The Role of Ideas that shape the Institutional Change in Cybersecurity:

Economic barriers of cyber-attacks.

by

RAQUEL MARASIGAN

A Conference Paper

8th Student GRIPS STUDENT CONFERENCE

Held last September 3, 2019

National Graduate Institute for Policy Studies

Roppongi, Tokyo Japan

Submitted to:

Professor David Jack Farber

Distinguished Professor Co-Director of Cyber

Civilization Research Center Global Research Institute (KGRI)

Professor Tobias Burgers

Project Assistant Professors

Cyber Civilization Research Center Global Research Institute (KGRI)

Table of Contents

Introduction

Institutional change in cybersecurity defines possibilities actions orders cyber shapes agendas that provide policy outcomes. The development of cyber security, a topic of national interest. However despite the threat of online fraud and scams, the Cybercrime Prevention Act of 2012 itself remains abstract among many digital users.

There are no Filipino words for "cybersecurity" or "cyberspace". We have little understanding of how secure online transactions are and do not know how to deal with our loss or personal space in the digital world. Seven years ago, the Philippines and Asian countries gathered to discussed the protection of personal information and infrastructure in cyberspace. The need for cyber security aims to preserve confidentiality, integrity, availability of information in cyberspace, and is continuous developing at both the public and private sector.

Fear, uncertainty, and doubt surround reports of cyber-attacks in the Philippines how can the inter-government agency relationship and private sector face the economic challenges of cybersecurity in spite of latest report of increasing cyberattacks in Philippines cyber? Cybersecurity was seen as strategies and process to eliminate risk of cyber-attacks, What do historical reports of DOJ-OCC year 2014-2017 suggest, in order to improve our cybersecurity capability given that are remaining three years to complete the National Security Plan 2022?

Incidents in 2000 and 2006 that prompted discussion about cybersecurity in the Philippines. The first was "I Love You" virus in September 2005. The in 2006, a 22 year old former call center agent broke into the computer system of Philippine's credit card company a accessed their database, which was maintained by a sister firm in the United States. using an internal IP address, he purchases goods online using credit cards. He was sentenced by Quezon City Metropolitan Court to a minimum of one to two year in jail and was fined Php 100,000 in concordance with E-Commerce law.

Technology evolves, cybercriminals becomes sophisticated regulators need to cope with increasing threats and malicious acts in cyberspace. After six years, the Cybercrime Prevention Act (CPA) of 2012 defines the following as cybercrimes, illegal access to data that breachers the confidentiality, integrity, and availability of computer data systems and computer related offenses such as related to forgery, fraud, identity theft and content-related offenses. Table 1 shows an increase in cybercrimes, and government claimed that cybersecurity is a priority in the National Cyber Security Plan 2022 protecting government and private critical infrastructure, supply chain and consumers.

Table 1: Cybercrime Report by Department of Justice - Office of Cybercrime

Category	Cyber behavior	**2014**	**2015**	**2016**	**Total**
Cyber crimes	Hacking	103	175	314	**592**
	Cyber squatting	4	2	1	**7**
	Data Interference	5	1		**6**

In this study, emphasis was places on role of ideas in implementing the cybersecurity policy particularly capacity building and cooperation. These ideas provide insight on identifying the economic challenges of mitigating cyber-attacks. According to Douglas North, “Institutions are the structures that humans impose on human interaction and therefore define the incentives that, together with other constraints (budget, technology, etc), determine the choices that individuals make that shape the performance of societies and economies over time”(North 1999 pages 1-2). In his view this model, regulates society, particularly inter-agency relationships in capacity building.

The Department of Justice Office of Cybercrime thru Cybercrime Prevention Act of 2012 appointed the National Bureau of Investigation and Philippines National Police as enforcement agency to regulates cybercrimes related to computer data, while the Cybercrime Investigation and Coordinating Center , inter-agency body that coordinate policy and enforced the National Cybersecurity Plan. The clout, Department of Justice Office of Cybercrime on the hook for international mutual assistance and extradition. The Supreme Court governs the application and administration of cyber-crime related court warrants as well orders related to preservation, discourse, interception, search, seizure or examination, custody and destruction of computer data . This was considered to strengthens the relationship with between public and private industry, and identify the economic challenges of mitigating cyber-attacks.

