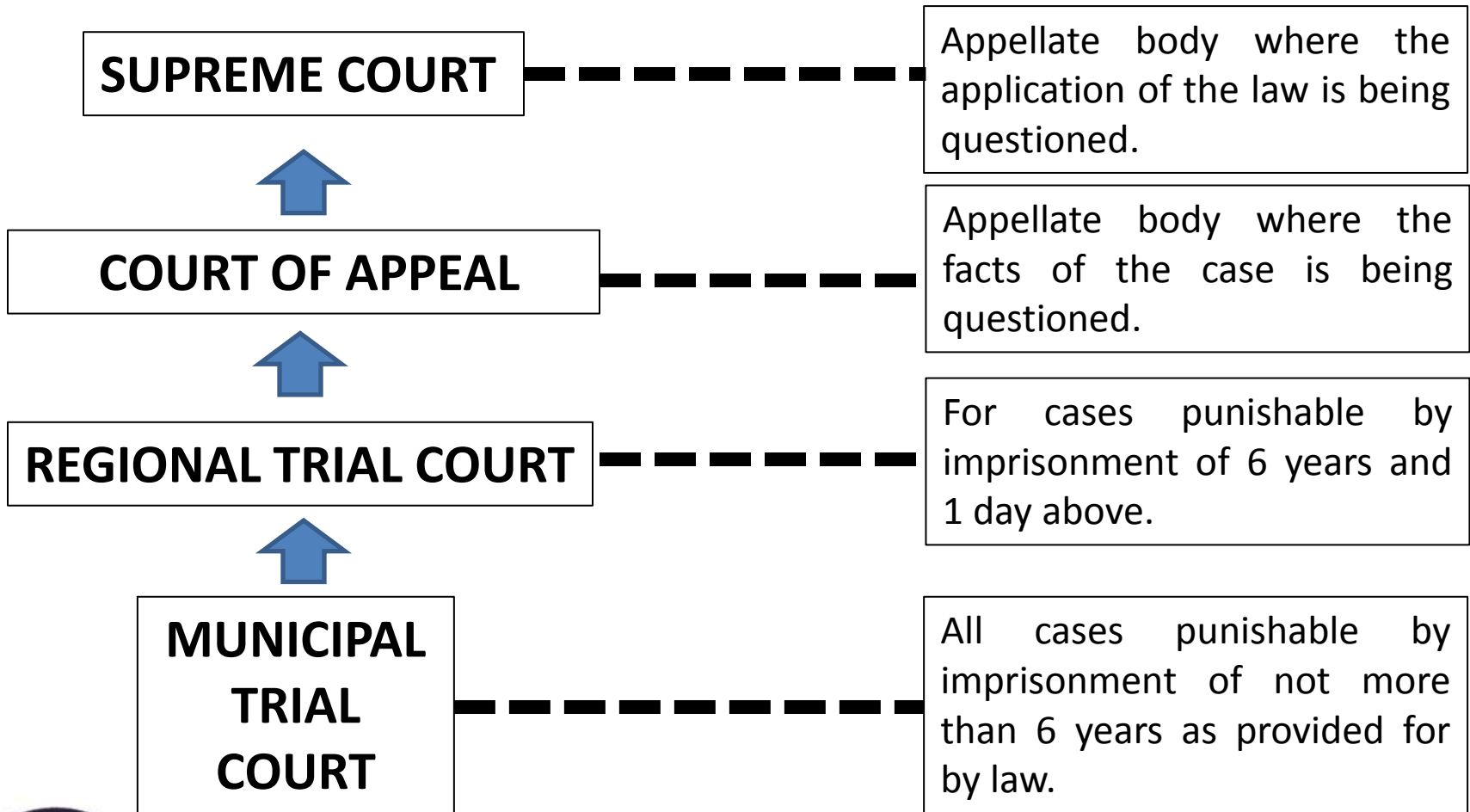


Legal System



PNP Anti-Cybercrime Group

HIERARCHY OF COURTS



Philippine Cybercrime and Related Laws Enacted

- **Cybercrime Prevention Act of 2012**
- Expanded Anti-Trafficking in Persons Act of 2012
- Data Privacy Act of 2012
- Child Pornography Act of 2009
- Anti-Photo and Video Voyeurism Act of 2009
- Electronic Commerce Act of 2000
- Access Devices Regulation Act of 1998





Cooperation with Private Sector



PNP Anti-Cybercrime Group

Cooperation with Private Sector

Memorandum of Understanding between Anti-Cybercrime Group and Microsoft Philippines was signed and is purposely designed to enhance the capabilities of the PNP-ACG in terms of trainings and other related programs.



