PNP- ACG STRATEGIC THRUST ON CYBERCRIME AND CYBER SECURITY

www.acg.pnp.gov.ph

www.pnpacg.ph

PNP- ACG STRATEGIC THRUST ON CYBERCRIME AND CYBER SECURITY

As the Philippines discover the wonders and benefits that cyberspace has to offer, it becomes increasingly dependent on it. However, with the rising dependence on the internet comes the danger of exposure to rapidly evolving threats and risks. It is therefore pertinent that the Philippine Government develop a logical, intelligible and strategic response to the security challenges that may arise from these ever progressing dangers.

Knowing the dangers of cybercrimes and the security threats pose in our cyberspace, the Philippine National Police (PNP) through the leadership of police Director General Allan La Madrid Purisima Chief, PNP, pushed for the activation of the PNP Anti-Cybercrime Group (ACG) on March 20, 2013 as strategic response to all cyber security challenges. The PNP-ACG has conceptualized and believed that to fight cybercrime and to strengthen cyber security, there must be a synergy among the following components: Competence and Capability building of the Organization and Personnel; Public and Private Partnership; strong International Cooperation; Advocacy and Public Awareness and; the implementation of strong Laws, Policies and Regulations.

Figure 1. Framework of PNP-ACG Strategic Thrust on Cybercrime & Cyber Security.

LAWS, POLICIES AND REGULATIONS

Everyone should feel secure and protected by the law, even in cyberspace. As the Philippines join the world in the transition from manual to digital, laws that safeguard the systems, processes and data needs to be created.

Since 2000, laws have been created in response to cybercrimes and cyber threats to national security. These laws are the RA 9995 or the Anti-Photo and Video Voyeurism Act of 2009, RA 9775 also known as the Anti-Child Pornography Act of 2009, RA 9208 commonly referred to as Anti-Trafficking in Persons Act of 2003 as amended by RA 10364, RA 8792 or the E-Commerce Act of 2000 and the RA 8484 or better known as the Access Device Regulation Act of 1998. But only in 2012 that a law has been signed significant enough to safeguard the Philippine cyberspace as it encompasses all the previously passed laws and more. It is called the Republic Act 10175 or the Cybercrime Prevention Act of 2012. But in response to public outcry, the Supreme Court of the Philippines has issued a temporary restraining order (TRO) suspending its implementation.

National policies and office regulations to prevent cybercrimes and strengthen cyber security must be adhered to at all times to attain success of the program. It is significant to understand that technology is fast evolving, cyber threats will likewise develop and cyber criminals become more creative. Thus, the enactment of laws that address the development of cybercrime is important in order to maintain a safe and secure Philippine cyberspace.

COMPETENCE AND CAPABILITY BUILDING

The Philippine National Police, as of the moment, has a great need of knowledge and comprehension of the current and future cyber situation of the Philippines. The rise in cybercrimes and cyber-attacks in the recent years indicates that criminals have a clear grasp of technology and is using it to their advantage. Knowing and understanding fully well how fast the development of new and dangerous computer programs and viruses and their effects, the PNP will have a clear idea on how to help avoid, and respond to possible cyber threats.

Under this program the PNP Anti-Cybercrime Group is undertaking a range of measures including:

1. COMPETENCE BUILDING

a. Strengthening Research and Analysis

A study of trends in cyber threats and statistics is fundamental in the combat against cybercrimes. Assessing when, knowing where and determining how these threats are carried out is vital.

Although cyber terrorists, criminals and hackers never run out of creative ways to wreak havoc in the worldwide web, an intelligent based analytics may help thwart or avoid them. That is why having the right statistical tools, the necessary research materials and the appropriate skills and knowledge will yield results which are vital parts of competence building.

b. Training and Seminars

To vastly improve and increase the current law enforcement capability of the PNP, continuous attendance and participation to various training / seminar / workshops / conferences both local and international is essential in order to be updated with the recent developments in technology.

