"Cybersecurity and Cybercrime: Philippine Perspective"
By: Geronimo L. Sy, Assistant Secretary,
Department of Justice, Republic of the Philippines

This paper outlines the cybersecurity landscape in the Philippines. It shall present a framework analysis and highlight the country's most significant challenges and threats. This paper shall also explore local developments and discuss its possible implications in the near term.

Framework Analysis

Cybersecurity and cybercrime are interrelated but may be distinguished in the context of law. Cybersecurity relates to the assurance of confidentiality, integrity, and availability of computer data and information and communications system. On the other hand, cybercrime is a species of penal law that punishes crimes committed with the use of computer systems or wherein the systems itself are the target. The fact that cybercrime is technology-related does not take it out of the operation of criminal law and procedure.

There is a classic tension between state protection of itself and encroachment on private citizen's rights, which is a whole species of civil liberties. The bigger the rights, the less power there is for the state to act. The smaller the rights, the more power there is for the state to act. In relation to cybersecurity and cybercrime, the more you have of cybersecurity shall mean the less you have of cybercrime, and vice versa.

In pre-World War I, there was a worldwide development of law codification programs. It was in 1932 that the Revised Penal Code\(^1\) was enacted, which codifies the punishable crimes in the Philippines. Subsequently, a new method of law-making developed, particularly the crafting of special penal laws to punish specific acts in response to emerging trends. The emergence of technology-driven laws came after the rise of internet technology.

Special laws enacted that are technology-related includes the following: (1) the Special Protection of Children against Abuse, Exploitation and Discrimination Act\(^2\), (2) the Access Devices Regulation Act of 1998\(^3\), (3) the Electronic Commerce Act of 2000\(^4\), (4) the Anti-Trafficking in Persons Act of 2003\(^5\), (5) the Anti-Violence against Women and Children Act of 2004\(^6\).

---

1. Act No. 3815, the Revised Penal Code of the Philippines (1932).
the Anti-Photo and Video Voyeurism Act of 2009,\(^7\) (7) the Anti-Child Pornography Act of 2009,\(^8\) (8) the Data Privacy Act of 2012,\(^9\) and finally, (9) the Cybercrime Prevention Act of 2012.\(^{10}\)

The Data Privacy Act and the Cybercrime Prevention Act came after the Philippine National Security Policy (2011-2016),\(^{11}\) wherein cyberattacks were identified as a security issue as it may lead to a paralysis of communication infrastructure, international financial systems, critical government services and defense/military command and control systems.

Republic Act No. 10173 or the “Data Privacy Act of 2012” was enacted to protect individual personal information in information and communications (ICT) systems in the government and the private sector. It created the National Privacy Commission, which shall administer and implement the provisions of the law, and monitor and ensure compliance of the country with international standards set for data protection.

On 12 September 2012, Republic Act No. 10175 or the “Cybercrime Prevention Act of 2012” (CPA) was approved, which is the comprehensive legislation on cybercrimes. Notably, it defined “cybersecurity” as the “application of security measures to ensure confidentiality, integrity, and availability of data. It is a collection of tools, policies, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization, as well as a user’s assets.”\(^{12}\) This strays from the usual practice of defining cybersecurity in executive pronouncements only, as the definition is now embedded in the law.

The Office of Cybercrime (OOC) under the Department was created by virtue of the CPA, and was designated as the central authority in all matters related to international mutual assistance and extradition. To enhance enforcement and implementation, the CPA also provided for the organization of a cybercrime unit or center manned by special investigators in the Philippine National Police (PNP) and the National Bureau of Investigation (NBI).

The CPA also created the Cybercrime Investigation and Coordinating Center (CICC), which is an inter-agency body under the administrative supervision of the Office of the President that coordinates policies among concerned agencies. It is also given the power to formulate and enforce the national cybersecurity plan and shall extend immediate assistance of real time

\(^7\) R.A. 9995 (2009).
\(^8\) R.A. 9775 (2009).
\(^12\) Section 3 (k) of Republic Act No. 10175 or the "Cybercrime Prevention Act of 2012" (CPA).
commission of cybercrime offenses through a computer emergency response team (CERT).\textsuperscript{13}

In Disini vs. Secretary of Justice,\textsuperscript{14} the Supreme Court upheld the validity of the CICC, ratiocinating that the law gave sufficient standards for the CICC to follow when it provided a definition of "cybersecurity". The case also upheld the constitutionality of the law, thus paving the way for further developments.

