Journal of Korea Multimedia Society Vol. 20, No. 2, February 2017(pp. 279-288)
https://doi.org/10.9717/kmms.2017.20.2.279

Business Process Reengineering of an Information Exchange Management System for a Nationwide Cyber Threat Intelligence

Yogha Restu Pramadi[†] and [††], Yousep Rosmansyah[†], Myonghee Kim[††], Man-Gon Park[††]

ABSTRACT

Nowadays, nations cyber security capabilities play an important role in a nation's defense. Security-critical infrastructures such as national defenses, public services, and financial services are now exposed to Advanced Persistent Threats (APT) and their resistance to such attacks effects the nations stability. Currently Cyber Threat Intelligence (CTI) is widely used by organizations to mitigate and deter APT for its ability to proactively protect their assets by using evidence-based knowledge. The evidence-based knowledge information can be exchanged among organizations and used by the receiving party to strengthen their cyber security management. This paper will discuss on the business process reengineering of the CTI information exchange management for a nationwide scaled control and governance by the government to better protect their national information security assets.

Key words: Cyber Threat Intelligence; Information Exchange Management; Business Process Modeling; IDEF0

1. INTRODUCTION

The term Advanced Persistent Threat (APT) in cyber threat context is given by a group of hackers which are well-funded and resourced; advanced and sophisticated in their tools, techniques, and procedures; and relentless in executing their attacks [1,2]. APT is the latest incarnation of hackers where the modern world has enabled them to profit from their hacking activities by committing banking frauds, selling weaponized malware or by carrying out espionage/sabotage mission. According to [3] the cyber world is now the new battleground of conflicting countries and APT has long been used as the new type of mercenaries that is comparable to special forces to accomplish a mission that previously seems impossible, such as sabotaging a nuclear reactor [4], eavesdropping on government top secret and even stealing PKI root certificates.

Traditional network parameter defense such as firewalls, IDS/IPS, and antiviruses becomes ineffective in facing this kind of threats. The reason behind this is because APT uses a sophisticated *kill chain* that doesn't rely on the weakness of the machine, but it attacks the weakness of the human behind the machine [5]. The term kill chain interestingly enough came from the military because of its methodological approach, and the way to mitigate such attack according to [4] is to use an intelligence-driven defence.

This intelligence approach is used by the US Government by issuing an Executive Order (EO) of the US President [6], where the EO authorizes the dissemination of cyber intelligence reports to critical infrastructure operators. The decision

※ Corresponding Author : Man-Gon Park, Address: (48513) Yongso-Ro 45, Nam-Gu. Busan, Rep. of Korea, TEL : +82-51-629-6240, FAX : +82-51-629-6230, E-mail : mpark@pknu.ac.kr
Receipt date : Jan. 7, 2017, Approval date : Jan. 26, 2017
※ This work was supported by a Research Grant of Pukyong National University (2016 Year).

[†] School of Electrical Engineering and Informatics, Institute of Technology Bandung, Indonesia
(E-mails: yogha.rp@s.itb.ac.id, yusep.ros@itb.ac.id)
[††] Dept. of IT Convergence and Application Engineering, PuKyong Nat. Univ., Rep. of Korea
(E-mails: mhgold@pknu.ac.kr, mpark@pknu.ac.kr)

maker in the oval office realizes the benefits of information exchange where it doesn't only share knowledge about a threat among critical infrastructures but also giving a better view to them for a strategic decision-making process by aggregating intelligence.

In this paper, we propose business process reengineering model for the Cyber Threat Intelligence (CTI) information exchange system on a national scale. The paper will use the IDEF0 method to reengineer the business processes of CTI to better suite a nationwide environment to help the government protect its national assets for a better national cybersecurity posture.

2. CTI ON A NATIONWIDE SCALE

In building a nationwide CTI information exchange model, we need to include all the CTI actors in the national cyberspace of a country from the public sector, the private sector, the military sector and add a new actor as the central of the information hub [7] (Fig. 1). The reason behind this is that a centralized information exchange with a hub and spoke model is the most suitable information exchange model for gathering all the data needed from all the actors involved to generate the information required for nationwide cyber security awareness that the national security analyst needs to make actionable intelligence of the current national cyber security issue. This new actor could be a new or an existing government organization that addresses cyber security issues on a national scale and for this case, it will be named as the national CTI information exchange operator.