The training and development of two to three forensic investigators and incident responders in each of the provincial and regional offices of the PNP is one of the goals of the Anti-cybercrime Group. They are envisioned to undergo local and International trainings on forensics and investigation, incident response, preservation of evidence, data recovery/retrieval and analysis, digital intelligence and other relevant courses to further hone their skills and kept abreast with the current technological advancements.

Prior, The PNP, through the ATCCD-CIDG, underwent ninety (90) trainings and seminars, both local and international since 2003. Thirty one

(31) trainings were conducted by ATCCD – CIDG in various PNP units nationwide.

Currently, the PNP ACG personnel underwent twelve (12) trainings and seminars, both local and international since it was activated. One (1) seminar was conducted by ACG to its personnel regarding Orientation to cybercrime, cyber security and cyber warfare.

2. CAPABILITY BUILDING

a. Establishment of National & Regional Forensic Laboratories

Key to the fight against cybercrimes is the creation of a National Forensic Laboratory. A modern digital forensic laboratory which serves as a processing center as well as a computer crime evidence depot will be established in every Police Regional Offices (PROs). This will be the epicenter linking all satellite forensic laboratories nationwide providing the necessary evidentiary support to law enforcement operations and investigation.

Through the US Diplomatic Security, Anti-Terrorism Assistance Program (ATAP), the PNP-ACG now is in possession of twenty one (21) Digital Forensic Equipment being used in six (6) Digital Forensic Laboratories nationwide capable of conducting computer, mobile and audio/video forensic examinations. The PNP ACG Digital Forensic Laboratories are strategically located at Camp Crame Quezon City, Legaspi City, Cebu City, Davao City, General Santos City and Zamboanga City. The need to establish Digital Forensic Laboratory in the other region is also necessary.

b. Establishment of Cyber Security Incident Response Team

Many corporate businesses and government, including critical digital infrastructure in the Philippines, have not undertaken sufficient measures to address security issues during normal daily operations. CSIRT serves to raise awareness, preparedness and response to pro-actively manage risk regarding

cyber security issues, and coordinates cyber information sharing for secure protection of critical computer system infrastructure and equipment against potential organized cyber-attacks.

c. Establishment of Cyber Terror Response Team

Terrorist are now spawning terror in the internet through the spread of malicious and intentionally harmful ideas and propaganda and strategically attacking computer programs and networks crippling critical infrastructure or financial system thus greatly affecting the economy both local and international. This program aims to create a specialized team trained to monitor and respond to cyber threat and attacks linked to terrorism.

d. Establishment of Online Child Exploitation Protection Center

A program aimed to protect children from internet dangers such as pornography, sexual abuse, cyber bullying, and gambling. It also seeks to raise public awareness on the dangers children face online. The project will use social networking site like Facebook, Twitter and YouTube to teach young children and teenagers basic lessons on how to avoid internet danger in order to detect cybercrimes and protect themselves from sexual offenders and other criminals prowling the Web.

A Special Project called Angel Net was established to address Internet-based concerns and abuses and to promote Internet safety among children with the active support of various stakeholders.

e. Establishment of Cyber Crime Complaint Center (C4)

This program envisions receiving, developing, and referring criminal complaints regarding the rapidly expanding arena of cybercrime. A website will be developed and maintained to give the victims of cybercrime a convenient and easy-to-use reporting mechanism. This will become the focal point for reporting cybercrimes and other cyber enabled criminalities.

f. Continuous Upgrading of Digital Equipment and Forensic Laboratories

Technology continue to develop each day thus, parallel to competence building is to continuous upgrade of organization's equipment, both software and hardware, in order to cope and keep pace with the progress of technology.

PUBLIC AND PRIVATE PARTNERSHIP

The dynamic participation of both the public and private sector is important in the never ending fight against cyber criminality.

The private sector's active support is indispensable. They have the resources to help in curbing cybercrimes. They will be best utilized in cybercrime prevention through information dissemination, especially in educating the people on the ill-effects cybercrimes has on the country's economic growth. Significant private companies like Telephone Companies (TELCO), Internet Service Providers (ISPs), IT schools, ICT companies and vendors and even financial institutions may also be tapped to share their expertise on system management, incident response and security matters.

