Clicking for Physical Security, Can It Be?

Cakti Indra Gunawan
Economic Faculty
Tribhuwana Tunggadewi University
Malang, East Java, Indonesia
cakti.gunawan@gmail.com

Putriyana Asmarani
Department of International Relation
International Research Development for Human Beings
Malang, East Java, Indonesia
Putriyana.irdh@gmail.com

***Abstract*— This research examines issue on physical security that can be solved through cyber security. Having Cakti Economic Theory (CET) as theory and at the same time software of governing management system, this research evaluates the possibility of how CET possibly maintains physical safety through its software. As a form of new theory exploring philosophical use of a software, this research challenges the conceptual building of CET which arrives to the conclusion that physical security can be maintained through CET software.**

Keywords— Cakti Economic Theory; Physical Security; Cyber Security; Security Management Introduction

I. INTRODUCTION

Raising question on how cyber security meets physical security is fascinating yet challenging. Forbes website released an article in 01/13/2017 signalling terrifying moment on physical attack which is trigerred by cybercrime. From how Ukraine experienced firsthand the result of cyber-induced blackouts to the creation of US cyber security forces aiming on protecting the lives of targetted influential people, cyber security danger is getting more physical [1]–[4]. The cybercrime goes beyond hacking datas, but attack physically, for warfare has been in a new order besides of air, water, and land [5]–[8]. Responding to this ever changing form of security, instead of (just) concerning at the safety of influential people, this research focuses on the safety of ordinary people as reflected to Cakti Economic Theory security pillar operating safety software for protecting the lives of people.

As a set of governing management idea, CET raises humanity issues to be solved in the five pillars which one of them is security. Theoretically, taking into consideration numbers of violence, corruption and terrorism, CET believes that the key of physical security can be solved cyberly [9, p. 16]. Hence, CET is form of software generating ordinary people to be the source of data by reporting crime or accident, they saw firsthand to the CET software, received by assessors then the output is physical action from police officers. Seeing closely what happens in developing country, it is indeed that the police officers have hotline available to receive emergency call 24 hours, but most people do not currently use manual call [10], [11]. It is then to consider that, by the changing of media choice, media should be functioned to generate the safety of people.

What is contested so far in most of researches are in the realm of how cybercrime attack important governmental or private sectors cloud data and cyber financial institution. But plenty about how cybercrime can actually trace people because ‘nowhere to hide’ [12] and new invention about how ordinary people can function technology to save the lives of others. Literature review in the research will expose, evaluate, compare and contrast what are rarely yet important investigation about the function of technology on how it should generate physical security. While, CET detail explanation and mechanism is discussed directly after introduction. The rest of this research exposes CET as a new software invention on how it is projected to maintain cyber security for physical security and come to conclusion in the cyber world, can we click for physical security?

II. CAKTI ECONOMIC THEORY (CET) AND RESEARCH METHOD

Scrutinizing CET in which it employs five gigantic pillars on humanity values, economic acceleration, education, security, and reward and punishment is somehow challenging to decipher. Moreover, this theory is barely used and criticized as the new branch of economic theory combining humanity and economic perspectives. This theory is founded in 2016, in fact it gains little of academic intention due to its less popularity. This research hereby takes one security pillar in CET in which the method will reflect to how it is work theoretically. As a software and at the same time as a theory, CET believes that the use of advanced technology is expected to maintain greater safety.

Since this research discusses how CET works and elaborates its contributions on maintaining better safety. Thus, this research uses descriptive analysis refering to how CET as a new theory. The steps of discussion is firstly talking about its philosophical foundation in CET in viewing about security, secondly about its mechanism on how the software manages the action for maintaining security, and the last is how the software is expected to contribute in the study and practice of security management.

The mechanism of how the software maintain security is the first thing to be known in CET is the mechanism of every pillar is operated in the same design, one user reports, user number two assesses and user number three is called to action and give notification of either giving reward or punishment [9, p. 17]. Focusing on security pillar in its mechanism, the individual user report is assessed then the user is notified. This software is designed in the simple operation because the user is ordinary people and projected to people in need [9, p. 18]. The individual user here can be the person experiencing crime who

is able to click report during the attack or other people who recognize the crime [9].