In the context of a nationwide CTI information exchange the national CTI operator handles the CTI collection from the other actors; CTI information storage; and actionable intelligence dissemination to other actors that needed them. The national CTI operator also has to manage the analyst with various cyber security expertise required for analyzing the collected intelligence. Unlike the public belief, cyber security is actually a very broad subject with consequences that is critical to the organization.

3. BUSINESS PROCESS MODELING WITH IDEF0

IDEF0 started as a part of the Integrated Computer-Aided Manufacturing (ICAM) program of the United Sates Air Force, ICAM is used to increase manufacturing productivity with the help of computers. IDEF0 was derived from the Structured Analysis and Design Technique (SADT) by its creator Douglas T. Ross. In 1993, the Institute of Electrical and Electronic Engineers (IEEE) started a project that developed the method further by making it a standard for the use of government and

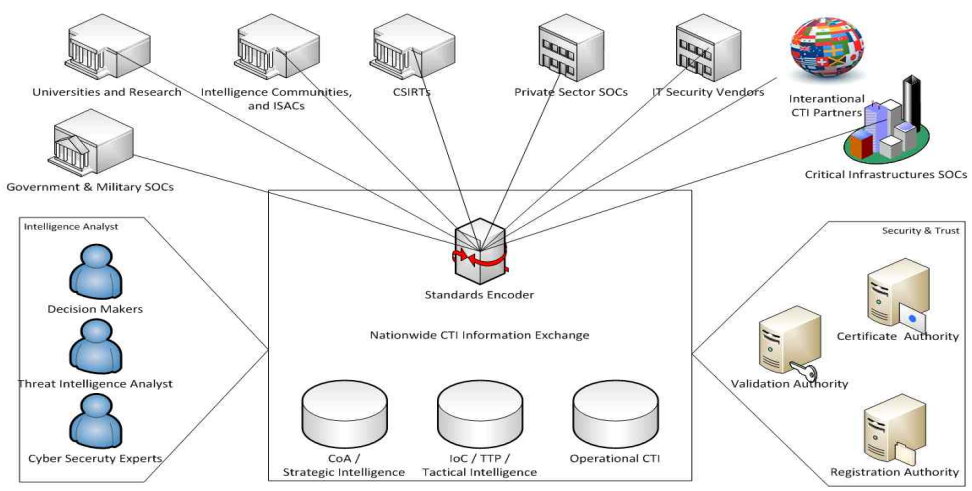

Fig. 1. Nationwide CTI Information Exchange Model.

industry, and published it under the ANSI IEEE Std. 1320.1-1998, the IEEE Standard for Functional Modeling Language -Syntax and Semantics for IDEF0[8].

The IDEF0 analysis starts with identifying the inputs, outputs, controls and mechanism of the context diagram. To identify the inputs of the system we must consider the most important thing in an organization cyber security capability, that is the knowledge, the concern and the attitude of the top level managements towards cyber security[9]. And for a nation, that top level management is the executive leader of the country.

For example, the President of United States of America has recognized the importance of intelligence sharing between their critical infrastructures and issued an Executive Order for it [6].

This is the main drive for the planning of a national scale CTI and also will provide the direction to where it will go once it is established. The other inputs are: The International CTI Exchange, CTI information or request from the nation's international counterpart; *the National CTI Actors*, CTI information or request from the nation's internal CTI actors. For the controls for a CTI implementation are: the government IT policies, government CTI regulations and CTI standards. The CTI regulation documents and cyber security laws must be a priority of the government to fulfill for a successful CTI Implementation. Some countries like the United States have an almost complete set of cyber regulation, legislation and policies to control its CTI operations [10].

The mechanisms needed for the business process is identified from the operational aspect of the CTI process, which are the analyst involved in the intelligence process, the decision makers that directs the intelligence process, the CTI repository that manages the all CTI gathered and produced, and the security mechanism. The decision maker on a national level is usually a government cyber security organization which in this case we will use the name the national cyber security agency. The analyst involved in the intelligence process are divided into two levels, according to the level of intelligence they analyze. The two level of analyst are the intelligence analyst and the cyber security experts. SSL is the most widely used secure communication protocol used in the internet and it is also used to secure CTI information exchange, thus the security mechanism here is the national public key infrastructure (PKI) operator.