PNP Anti-Cybercrime Group

Cooperation with Private Sector



PNP Anti-Cybercrime Group

Cooperation with Private Sector

CYBERCRIME SUMMIT 2016



PNP Anti-Cybercrime Group



Cooperation with Private Sector

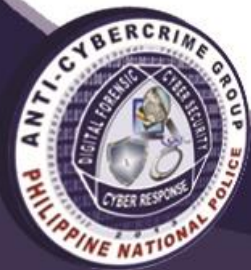
Angelnet Summit 2016. As part of the annual celebration of PNP-ACG Anniversary various groups of professionals, IT Security practitioners and other stakeholders were gathered together to share their respective expertise and learn on the current trends, share experiences and other cyber related information. It also highlighted the roles and responsibilities of the participants in the protection of the well-being of the children and their pledge of commitment in combating online child abuses and is sponsored by Unite for Children (UNICEF) and PSSSLAI.



PNP Anti-Cybercrime Group



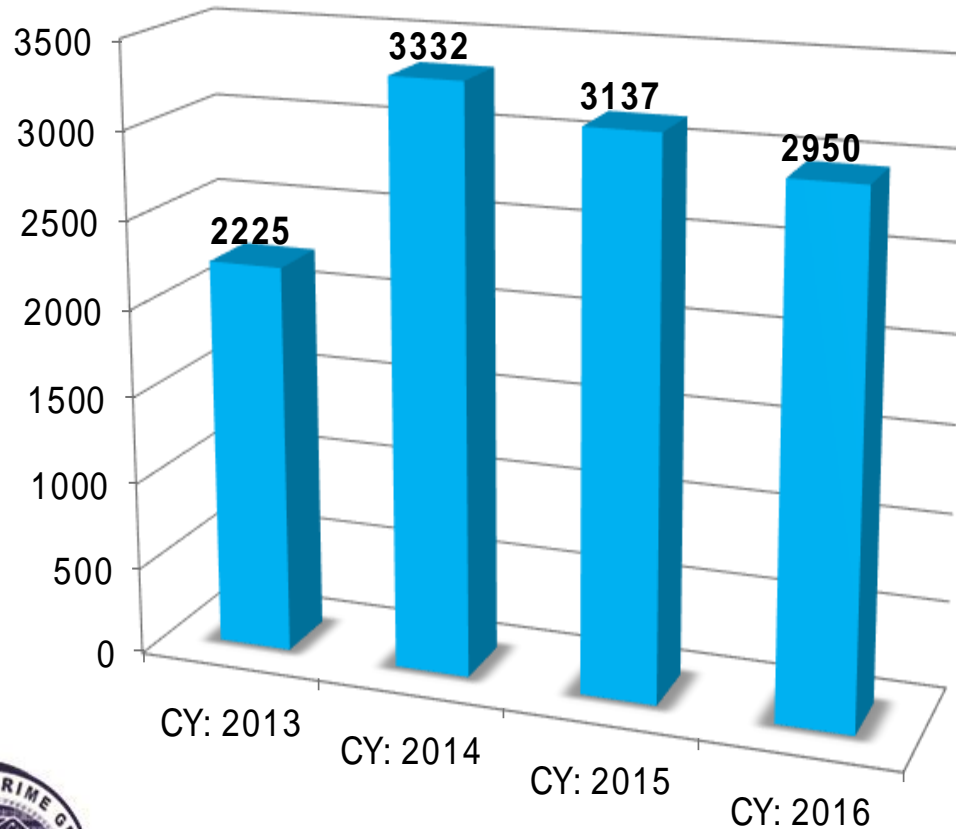
Digital Forensics



PNP Anti-Cybercrime Group

Digital Forensics

Comparative Data on Digital Evidence Subjected to Forensic Examination



There is a glaring increase in the numbers of digital evidence submitted to this Group for examination after 2013. This is due to the numbers of PNP investigative units that relied on forensic examination of digital evidence that could lead to crime solution.



■ Nr of Evidence Examined



Training for Officers



PNP Anti-Cybercrime Group

Standard Mandatory Training for an ACG member:

- Introduction to Cybercrime Investigation
- Identification and Seizure of Digital Evidence
- Introduction to Digital Forensic Investigation
- Proactive Internet Investigation



Trainings & Certifications



- 4 personnel are Certified EnCase Forensic Examiner (EnCE)
- 3 other personnel are undergoing certification process



- 18 personnel are Certified Cellebrite Cellphone Forensic Examiner



- 2 personnel are Certified XRY/XACT Cellphone Forensic Examiner





International Cooperation



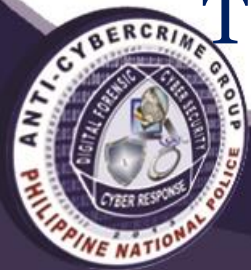
PNP Anti-Cybercrime Group

International Cooperation



INTERPOL

G7 and Interpol 24 / 7 Points of Contact for High Tech Crime Emergencies



PNP Anti-Cybercrime Group



Case Study



PNP Anti-Cybercrime Group

The INTERPOL tagged the Philippines, Morocco and Ivory Coast as the top three countries where “sextortion” rings operate.