CET's design is formed from the relation between bottom to up and up to bottom. Reflecting the government structure of Indonesia, CET is developed for prioritizing the very low level of government system to be more active and considered [9]. The individual report here refers to the citizen level where they become the central concern of economic growth and welfare. Sub-levels of servers are designed to monitor its district and people [9]. The figure 1 below present CET server flow and mechanism on how data is transferred;

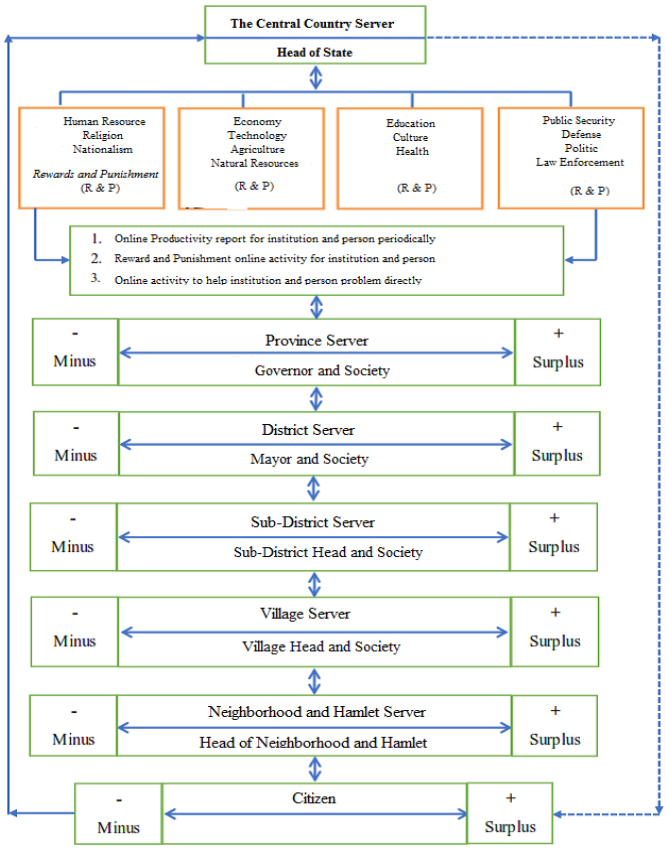


Fig. 1. CET's Model and Mechanism [9]

The orange boxes are CET pillars which each box R and P or Reward and Punishment is included within the boxes. Reward and Punishment are the system respond after the report. Person who has reported the crime will be rewarded. Green boxes are the regulation on how the report is delivered, received and responded. While the blue lines links the overall stakeholders and the system as well [9]. The description of surplus and minus are referring to collaboration on the economic sharing between the surplus village with the minus village. The delivering system of report in the security pillar is sending the data in each the police office placed in the district.

Theoretically, CET is developed under humanity foundation aiming on the economic betterment. Under this foundation, security pillar is maintained because CET believes that the security of nation influences the economic condition of a country [9]. Mirroring to Bastiat's 'The Broken Window Fallacy' discoursing the big loss of national funding caused by natural disasters by analogizing bakery shop's broken window [13], [14] CET believes that by having good security management the nation does not have to suffer big loss [9]. Not limited to what is explained by Bastiat (2001), CET is ignited by the believe that technology could be a media and bridge to better economic condition [15]–[19]. The five pillars, as CET believes are the components that a country should pay attention to.

This research takes security pillar because security is essential [2], [3], [11], [20], [21]. The researcher believes that if security is not yet fulfilled the society will experience fear which leads to hatred and hatred leads to violence [8], [22]–[25]. Security in modern world has to also adapt with the creation of artificial intelligence to give what beyond modern protection [3], [23], [26]. This research brings new theoretical approach for physical security maintained by cyber security which is elaborated in discussion.

III. RELATED LITERATURES

Modern security, the study of its form and management has been issued in many researches. Most of these researches come to the same conclusion which aim to the new consideration of modern security that should not be neglected, then it examines mostly in the security of data cloud computing, risk management and cyber attack on how to solve it [1], [25], [27]–[30]. The closest research on physical security and the idea that preparation in security management is crucially needed is Blake D. (2017) on Get prepared: Discourse for the privileged?, Lemay A., Calvet J., Menet F., Fernandez J.M. (2017) on Survey of Publicly Available Reports on Advanced Persistent Threat Actors and Shamala P., Ahmad R., Zolait A., Sedek M., (2017) Integrating Information Quality Dimensions into Information Security Risk Management (ISRM).