And finally the outputs or the products of the process, the first one is actionable CTI information that could be consumed by all the organizations related to the threat, in this process we divide the outputs into two, the national CTI dissemination and the international CTI dissemination. And as the center hub of the national cyber threat intelligence, it is possible to detect a cyber threat in its early stages and can disseminate a national cyber security alert for an early warning system.

After defining all the inputs, controls, mechanism, and outputs, the context diagram (A-0) is developed and shown in Fig. 2. The context diagram makes the base requirement (input, controls and mechanism) to produce the desired outputs of the business process very clear, this makes decision makers can identify any unmet requirements and try to fulfill them.

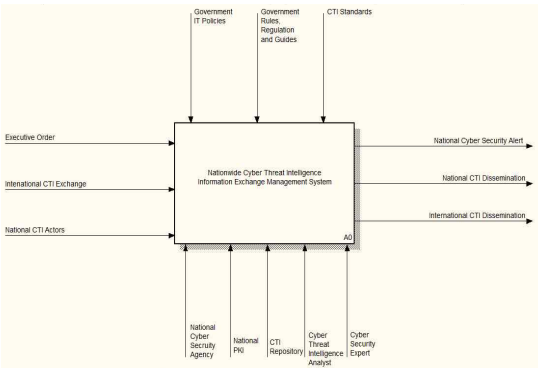

Fig. 2. Context Diagram of National CTI. Information Exchange Management System.

4. BUSINESS PROCESS REENGINEERING OF NATIONWIDE CTI INFORMATION EXCHANGE MANAGEMENT SYSTEM

The CTI concept is built upon the intelligence lifecycle, and as a relatively new concept, there are a lot of different definition of CTI, but the most used definition of CTI is from Gartner [17]. Gartner

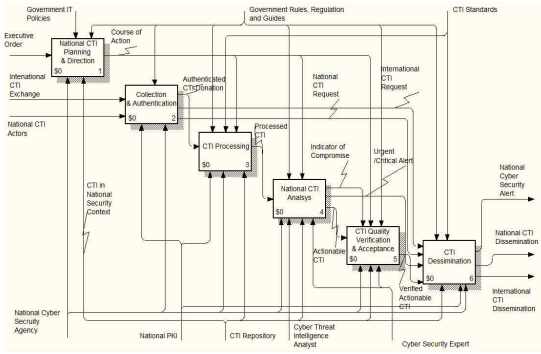

Fig. 4. A0 Diagram.

defined Cyber Threat Intelligence as an "evidence-based knowledge and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard." There are various models and standards used in CTI information exchange management such as the Mitre Standards and Managed Incident Lightweight Exchange (MILE) Standards. Mitre researchers have made three different standards to fulfill the different level of needs of information exchange in a CTI such as the Cyber Observable eXpression (CybOX), Structured Threat Information Expression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) models for fundamental and radical improvements of nationwide CTI information exchange management systems.

In designing the A0 diagram and the node tree diagram looks like an up to bottom activity, but in practice it is more of a mixed approach. Only the main activities are designed up to bottom according to the theories but when we start designing the arrows it actually is more of a bottom up approach. The main activities (A1-A6) are created based on the intelligence where the main activities are: planning, collecting, processing, analysis, and dissemination. The verification and acceptance process is added for quality assurance in the actionable CTI that is produced by the analysis process. These main activities later will be decomposed in detail, and is completed by adapting intelligence activities in military and government intelligence guides [16].

The node tree diagram of the business process model (shown in Fig. 3) is developed for users so they could better understand the structure and the hierarchy of the activities in the nationwide CTI information exchange management system business process, and it also helps the system analyst in designing the whole business process more easily by identifying the core activities without having to worrying to much about the relation between the activities. Under the business node tree diagram, we can draw A0 diagram as shown in Fig. 4.

With the A0 diagram created, it has to be decomposed to capture the important activities in the nationwide CTI information exchange management system. In the following steps the A0 diagram is decomposed into sub processes, and because the IDEF0 is focused on the activities of the business process the research conducted used the intelligence process life-cycle as its main activity and the decomposition will follow the intelligence theories available.