Three core cybercrimes exist under the law, namely: (1) the offenses against the confidentiality, integrity and availability of computer data and systems; (2) computer-related offenses; and (3) content-related offenses. The penalties are increased\textsuperscript{15} in case the first type is committed against critical infrastructures.\textsuperscript{16}

The first class of core cybercrimes may be said to apply to cybersecurity and data privacy. The second class may also apply, particularly the act of identity theft as its subject is personal information.

\textbf{Challenges and Threats}

The problem of cybersecurity lies on the enforcement, particularly on what agencies should lead the effort and up to what extent should it be led. To illustrate, the Data Privacy Act created the National Privacy Commission but there is a gap on implementation as the office has not yet been constituted.

A basic challenge in implementing the law is the lack of lawyers who know technology, and lack of technical staff who know the law. Cybersecurity and cybercrimes, however, require the combination of both disciplines.

Another significant challenge is the raising of the issue on the freedom of speech and expression with respect to cybersecurity. There are no issues on cybercrimes involving online child abuse, online fraud, bullying, or other social norms.

Furthermore, there is no way to find out exactly what we’re up against. At best, we can only look at anecdotal figures or major estimates. It may also be said that there is no feedback mechanism to determine whether a cybersecurity/data privacy plan is working and it can only be measured by its failure.

\textsuperscript{13} Section 24 and 26 of the CPA.
\textsuperscript{14} G.R. No. 203335, 11 February 2014, Disini vs. Secretary of Justice.
\textsuperscript{15} Section 8 of the CPA.
\textsuperscript{16} Section 3 (j) of the CPA defines "critical infrastructures" as computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data so vital to the country that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters.
Developments

A lot may be said on the developments of cybersecurity/data privacy in the Philippines. In particular, the implementing rules and regulations of the Cybercrime Law was launched on 12 August 2015. It is anticipated that the Philippines will soon ratify the Convention on Cybercrime.

The Philippines was invited to accede to the Budapest Convention without objection in June of 2011 and is annually invited to join the Octopus Conferences. The Budapest Convention or the International Convention on Cybercrime provides countries an updated tool suited for the 21st century.

To show that cybercrimes and cybersecurity are taken seriously, a National Prosecution Task Force on Cybercrime was constituted, through Department Order No. 746 dated 08 September 2014, to handle cybercrime cases. Department Order No. 814 dated 14 October 2014 established the Cybercrime Desk, which handles Mutual Legal Assistance and Extradition requests. The Cybercrime Desk is the contact point in the Department on international legal cooperation involving cybercrime and related matters.

The Sub-Committee on Cybercrime (SOCY) was also constituted by the National Law Enforcement Coordinating Committee (NALECC),17 to which the DOJ Office of Cybercrime (OOC) was designated as Chair.

SOCY was established as one of the functional sub-committees of NALECC. The functions of the sub-committee are as follows: (1) Provide assistance in the anti-cybercrime campaign to other government agencies, private sector and non-government organizations, such as facilitating information sharing and arrest of personalities involved in cybercrime; (2) Strengthen inter-agency coordination regarding anti-cybercrime and other cybercrime related activities; and (3) Provide a venue of discussion and recommendation on various issues and concerns affecting the anti-cybercrime campaign of the Sub-Committee member agency.

The Department also constituted the DOJ Cyber Security Incident Response Team (DOJ-CSIRT), through Department Order No. 526 dated 19 May 2015, which is a multi-disciplinary group covering relevant offices under the Department and is headed by the DOJ Chief Information Officer (CIO).

The DOJ-CSIRT has the following duties and responsibilities: (1) Respond and extend immediate assistance to the concerned agency on cybersecurity incidents; (2) Issue and promulgate guidelines, advisories, and procedures in all matters related to cybersecurity, in accordance to the national cybersecurity plan; (3) Conduct cybersecurity trainings and

17 NALECC was established pursuant to Executive Order No. 829, as amended by E.O. No. 41 dated 9 December 1992, to serve as the venue for the coordination of all enforcement activities of various government law enforcement agencies.
awareness; and (4) Ensure proper coordination among DOJ constituent and attached agencies and other relevant sectors in the preparation of appropriate and effective measures to strengthen the cybersecurity capabilities of the Department against cyber threats.

The National Telecommunications Commission (NTC) also recently released a memorandum circular, which provides the guidelines on blocking/filtering technologies required to be installed by Internet Service Providers in their systems. There is also an envisioned designation of cybercrime courts, which shall focus on cybercrimes.

Lastly, the Philippines will soon experience the full implementation of the National Justice Information System (NJIS) – a project that interconnects and integrates the respective databases and information systems of all criminal justice agencies into the Single Carpeta System.