Internet defining as human rights access, concerns arise of government intervention with this consumers are willing to invest in securing their online devices for internet shopping (tangible goods). Resource are limited by constraints (time, money and skills) this fear, doubt and uncertainty continue to increase. Some studies have investigated the economic challenges of cybersecurity and theories in deterrence and dissuasion have been proposed (Joseph Nye, page 44).

In this paper, we explore the activities of the Philippine Cybersecurity Prevention Act 2012 over the last two years of implementation. First, we outline that endogenous institutional change was the reason behind the agents made decision-making in competing situations. Outcomes are based on the actions of the other actors, yet we will focus on coordination using the repeated game-theory, wherein players often failed to produce efficient outcomes. Second, we examined the ideas of underlying the Global Cybersecurity Index Report 2018. Capacity Building and Cooperation reflected led to inter-agency coordination information sharing, decreased misaligned incentives to protect the digital society.

We performed the qualitative method analyses in this study., investigating cyber-attacks report from 2017 and 2018 in Philippines was challenging because considerable uncertainty surrounds this field. Interpreting the conceptions of agents and organization and their attempts to create efficient policy outcomes motivated us to use the hermeneutics approach, which interprets meaning from context, pattern, and behavior.

The study has potential limitations; the results were descriptive inquiries into institutional changes of the Cybercrime Prevention Act 2012, so are subject to biases. However, we provided documentary evidence from the department, agencies and organization both the public and private sector to allow causal inference.[1]

Second we evaluated and use the online content reports from private firms since the 2018 impediment inter-agency cybersecurity report from DOJ-Office of Cybercrime. Further quantitative analysis using predictive mode of cyber attacks and monitoring the capacity building between agencies is needed for future research. In the same way, the idea of institutional change evaluates the development of inter-agency

[1] Marc Bloch the Historian's Crafts, 1953 p.129

capability building and cooperation in economic perspective, where both are contributor in economic barriers that cost cyber-attacks.

Literature review

Twenty-five years ago, internet was not available in the Philippines. On March 29, 1994, at precisely 1:15 am (PH time) the router (Cisco 7000) that connected the Philippines to the internet was switched on. [2] Between 2012 and 2018, the Philippines' Cybersecurity Plan 2022 continue to adopt to the changing technologies and strategies of hackers. To protect critical information and private consumers, the Cybercrime Prevention Act of 2012 was adjudicated as the Republic Act No. 10175 until it was finally implemented on February 18, 2014.

A cyber-attacks is any unlawful act to manipulate the target systems, infrastructure, or computer networks, of a person's digital device. This usually involves, a person or process with malicious intent attemptings to access data withour authorization. In reference above institutional change, Cybercrime offenses in the cybercrime prevention act, 2012 include cybersquatting, cybersex, child pornography, identity theft, illegal access to data, and libel. Cybercrime has increase every year. The black hat hacker's motivation is to get money, while hactivism looks to obliterate the data systems of business and government firms.

In addition, the substantial disparity lies from 2016-2017 Philippines Cybercrime Report[3], implementation of formal rules in cybersecurity within the inter-agency was challenge due to absence of governing issuance of cyber warrants.

[2] https://ph.news.yahoo.com/timeline-philippine-internet-20th-anniversary-225454753.html
[3] https://doj.gov.ph//files/OOC/ooc_report_corrected.pdf}.

Most security studies have investigated the five domains of military operation: land,sea,air and space and newest domain in warfare the cyberspace. The effect of fifth domain can as force multiplier with other domain will not be possible without digital equipment. We observed that little is understood about cyber-attacks from an concept of economics. Where cyberspace is market system where network of buyers and other actors are private-public sector that come to trade which is to use the internet service. The participants in the market systems are consumers who drive economic activity in should be using secure internet access.

The theoretical framework of repeated game-theory postulates that same stage of a game is repeated in each period. It captures the way people view their environment and make decisions(Greif and Latin), and the role of ideas or the importance of cultural variables to institutions(Peter Hall,1998). Based on this theoretical framework economic constructs or variables, institutional change, misaligned incentives and information asymmetries have been generated as technology advance.

The research paper is part of the growing literature on the economics of cybersecurity in the Philippines, as behavior of cybercriminals to continue increase cyber threats are growing, so understanding the underlying economic challenges is important to eliminate fear, uncertainty and doubt of participants in market system.