Due to this, a massive operation dubbed as **“OPERATION STRIKE BACK”** were launched by the PNP ACG aimed at neutralizing cybersex syndicates in the country particularly those involved in so-called SEXTORTION.



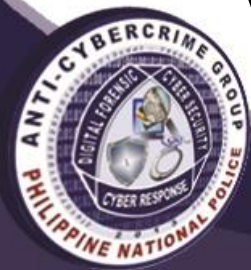
“Operation Strike Back”

“SEXTORTION” means extortion where the extorter obtains nude pictures or videos from his victim, then blackmails them for money to avoid the publication of the nude material.



“Operation Strike Back”

- November 11-13, 2013 - 1st Eurasian Working Group Meeting for Heads of Cybercrime Units in Singapore.
 - Sextortion was traced in the Philippines
 - Suspect/s: Filipinos
 - Victim/s: Foreigners



Operation Strikeback: (Modus Operandi)



Profilers job is to scan and search the internet specially social media site like Facebook, twitter etc. for vulnerable and BIGTIME targets.



Operation Strikeback: (Modus Operandi)



Chatters job is to use **pre recorded video** of beautiful woman and lure the victims to perform sexual acts, and record the video of the victims while performing.



I'll show you mine if you show me yours first, HONEY



Operation Strikeback: (Modus Operandi)



Because the syndicates have the copy of the video of the victims performing sexual act, Blackmailers job is to pressure the victims to send money.



Operation Strikeback: (Modus Operandi)



The Receivers will confirm that the Cyber Sextortion Operation is success, when they get the money from the victims to any Money Transfer Company



“Operation Strike Back”

DECEMBER 2013

Facebook Security eCrime shared information about the ‘Bicol Group’ based in Naga City as being involved in sextortion.

More than 100 suspects were linked to this particular syndicate



PNP Anti-Cybercrime Group

“Operation Strike Back”

Case of Daniel David “Perry” Aiton



FEBRUARY 2014

- Police Scotland officially joined the cybercrime taskforce to combat sextortion, after working with the UK’s National Crime Agency (CEOP command) that led to the identification of a criminal network linked to the death of Scottish teenager Daniel Perry.



PNP Anti-Cybercrime Group

“Operation Strike Back”

JANUARY 2014 – FEBRUARY 2014

- Investigations identified victims of this group in a number of countries / jurisdictions including Hong Kong (China), Singapore, the United Kingdom and the United States.
- Additional potential victims were also identified in Australia, Malaysia, Korea and Philippines.



PNP Anti-Cybercrime Group

“Operation Strike Back”

APRIL 30 – MAY 1, 2014



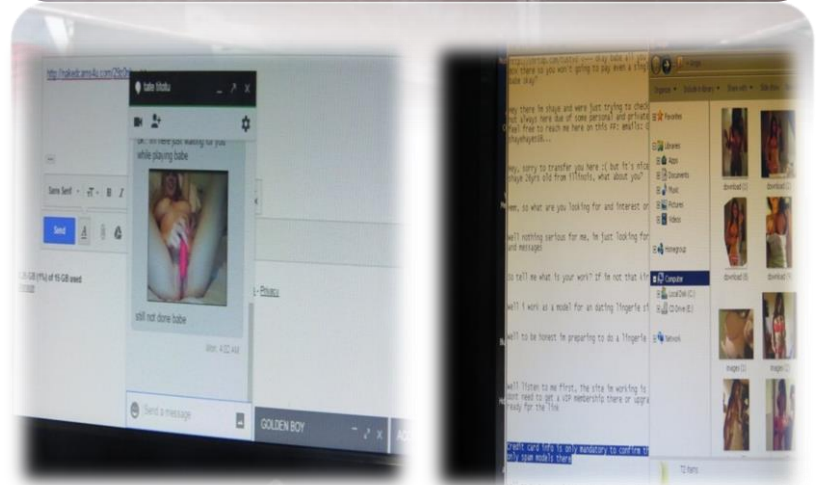
- As a result of the intelligence sharing between the involved countries and the private sector, an operation targeting the organized crime groups were mounted in the Philippines on 30 April and 1 May 2014.
- Raids were conducted at premises in Bicol, Bulacan, Laguna and Taguig City, resulting in the arrest of 58 individuals and the seizure of 250 pieces of electronic equipment.

PNP Anti-Cybercrime Group



“Operation Strike Back”

- Implementation Of Search Warrant at Cabanatuan City last March 1, 2016;
- Seven (7) female and twenty (20) male persons were arrested;
- Violations of Article 201 of the RPC “Immoral doctrines, obscene publications and indecent shows” pursuant to Section 4 (c) 1 of R.A. 10175 was filed.