4.1 Decomposition of the CTI Planning Activity (A1)

Planning and directing an intelligence operation is the foremost important task, because it gives a focused direction of the whole CTI process by producing a guide for the whole intelligence process. And to decompose this process of the context of CTI planning activities, we refer the Joint Intelli-

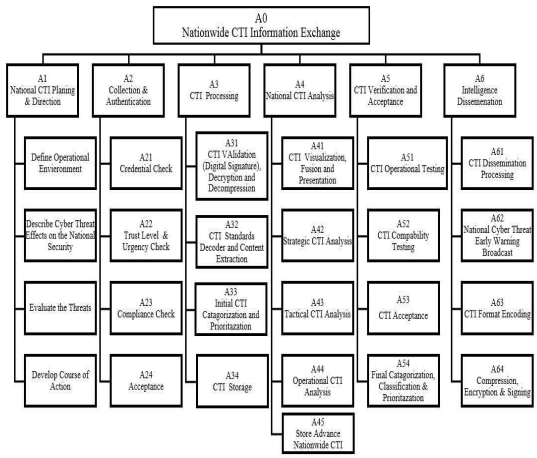

Fig. 3 Business Node Tree Diagram.

gence Preparation of the Operational Environment (JIPOE) from the Joint Publication 2-0 of the US Joint Intelligence Organizations [10] as shown in Fig. 5.

The JIPOE process consists of four steps starting from defining the operational environment, describing the impact of threat, evaluating the threat, and at the end of the process it produces a document called the Course of Action (CoA) as the guide of the whole intelligence related process that follows. This process is adopted in a cyber threat intelligence context in the A1 diagram shown in Fig. 6, where the operational environment is the national cyber landscape and the threats actors are adversaries that have a motive and a goal in the national cyber environment.

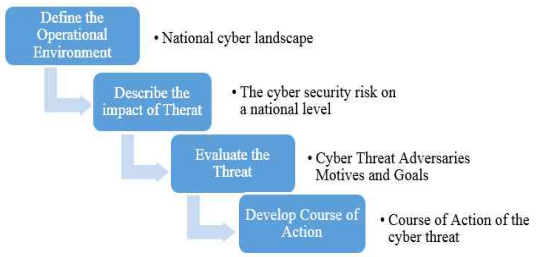

Fig. 5. The Intelligence Planning and Direction Process.

The detail of each activity is described as follows:

• Activity A11, Define Operation Environment: the executive order is the main driving input that initiates the whole CTI process, and the government IT policies, rules, regulation and guides becomes the control of the process and the National Cyber Security Agency and CTI in context of national security from the CTI repository as the mechanisms to help the decision makers to define the operations environment.

• Activity A12, Describe Cyber Threat Effect on National Security: the decision makers must describe the effect of the cyber threat on national security, this can help determine the urgency and the degree of the risk that the country face if such of a threat occur.

• Activity A13, Evaluate The Threat: in this activity the decision makers must define a national level strategic plan on facing cyber threats, such information includes *who* are behind the threats, *what* are their motives, resources and capabilities, and *where* does the threats come from.

• Activity A14, Develop Course of Action: the course of action document is a document that describes the prediction of the course of action of the adversaries based on prior analysis and also determine the needed actions that the nation must do to minimize the risk or to mitigate the cyber threat.

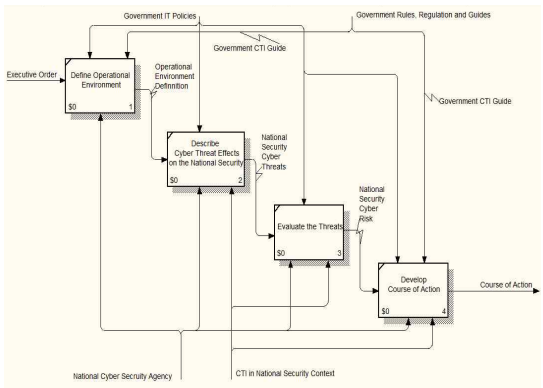

Fig. 6. A1 Diagram: The National CTI Planning and Direction.

4.2 Decomposition of the CTI Collecting Activity (A2)

In decomposing the CTI collecting activity, we must meet the requirements of CTI information sharing requirements describe in [11], where trust, security, interoperability is stated as the main challenge in gathering intelligence. We can draw decomposed A2 diagram as shown in Fig. 7. And the detail of each activity is described as follows:

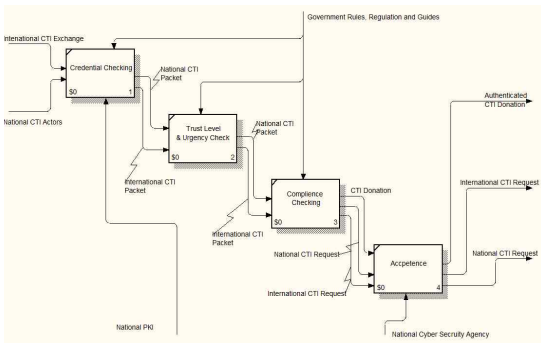

Fig. 7. A2 Diagram: Collection and Authentication.