Ideas matter, some scholars in cybersecurity think they can anticipate the outcome of action cyber attacks or believe that they can act rationally in their organization. The variables relate to causal factors regarding these ideas has been investigated(Goldstein and Keohane 1994: 26027) have described the basic heuristic behind the approach They argued that ideas should be imported into analysis only after the interest-based applications for the outcomes have proven inadequate Hass (1992) and Siknik(1991) have argued that economic policies' chosen by the government or the strategies chosen by firms are strongly influenced by the ideas on the appropriate policy or best practices that are dominant within the relevant processional community[4].

Inter-agency task force, Harmonization of National Government Performance Monitoring, Information and Reporting Systems, has been established according to the Malacanang Administrative Order 25 2011, tasked to monitoring and evaluating the performance of government agencies such Department of Information and Communication Technology non-compliance on Good Governance Conditions while Cybercrime Investigation and Coordination Center (CICC) newly establish attached agency non-compliant on Transparency Seal and Citizens Charter these departments are both under the Office of the President [5].

Institutions have changed since the republic Act 8792 or the Electronic Commerce (E-Commerse) Act of 2000 was amended to the Cybercrime Prevention Act 2012. For the past 12 years the web-based to cyberspace has been forefront of technology innovations. Moreover, 2010 and 2017 research into the economics of cyber security increased significantly. Moore argued that very few scholars have explained how the economics of cybersecurity affect the development of national security. Other might argue that persistent cyber-attacks are economical; certainly, private-public cooperation, incentives and successful market will substantially improve cyber security capability.

Conversely, Wirth suggested that cybersecurity needs more than just technical elements. Instead, it should include leadership, as well as societal economic and socio-political elements[6]. The idea is not to just spend excessive money on cybersecurity, slightly decreasing transaction cost. Although the empirical results seem to mixed from an economic perspective, evidence cyber-attacks after Cybersecurity Prevention Act 2012 was enforces suggest that particular challenges needs to be addressed.

Corresponding with, Mr. Domingo had claims that National Cybersecurity Plan 2022 was the government's priority, and that – cybersecurity needs to have the necessary computer network operations to achieve its goal. Technical capabilities allow upgrades of computer infrastructure in law enforcement

[4] The Role of Interest, Institutions and Ideas Peter Hall 1983 pp-184-185
[5] https://www.dap.edu.ph/rbpms/agency/cybercrime-investigation-and-coordination-center/
[6] The Economics of Cybersecurity [Commentary] 2017 p 52 by Axel Wirth

agencies and in military forces[7]. However, the governments have not made it clear how they plan to support the three year systems upgrade. There is asymmetry in the information held by private firms and the data they share with the government.

Greif and Latin integrated game-theory and complementary perspective into endogenous institutional change. This requires a more dynamic approach than presently offered by self-enforcing institutions[8]. Game-theory usually assumes that players have a complete model and shared priority. Each player has complete information about the details of the situation, including the actors' preferences[9]. Unfortunately, when such information is missing the player makes the wrong decisions regarding the unknown parameters. In context of market, other actors such cybercriminals take advantage of this vulnerability in system, rein forcers inadequate cybersecurity tools halt to have date needed to predict cyber-attacks while private firms continues to control internet are elements of unknown parameters in capabilities.

As with cyber-attacks, scholars have context definition of everyone should feel secure in cyberspace. For instance, the ever-changing digital landscape, it is essential to keep pace with the trends in cyber-attacks. These constantly change according to evolving targets, impact, and techniques. The data from Accenture Cybercrime Report 2019 cybercriminals are now targeting vulnerable users through phishing and malicious insiders [10].

Akerlof argued about information asymmetry in his research paper "The Market of Lemons", he use lemons as second hand cars, in cybersecurity context NBI, PNP and CICC should have credible and ethical information. Empirical research from misaligned incentives work against cybersecurity, focus on governance, the processes, rules, and structure companies use to manage, make decisions on resources and technology, and compete— because these processes will usually be slower and less nimble than the market forces that

[7] SRI The Strategic Importance of National Cybersecurity Plan 2022 by Francis Domingo June 5, 2017
[8] A Theory of Endogenous Institutional Change Vol 98 No 4 November 2004 American Political Science Avner Greif and David D. Laitin 2004 p 2
[9] AVNER GREIF and DAVID D. LAITIN, A Theory of Endogenous Institutional Change, Vol 98. No 4, November 20019 p.637

[10] Accenture 2019 Cost of Cybercrime: Unlocking the value of improving cybersecurity protection

drive attackers. Align incentives -where freelance participants in the market must get a performance reward, align the incentives from leadership to technical experts.[11]

The result of this study contributes to qualitative analysis economics of cyber security in Philippine context, results of the research found that ignoring the cooperation, misaligned incentives and information asymmetry exposed the organization cyber threats.