The public sector or the government on the other hand plays a major part in the actual cybercrime suppression. With strong inter-agency cooperation, appropriate responses may be coordinated quickly. The Philippine National Police, the National Bureau of Investigation, the Department of Justice and other similar government agencies may pool their resources to intensify the effort to fight cybercrime and streamline judiciary processes.

Each sector has a role to play and everyone must contribute their part in this worldwide problem. If all sectors commit to this shared responsibility and when there is great partnership built on a passionate desire to alleviate cybercrimes, success is almost always assured.

In this program, the Anti-Cybercrime Group will be embarking on a range of measures which includes the following:

1. ACG aims to strengthen partnerships with the private sector which involves information exchange and sharing of knowledge pertinent to cyber threats, mitigation and disaster recovery. (Example: PHCERT, CIOF, etc)

2. Constant communication and cooperation with Telephone Companies and Internet Service Providers (ISPs) to increase awareness on evolving cyber threats, risk assessment and mitigation and strategies to be applied in case of cyber-attacks.

3. Collaboration with telecommunication, banking and finance industries, and other critical infrastructures is likewise envisioned. These involved high risk sectors prone to cyber terror strikes because successful attack on one of these will have adverse effects on the Philippine economy.

4. Through partnerships with foreign governments and educational institutions, local and abroad, the ACG plans to send qualified representatives to undergo relevant and up to date trainings and seminars.

5. The establishment of a cyber security informants and volunteers coming from the private and public sectors who will serve as force multipliers of the ACG is in the wraps.

INTERNATIONAL COOPERATION

Forging alliances through coordination, cooperation and collaboration with different foreign law enforcement and international organizations is one of the ACG's priorities. This will enable the sharing of best practices, review evolving cyber issues, identify problem areas, initiate reforms when needed and aid in the ACG's competence building program.

Under this program, the Philippine National Police through the Anti-Cybercrime Group is pursuing an active approach to international participation on the further development of cyber security through the following:

1. ACG, through channel, plans to strengthen partnerships against cybercrime with ally nations by signing multilateral agreements concerning cybercrime and security.

2. To develop and recommend, through channel, an international engagement strategy to clearly define and articulate Philippine's national interests and priorities in relation to cybercrime and cyber security.

3. Fostering an international cooperation for a strategic, coordinated global response in battling cybercrimes, cyber security threats and risks is part of the ACG's long term goal.

Currently, the PNP have good partnership on the following international agencies in investigating cybercrimes:

1. U.S. – High Technology Crime Consortium, International – High Technology Crime Investigation Associations
2. U.S – National White Collar Crime Center (NW3C)
3. Asia – Pacific Computer Emergency Response Team (AP – CERT)
4. Cyber Crime Technology Information Network system (CTINS)
5. Interpol Asia – South Pacific Working Party on Information Technology Crimes
6. INTERPOL
7. Japanese National Police Agency / Japan International Cooperation Agency (JICA)
8. Korean International Cooperation Agency (KOICA) / Korean National Police Agency
9. AUSTRALLIAN FEDERAL POLICE (AFP)
10. US – Federal Bureau of Investigation
11. US – Immigration and Custom Enforcement
12. US – Homeland Security

13. US Department of State, ATAP
14. National Cyber Forensic and Training Alliance (NCFTA)

ADVOCACY AND PUBLIC AWARENESS

This program will focus on implementing a cyber security advocacy program that will rally the general public to protect and preserve the Philippine cyberspace. This program will specifically focus on Computer Ethics, Computer and network Security and Incidence Response.

The Philippine National Police (PNP) Through The PNP Anti Cybercrime Group will be the frontrunner in raising awareness of cyber security at all levels of government especially the PNP, and has the following goals to help in raising public awareness to the Philippine cyberspace users:

1. The creation of a website designed to inform home and leisure users, small business owners and those who have limited knowledge and skills about cybercrime and cyber security, the dangers of unprotected internet access and possible ways to avoid known threats. The website will contain alerts and advisories and will be written in plain language to appeal to even the most unaccustomed to using the internet. It will also include information on new cyber security risks and give suggestions on how to address them.