The importance of preparation on how it is expected to be for most civilian not just the privileged [31] believes citizen should get the access to security as much as the privileged do. The belief that the basis of structural violence is caused by insecurity, this research exposes the current ignored preparation mainly in New Zealand. This research concerns in the most vulnerable groups who actually experience the damage even worse. Providing the folks sufficient information and educate the children about risk and preparation become the major topic of discussion in this journal. Reflecting to CET, the websites of such have been everywhere and people can learn it in Youtube as well. This research believes with the idea that security must also privileged the most vulnerable group, but the CET website is a media for people to report any accident, bribery, thief, illegal drug and etc.

The act of espionage and spying in attempts to gather information of particular leader, person and group [32] become the concern of the second related studies. This research concerns on the protection of particular data related to people as in FireEye blog named 'The EPS Awakens' and also identifying tools that are commonly used to in cyber crime. Research with the same view Integrating Information Quality

Dimensions into Information Security Risk Management (ISRM) also manages information received that stores just the important one [1]. ISRM methods of collecting important information and assessment model are through the website system while CET uses assessor user. Thus, the above gaps and similarities are defined in this research as general outlook on how CET works in maintaining security.

IV. DISCUSSION

Physical or personal security has been highly concerned in developing countries because it is targeted to be having traditional easy-hacking or vulnerable physical safety management [33]. It is also reported that besides of financial insecurity happening in 2017, personal security is placed in the second place after financial security [33], [34], hence it is a must to set priority to physical security. The national concern of economic development is generated from how much human is developed, freedom from fear makes it obvious on how it impacts to human development. Thus, providing security is essential [35]. The figure 2 below shows that developing countries, especially Philipine reaches the highest insecurity;

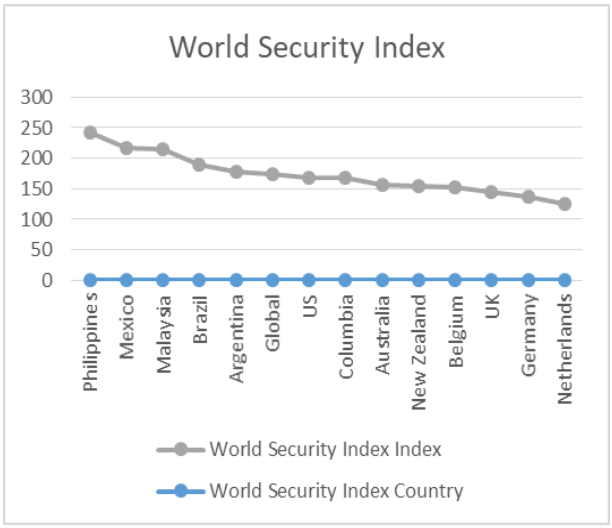


Fig. 2. World Security Index [33]

Not limited to Philipine, Myanmar, and many of Middle East countries experience the hardship of having freedom of fear. Thus, it is important to examine what goes wrong in their security management. Aiming at gaining ideal democracy based on the identity of Philipine, thi developing country has experienced Al-Qaeda attack planned in Mindano, endless insurgency since 1970s, The Moro Islamic Liberation Front, Moro National Liberation Front, The Abu Sayyaf Group, world longest communist insurgency Communist Party of The Philipines, New People's Army since 1973, till external threat on maritime cases [36]. The national policy of Philipines urges the importance of celebrating diversity under the banner of democracy [37]. Elements of peace from the socio-political to harmony is set to accept differences among tribes and territorial integrity [37], the security is maintained manually meaning people go to police office to report problem.

Insurgency is done invisibly, its group and its place of meeting. The central security might not figure this out but the citizen who personally experience this suspected activity might recognize their lair. CET security is a system where people can bring security with them [9], in their handphone or computer. Online report from individual recognizing suspicious movement can report. They do not have to come to the police officer which probably take two public tranportation rute or trapped in terrafic jam. The importance of having self-centered report create wider security. This is reflecting to what happens in Indonesia the Bali Bombing and Kampung Melayu Jakarta Bombing whose one of the terrorist is found in Malang recognized by individual in society who choosed to report to the police [23], [38]. Studies on terrorism reflect that the activities of spreading their innate ideology, movement and recruitment are designed unrecognizeable [2], [7], [31], [34], [39].