Methods and Qualitative Data Analysis

The above studies have established the causal and descriptive basis for preliminary research economics of cybersecurity with endogenous institutional change. The causal approach was used to constract a model that explains the relationship between concepts related to cyberattacks (Asher 1983). This methodology relied on qualitative data from online information security journals, commentaries and cybersecurity reports from the Philippine government and private companies. From 2014 to 2016 data from the Department of Justice Office of Cybercrime was gathered to analyze (refer to Table 2) inter-agency coordination of Philippine National Police and National Bureau of Investigation, cybercrime reports increased between 2014 and 2016 (Table 3). This shows that agents are adapting to endogenous institutional change.

Table 2: Cybercrime complaints received by agency

Category	Agency	**2014**	**2015**	**2016**
Cybercrime complaints	PNP-ACG	540	1098	1937
	NBI-OCD	1013	1436	1964
	DOJ-OCC	46	33	50

Table 3: Cybercrime complaints received by agency

Category	Cyber behavior	**2014**	**2015**	**2016**	**Total**
Cyber crimes	Hacking	103	175	314	**592**
	Cyber squatting	4	2	1	**7**
	Data interference	5	1		**6**

[11] Titlling the play field : How Misaligned Incentives work against cybersecurity February 2017

The Global Cybersecurity index report shows that capacity building in the Philippines was 35% in 2017 [12] and 58% in 2018 [13]. Capacity building was measure based on research development, education and training programs, the number of certified security professionals and public sector efforts. The National Computer Emergency Response team reported 95 incidents in September 2019 [14] whereas the report four cyber threats to watch in Q3 2019 where Philippines rank 5th from Kaspersky report[15].

Table 4: NCERT Reported Incidents.

Cybercrime Category	Percentage
Social media hacking	11.60
Cyber-attacks/hacking	11.60
Email/Web phishing	21.10
Online crimes such as;	
a.) Online threats	10.50
b.) Online fraud/scam	10.50
c.) Online libel	6.30
d.) Identity theft	11.60

The data suggest that the cost of cybersecurity continues to increase each year, establish inter-agency information asymmetry with private firms and align incentives would create cybersecurity economics equilibrium. As cybersecurity professionals, we have separated our own biases from technical perspective, so as not to interfere with the data collection or data interpretation. To ensure the validity of our data analysis, we analyzed data reports from both government and private firm, and made our interpretations as previously describe (Creswell, 2013).

Results

We can offer two possible explanations from the observed study. The first possibility, the need for ideas to act as roadmaps for the economics of cyber security, one cannot control endogenous institutional

12 ITU (2017), *Global Cybersecurity Index 2017*, ITU, Geneva, http://handle.itu.int/11.1002/pub/80f875fa-en.
13 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
14 https://ncert.gov.ph/
15 https://bitpinas.com/feature/philippines-4-types-cyber-threats-watch-towards-end-q3-2019/

change but repeated game theory approach of coordination and cooperation will decrease information asymmetries. However, we believe that this will unlikely because of misaligned incentives between agency, departments and private firms who hold the largest ownership of Internet Service Infrastructure and civil society who relied on digital technologies.

The underlying idea was unless institutions incentivize them to do. Agents and private firms as well as organization both tend to act in their own self-interest. As such well programs for information security training within inter-agency and private firms aligning to Global Security Index of ITU. Develop an upgrade systems plan within that will accommodate information disclosure and available upon request to private firms operating largely in cyberspace.

The evidence seems inconsistent with theoretical framework expectations, since in another paper Philippines, Vietnam and Thailand do not provide legal provisions for Rights Holder to directly enforce their copyright protections through ISP notification systems, and are instead forced to seek copyright enforcement though legal action or referred as Judicial System[16]. One of the possibility is that our inter-agency and department process on cybercrimes is new institutions and that none of specialize courts are experienced to handle the cybercrimes specifically cyber-attacks. We believe that this will be more likely to explain in economics and law of cybersecurity.