• Activity A21, Credential Checking: the credentials of the actors involved in the national CTI must be checked before gaining access to the services that the nationwide CTI information exchange management system provides.

• Activity A22, Trust Level & Urgency Check: the trust level and the urgency of the actors are checked.

• Activity A23, Compliance Checking: the actors are checked for their compliance to the controls of the system.

• Activity A24, Acceptance: if all the activity above is cleared, the access is granted.

4.3 Decomposition of the CTI Processing Activity (A3)

In processing CTI, NIST Special Publication 800-150, the Guide for the Cyber Threat Information Sharing [12], explains the activities in processing CTI that includes: validation, encryption, decompression, content extraction, prioritization, and categorization. These activities are adopted into the A3 diagram (Fig. 8). The business processes by grouping some processing activities are as follows:

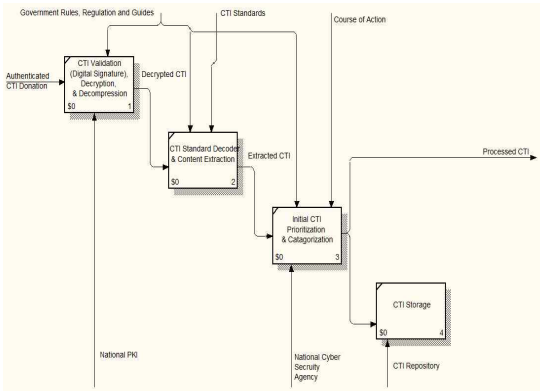

Fig. 8. A3 Diagram: CTI Processing.

• Activity A31, Validation, Decryption, and Decompression: are group into one activity because in real world implementation it is handled by the SSL protocol. The mechanism here is the national PKI that provides certificates for both party for a mutual authentication to establish trust (authentication), confidentiality, and integrity.

• Activity A32, CTI Standard Decoder and Content Extraction: the content extraction activity is added with a CTI standard decoder activity to form the second activity, because in real life the extraction process of the CTI will have to decode the various CTI standards and formats used by the actors that donated the CTI.

• Activity A33, Prioritization and Categorization: the two activities are grouped together into one activity as it is handled by the same mechanism and controls.

• Activity A34, CTI Storage: all the gathered intelligence must be stored in a data center for future analysis.

4.4 Decomposition of the National CTI Analysis Activity (A4)

In designing the decomposition of the national CTI analysis activity, the intelligence pyramid [13] depicted in Fig. 9 is used as reference where it describes three level of intelligence: strategic, tactical and operational. The three level of intelligence is translated into three different activities in the decomposition because they are carried out by different level of analyst and also produces three different outputs. The pyramid also shows that the to produce strategic intelligence, the decision makers cannot consume CTI directly, they need aggregated high level data, therefore before any CTI can be consumed by the top level managements it must be sorted, grouped, fusion and present it in a visual manner [14]. To accommodate those needs a CTI visualization, fusion and presentation activity to be added before the CTI is passed to the strategic CTI analysis.

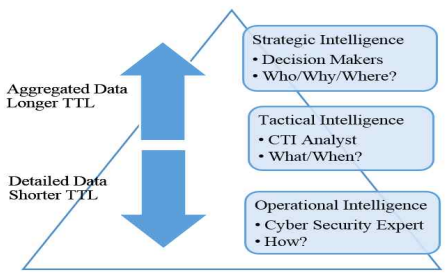

Fig. 9. The Intelligence Pyramid.

The decomposition of the activity as drawn in Fig. 10 is described as follows:

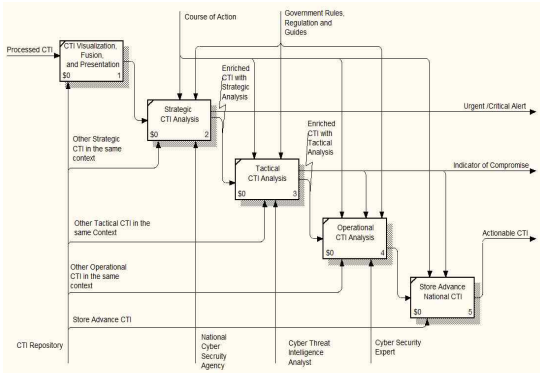

Fig. 10. A4 Diagram: National CTI Analysis.