Drug abuse as well as sexual abuse are done in possible unrecognizable place where police cannot find them, but their concerned neighbor or a person who recognized sexual abuse in some quite street without the present of CCTV can report. There is one security solution, which in this research believe to be creating and maintaining security for others. It is not rare to find any of physical abuse posted by a person in the social media exposing not to do this or that [40]–[42]. This is quite mind-bogging because the one who posted those might intend just to get lots of like and comment. The idea that it should be reported first than to post it is debatable. Responding to this kind of behavior, it is important to have media to connect people with security officers. Instead of sharing their videos gaining likes or comments, it is better to directly contact their claim through CET.

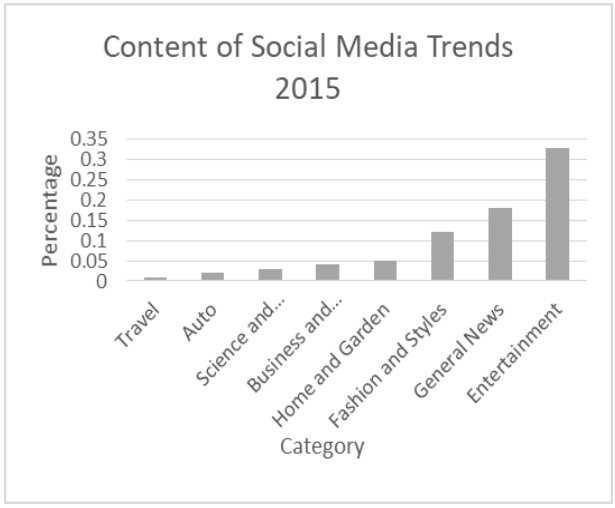
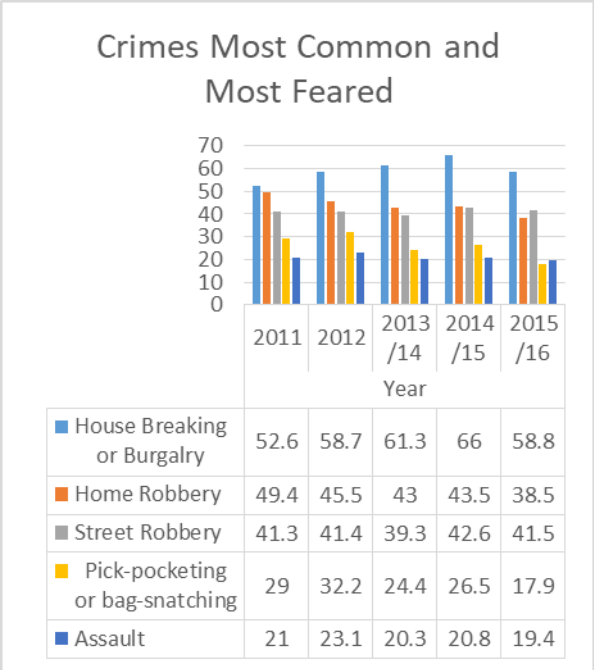


Fig. 3. Content of Social Media Trends [43]

Content of social media above which posts are majorly about entertainment is seen as common use of social media especially following the updates of admired actors. However, the up bringing of social media instead of connecting people has been reported above the mass sharing of general news. This postings reach the second place after entertainment,

presenting the high rate of news interest and postings [43]. Crimes such as house breaking, home robbery, street robbery, pick-pocketing or bag-snatching, and assault, since police do not stand everywhere, individual report recognizing this have media to send the report to the police before it goes fatal. Houses owned by middle-low class society might find it hard to employ guard to keep the house safe, and again security is not only those who are privileged [31]. Everyone is responsible towards their own security and act beyond giving sympathy is all it takes to have secure environment.

Responding to the current crimes which are done very often and threatened almost every day is described in the figure 4. This example is surveyed in South Africa from 2011 to 2016 because this region has been showing great number of crimes attacking common people. The related crimes used in this research is the sample of few crimes that attack everyone, it does not mean to classify whether or not the examples are most dangerous crimes instead of others but as it is referred, these samples are the most feared in South Africa. Involving the most common for what happen in the developing countries in South Africa.