2. The Publication of Cyber Security Bulletins will ensure the Internet community has access to information on cyber security threats, vulnerabilities in their systems and information on how to better protect their information technology environment.
3. Cyber security lectures and seminars for primary and secondary schools should be conducted. This promotes cyber security awareness, culminating in an annual Cyber Security Awareness Week, conducted in partnership with business, consumer groups and community organizations.

Ultimately, the public needs to have a well-defined idea of the dangers that cyber space poses. They all have to be educated on both the positive and negative effects of using the internet and the ill-effects of cybercrimes not only in their individual lives but also to other internet users, to the whole internet community and to the country. Having a clear picture of the draw backs of cybercrimes to the society will greatly lessen the possibility of unintentional cyber strikes like the infamous “I Love You Virus” which caused a major fiasco worldwide.

The internet community is a great partner in the battle against cyber criminality because they will be able to provide suggestions on how to improve cyber security on their levels. They will be able to give an insight on cyber threat trends and may be able to assist by giving relevant information pertaining to the sources of cyber-attacks. Their perception of existing laws and policies which relate to their use of the web will prove valuable in making reforms and possible creation of new laws and guidelines in the future.

Everyone deserves to have a secure and reliable internet access. Therefore, everyone should take part in fighting those who threaten to take away this right. The public should be aware because awareness is already half the battle.


Implementation of the following laws
• RA 10175 Cybercrime Prevention Act
• RA 9995 Photo & Video Voyeurism Act
• RA 9725 Anti-Child Pornography Act
• RA 9208 Anti-Trafficking in Persons Act
• RA 8792 E-Commerce Act
• RA 8484 Access Device Regulation Act
• Act as Resource person and assist In the creation/amendment of future laws on cybercrime and cyber security.
Laws, Policies Regulations
Advocacy and Public Awareness
PNP-ACG Strategic Thrust on Cybercrime and Cyber Security
Competence and Capability Building
• Creation of a website
• Publication of Cyber Security Bulletins
• Cyber security lectures and seminars in government Institution, Private Companies and home users.
Trainings and establishment of the following:
• Research & Analysis
• Local and International Training & Seminars
• Digital Forensic Laboratories
• Cyber Terror Response Center
• Child Exploitation & Cyber Protection Center
• Cybercrime Complaint Center (C4)
• Continuous Upgrading of technological Equipment
International Cooperation
Public/Private Partnership
Partnership with the following organizations:
• U.S. – High Technology Crime Consortium, International – High Technology Crime Investigation Associations
• U.S – National White Collar Crime Center (NW3C)
• Asia – Pacific Computer Emergency Response Team (AP – CERT)
• Cyber Crime Technology Information Network system (CTINS)
• Interpol Asia – South Pacific Working Party on Information Technology Crimes
• INTERPOL
• Japan National Police Agency
• JICA-Japan International Cooperation Agency
• KOICA- Korean International Cooperation Agency
• Korean National Police Agency
• Australian Federal Police (AFP)
• US LAW Enforcement Agencies(FBI,ICE, HS, ETC)
• US Department of State, ATAP
• NCFTA- National Cyber Forensic and Training Alliance
▪ Coordination with Telcos & ISPs
▪ Collaboration with banking/finance industries and operators of critical infrastructures
▪ Coordination and collaboration with the judges and prosecutors.
▪ Establishment of Cyber Security Informants (CSI)
▪ Coordination & Collaboration with PHCERT.CIOF, etc)
▪ Coordination and collaboration with other government agencies
▪ Partnership with different schools for research and development.

For more information, visit the

PNP ACG websites:

www.acg.pnp.gov.ph

www.pnpacg.ph

CONTACT US:

PNP ACG Cyber Operations Center

Contact Numbers:

Hotline: (02) 414-1550

Fax: (02) 414-2199

Email: pnp.anticybercrimegroup@gmail.com