“Operation Strike Back”

- Implementation of SW in San Jose Del Monte Bulacan last June 23, 2016;
- Arrested 20 persons, 13 of them are male;
- Violations of Article 201 of the RPC “Immoral doctrines, obscene publications and indecent shows” pursuant to Section 4 (c) 1 of R.A. 10175 was filed.



PNP Anti-Cybercrime Group

Police nab 20 in Bulacan on ‘sextortion’ charges

posted June 24, 2016 at 12:01 am by PNA



The Philippine National Police Anti-Cybercrime Group arrested 20 persons for cybercrime charges during an operations in San Jose del Monte City, Bulacan, PNP-ACG director, Senior Superintendent Guillermo Lorenzo T. Eleazar said Thursday.

Eleazar said that before midnight Wednesday the cybercops raided a cybersex den in San Jose del Monte City, Bulacan where they arrested 20 persons, 13 of them males accused of recording the sex act of their victims and threatening to send the video to their target's families if their extortion demand is unheeded.

“Through our Strikeback Operation 2016, we have smashed another local cybersex ring victimizing foreigners and even Filipinos, luring them into webcam chats and blackmailing the victims with the footage showing them in compromising situations,” said Eleazar.

“A compromising situation,” said Eleazar.

and even Filipinos, luring them into webcam chats and blackmailing the victims with the footage showing them

“Through our Strikeback Operation 2016, we have smashed another local cybersex ring victimizing foreigners and even Filipinos, luring them into webcam chats and blackmailing the victims with the footage showing them

IDENTITY THEFT

Suspect/s using fake identification card will be applying for credit cards to banks and other financial institution. With the cooperation of financial institutions, suspects are then subjected for an entrapment operation.

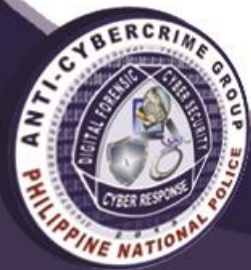


Significant Accomplishments

Identity Theft

- Joseph Nicol Ongwas was arrested in an entrapment operation in Parañaque City last April 29, 2016;
- The suspect presented fake IDs to claim the credit cards delivered to him but bearing the name of his uncle.
- The complaint stemmed from a request from Union Bank of the Philippines regarding the presence of an unknown person misrepresenting their client to gain advantage of their real client's credit cards.

The screenshot shows a news article from INQUIRER.net. The main headline is "Jobless man nabbed for ID theft, attempt to use uncle's credit card". The article is by Julie M. Aurelio, published on May 2nd, 2016. The text of the article describes the arrest of Joseph Nicol Ong, 43, in Parañaque City. He was caught after presenting fake IDs to claim credit cards delivered to him under the name of his uncle. The article also mentions that the Philippine National Police Anti-Cybercrime Group warned the public about identity theft, especially with the hacking and leak of data from the Commission on Elections website. A photo of a hand holding a credit card is visible on the right side of the article.



IDENTITY THEFT

Suspect/s will be capturing pictures of known personalities and create a new Facebook account pretending that as if a new account was created by the legitimate owner of the picture as well as create accounts of the relatives and friends of the victim to be part of the friends list to make it appear as a legitimate account. Thereon will send friend request to possible target and once accepted the friend request on Facebook, suspects will request for financial assistance for either personal or for a foundation.



Significant Accomplishments

Identity Theft

- Myca Acobo Aranda was arrested by during the entrapment operations conducted by ACG last June 7, 2016;
- The suspect created fake Facebook accounts in the name of Pangilinan, Laxa and their four children;
- Using their pictures and other personal data, the suspect used these to communicate with their friends and relatives, asking them to donate money for an “outreach program.”



PNP-ACG vs RAINIER M TAMAYO

Violation of Section 177, in relation to Section 217 of RA 8293 otherwise known as **“Intellectual Property Code of the Philippines”** committed by, through and with the use of Information and Communications Technology



Item seized against the suspect which are used or intended to be used in his illegal activity were the ff:

- One (1) computer set;
- Two (2) routers;
- One (1) modem;
- One (1) external drive;
- One (1) flash drive;
- One (1) IPHONE ;
- One (1) Black Berry;
- One (1) tablet;
- One (1) UPS;
- One (1) head set; and
- One (1) LAN cable.



A case of for the Violation of RA 8293 otherwise known as Intellectual Property Code of the Philippines was filed against RAINIER M TAMAYO and was ordered detained by the DOJ.



PNP Anti-Cybercrime Group



**Thank You
and Good Day!**



CONTACT US:

PNP ACG 24/7 Cyber Operations Center

Contact Numbers:

Hotline: (02) 414-1560

Fax: (02) 414-2199

Email: pnp.ancybercrimegroup@gmail.com