	2011	2012	2013/14	2014/15	2015/16
House Breaking or Burgalry	52.6	58.7	61.3	66	58.8
Home Robbery	49.4	45.5	43	43.5	38.5
Street Robbery	41.3	41.4	39.3	42.6	41.5
Pick-pocketing or bag-snatching	29	32.2	24.4	26.5	17.9
Assault	21	23.1	20.3	20.8	19.4

Fig. 4. Crimes Most Common and Most Feared [44]

Fall by the year 2015/16 does not make house breaking is less feared. It is further reported that the attainment of safety cannot be accomplished until it drives every individual to feel safe leaving their homes or walking alone in the dark [44]. This is to show that the treatment of maintaining physical security must be somehow revised. People do not have to be physically injured first and then the claim fall after the destruction. The online system is far faster in delivering the report than the depressed victim must go to police office, or the person seeing it (who might be too burdened to reach police office or even the person seeing it post the crime in social media.

The level of physical security from minimum to maximum, high security locks to alarm system [45] are the epitome of current defense. Alarm system put in the doors, protected areas, or vital areas are helpful but insecurity can be anywhere, the problem is this alarm is not anywhere. Then, the security might be barely achieved [46]. Where crimes take place also remained a question even some places have been labelled as vital in accordance to many crimes happened there. It is unexpected either the place or the time and it attacks everyone. The need to have the fastest and inclusive connection with security officers is vital, this is the idea of how CET designs the security management.

V. CONCLUSION

The fact that physical insecurity remains the biggest fear after the financial attack through cybercrime become the basis of this research to describe security management system. Since the problem remains it means that the new vision on tackling down physical insecurity is vital. Developing countries such as Philipines and South Africa experience the high rate of physical security. The idea that physical security is possible to be eliminated through online system in CET give the insight of managing security system. The system in which security can be brought everywhere and connect directly to the police officer.

REFERENCES

[1] P. Shamala, R. Ahmad, A. Zolait, and M. Sedek, “Integrating information quality dimensions into information security risk management (ISRM),” J. Inf. Secur. Appl., vol. 36, pp. 1–10, 2017.

[2] U. Human Security Unit, “Human Security in Theory and Practice: An Overview of the Human Security Concept and the United Nations Trust Fund for Human Security,” Un, pp. 1–45, 2009.

[3] F. Whitman, Martin J,. & Diz, Modern Security Analysis. 2011.

[4] D. Hutter, “InfoSec Reading Room Physical Security and Why It Is Important,” 2013.

[5] T. Economist, “Cyberwar,” Am., 2011.

[6] T. Economist, “The_EconomistThe Battle Ahead.pdf.” 2017.

[7] A. Kankanhalli, H.-H. Teo, B. C. Y. Tan, and K.-K. Wei, “An integrative study of information systems security effectiveness,” Int. J. Inf. Manage., vol. 23, no. 2, pp. 139–154, 2003.

[8] I. S. Ladan-baki, “Corruption and Security Challenges in Developing Countries,” vol. 5, no. 5, pp. 1–19, 2014.

[9] C. I. Gunawan, “Cakti Economic Theory,” 2016.

[10] The Economist, “The Economist - The New Tech Bubble.” 2011.

[11] T. Economist and I. Unit, “THE MEANING OF SECURITY IN THE 21st CENTURY Understanding root causes of security threats— and steps companies can take now.”

[12] A. T. S. ASIA, “Nowhere To Hide,” 2004.

[13] C. F. Bastiat, “What Is Seen and what is not seen,” Ideas Lib., pp. 12–14, 2001.

[14] E. In, E. In, O. N. E. Lesson, and O. N. E. Lesson, Economics in one lesson. 1979.

[15] A. Feenberg, Transforming Technology: A Critical Theory Revisited, no. 1. 2002.

[16] A. Feenberg, Questining Technology, vol. 53. 1989.

[17] A. Feenberg, “Critical Theory of Technology,” pp. 245–370, 1992.

[18] T. Standage, “The Return of the Machinery Question,” Econ., vol. Special Re, no. June 25th 2016, pp. 1–14, 2016.

[19] T. Economist, “Humans and Machine,” Econ., p. 1999, 1999.