Coordination failure is the second of economic barriers that lead to changed the behavior of agents within the organization(Greif and Latin 2004). There are three reasons for coordination failure; free-rider, uncertainties and information asymmetric. When both inter-agency generates patterns repeated game with considerable align information such as predictive data report cyber-attacks, systems resources upgrade and coordinated plan and action within executive level.

Limitation was time and data specially interview from participant leaders of department and agencies that will validate the process and structure of their online reports. Even though were working in

[16] Sunkpho, Jirapon & Ramjan, Sarawut & Oottamakorn, Chaiwat. (2018). Cybersecurity Policy in ASEAN Countries.

field, we as information security professionals and researchers carrying out this study, separated our biases from a technical perspective, so it does not interfere with data collection or data interpretation.

For researchers, this highlights the presence of inevitable misaligned incentives and information asymmetries. It indicates that information disclosure on cyber-attacks between public-private sectors will provide necessary protection for consumers. It outlines a clear agenda for future research looking for economics of cyber security policy engagements, focusing on same research design across multiple countries in ASEAN region will permit a more detailed analysis of the causal mechanism in cyber-attacks that affects consumers feeling of uncertainty, fear and doubt.

Discussion and Recommendation

The study found that the role of ideas serves the purpose of guiding behavior under conditions of uncertainty by stipulating causal patterns or by providing compelling ethical or moral motivations for action[17]. The inter-agency report from 2014-2016 was accurate in their agreement about the required outcome to protect the nation in cyber. Indeed, it is vital to understand the economics of cybersecurity as well as how Cybersecurity Philippine Policy and law enforcement need to overcome the economic barrier to mitigate the threat of cyber-attacks. However, arguing that misaligned incentives and information asymmetric are significant in capability development, it was observed that having updated the incident report into data-driven analytics will provide sufficient awareness to society. Additional empirical research needs to be conducted to determine the causal mechanism of cyber-attacks that affects consumers and private sectors that leads to loss of identity and online reputations. As such, only when private-public sector cooperation and coordination would develop a decrease transaction cost of cyber security.

[17] IDEAS, BELIEF, Institutions, Political Change: Foreign and Policy: Goldstein and Keohane p16

REFERENCES

1.Marc Bloch the Historian's Crafts, 1953 p.129

2.YAHOO Report https://ph.news.yahoo.com/timeline-philippine-internet-20th-anniversary-225454753.html

3.DOJ OCC Report https://doj.gov.ph//files/OOC/ooc_report_corrected.pdf}.

4.Titlling the play field : How Misaligned Incentives work against cybersecurity February 2017

5.The Role of Interest, Institutions and Ideas Peter Hall 1983 pp-184-185

6.https://www.dap.edu.ph/rbpms/agency/cybercrime-investigation-and-coordination-center/

7.The Economics of Cybersecurity [Commentary] 2017 p 52 by Axel Wirth

8.SRI The Strategic Importance of National Cybersecurity Plan 2022 by Francis Domingo June 5, 2017

9.A Theory of Endogenous Institutional Change Vol 98 No 4 November 2004 American Political Science Avner Greif and David D. Laitin 2004 p 2

10.AVNER GREIF and DAVID D. LAITIN, A Theory of Endogenous Institutional Change, Vol 98. No 4, November 20019 p.637

11.Accenture 2019 Cost of Cybercrime: Unlocking the value of improving cybersecurity protection

12.Titlling the play field : How Misaligned Incentives work against cybersecurity February 2017

13. ITU (2017), Global Cybersecurity Index 2017, ITU, Geneva,http://handle.itu.int/11.1002/pub/80f875fa-en. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

14.National Certificate Report https://ncert.gov.ph/

15.BitPinas.com https://bitpinas.com/feature/philippines-4-types-cyber-threats-watch-towards-end-q3-2019/

16.Sunkpho, Jirapon & Ramjan, Sarawut & Oottamakorn, Chaiwat. (2018). Cybersecurity Policy in ASEAN Countries.

17.IDEAS, BELIEF, Institutions, Political Change: Foreign and Policy: Goldstein and Keohane p16