[20] D. A. BALDWIN, “The concept of security,” Rev. Int. Stud., vol. 23, no. 1, p. S0260210597000053, 1997.

[21] P. Suchý, “Role of Security and Strategic Studies within International Relations Studies,” Def. Strateg., no. 2, pp. 7–16, 2003.

[22] J. T. Checkel, “Socialization and violence,” J. Peace Res., vol. 54, no. 5, pp. 592–605, 2017.

[23] W. Paper, “Development and Security By Frances Stewart,” Development, no. No. 3, p. 43, 2004.

[24] S. Moncrief, “Military socialization, disciplinary culture, and sexual violence in UN peacekeeping operations,” J. Peace Res., vol. 54, no. 5, pp. 715–730, 2017.

[25] O. Ali, J. Soar, and J. Yong, “An investigation of the challenges and issues influencing the adoption of cloud computing in Australian regional municipal governments,” J. Inf. Secur. Appl., vol. 27–28, pp. 19–34, 2016.

[26] Z. Yang, C. Liu, W. Liu, and S. Luo, “Randomized authentication primitive problem in key exchange with strong security,” J. Inf. Secur. Appl., vol. 36, pp. 127–134, 2017.

[27] B. Von Solms and R. Von Solms, “The 10 deadly sins of information security management,” Comput. Secur., vol. 23, no. 5, pp. 371–376, 2004.

[28] R. M. Daniel, E. B. Rajsingh, and S. Silas, “Analysis of hierarchical identity based encryption schemes and its applicability to computing environments,” J. Inf. Secur. Appl., vol. 36, pp. 20–31, 2017.

[29] J. C. Bertot, C. R. McClure, and P. T. Jaeger, “Public libraries and the Internet 2007: Issues, implications, and expectations,” Libr. Inf. Sci. Res., vol. 30, no. 3, pp. 175–184, 2008.

[30] J. Li, Y. Zhang, X. Chen, and Y. Xiang, “Secure attribute-based data sharing for resource-limited users in cloud computing,” Comput. Secur., vol. 72, pp. 1–12, 2018.

[31] D. Blake, J. Marlowe, and D. Johnston, “Get prepared: Discourse for the privileged?,” Int. J. Disaster Risk Reduct., no. August, 2017.

[32] A. Lemay, J. Calvet, F. Menet, and J. M. Fernandez, “Survey of publicly available reports on advanced persistent threat actors,” Comput. Secur., vol. 72, pp. 26–59, 2018.

[33] UNISYS, “UNISYS Security Index : Brazil,” Security, vol. 2009, no. October, pp. 2–19, 2009.

[34] S. Werthes, C. Heaven, and S. Vollnhals, “Assessing Human Insecurity Worldwide The Way to A Human (In) Security Index,” p. 68, 2011.

[35] O. a. Gómez and D. Gasper, “Human Security: A Thematic Guidance Note for Regional and National Human Development Report Teams,” pp. 1–16, 2013.

[36] Z. Abuza, “Special Report The Philipines Internal and External Security Challenge,” no. 4584, pp. 12–17, 2012.

[37] R. O. Philipine, “Philippines National Security Strategy,” 2011.

[38] Bureau of Counterterrorism. United States Department of State, “Country Reports on Terrorism 2016,” no. July, p. 447, 2017.

[39] D. Yergin, The Quest Energy, Security and The Remaking of The Modern World. The Penguin press, 2011.

[40] Y. Dominguez-Whitehead, K. A. Whitehead, and B. Bowman, “Confessing sex in online student communities,” Discourse, Context Media, vol. 20, no. June, pp. 20–32, 2017.

[41] C. M. Jacknick and S. Avni, “Shalom, bitches: Epistemic stance and identity work in an anonymous online forum,” Discourse, Context Media, vol. 15, pp. 54–64, 2017.

[42] D. Landert and G. Miscione, “Narrating the stories of leaked data: The changing role of journalists after Wikileaks and Snowden,” Discourse, Context Media, vol. 19, no. February, pp. 13–21, 2017.

[43] World Newsmedia Network, “Global Social Media Trends 2015,” Eur. Publ. Counc., 2015.

[44] Statistics South Africa, “Victims of crime survey 2015/16,” p. 127, 2017.

[45] M. Perry, Effective Physical Security (Fourth Edition). 2013.