• Activity A41, CTI Visualization, Fusion and Presentation: the activity here is maybe the most complicated technical activity because it requires sophisticated techniques and algorithm to filter, aggregate and fuse relevant intelligence from different intelligence types and then present them using numbers, chart, maps, images and animation (visualizing it) for consumption of the decision makers to make strategic CTI Analysis.

• Activity A42, Strategic CTI Analysis: strategic analysis in this activity analyze the adversary. The difference of this activity and the strategic analysis activity A1 is that this activity is more on a specific threat scope.

• Activity A43, Tactical Analysis: based on the strategic analysis, cyber threat intelligence analyst can use more technical intelligence fused with the high level strategic intelligence to determine the TTP that the adversary use to compromise a target and develop an indicator of compromise (IoC).

• Activity A44, Operational CTI Analysis: in this activity cyber security analyst with high technical abilities must create actionable CTI based on the IoC, this actionable CTI is an operational level intelligence that consists of signatures or configurations that is ready to be consumed by the security tools and products.

• Activity A45, Store Advance National CTI: the produced intelligence from all above activities must be stored for future analysis and evaluation.

4.5 Decomposition of the Quality Checking and Acceptance Activity (A5)

The quality checking and acceptance activity is the only activity that is not in the intelligence lifecycle that is included in the business process, the reason behind adding an extra activity is that interoperability and automation is one of the biggest challenge in CTI information sharing[14] that needs to be addressed. The nationwide CTI information exchange has to accommodate various security tools and products that the actors uses, the CTI that it disseminates must be a true actionable intelligence that could be used to auto configure security products for a fast mitigation of a cyber security threat.

Explanation of the activities as drawn in Fig. 11 in this decomposition is as follows:

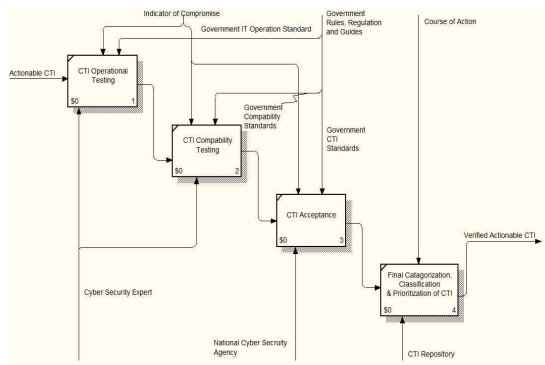

Fig. 11. A5 Diagram: CTI Quality Verification & Acceptance.

• Activity A51, CTI Operational Testing is responsible in testing the intelligence on an operational level by using the IoC as the guiding control. For example, a malware that communicate to its C&C at a certain URL or IP address must be blocked using a certain firewall rule, this activity must test if the rules work as intended.

• Activity A52, CTI Compatibility Testing is the activity where the approved operational intelligence from the previous activity is translated into an automated format that could be consumed by various security products. For example, the firewall rule is translated into a specific firewall rule format that is acceptable by a specific firewall

vendor. The national CTI if possible must support all the common automated formats that is available in its market, or force the vendors to comply to a specific open format that the government endorse.

• Activity A53, CTI Acceptance is the activity where the CTI produced is checked and verified whether it meets the quality threshold and meets the government CTI standard.

• Activity A54, Final categorization, classification and prioritization of CTI, is the activity where the CTI is categorized according to the target actors (for instance the CTI is targeted to critical infrastructures), classified according to the degree of secrecy, and prioritization according to the degree of urgency. In this activity the storage of the verified actionable CTI is also stored along with its categorization, classification and prioritization information.

4.6 Decomposition of the Intelligence Dissemination Activity (A6)

The last activity in the CTI lifecycle is the dissemination of the produced actionable nationwide CTI drawn in Fig. 12, the essence of this activity is that the information could be disseminated in a fast and secure manner. Because the nature of intelligence according to [15] is timely, in this activity we added a national cyber threat early warning system so that a catastrophic outcome from a high risk cyber threat could be mitigated if it is detected in an early stage. This activity is decomposed into four activities as follows:

• Activity A61, CTI Dissemination Processing, handles all the CTI request and outgoing CTI that needs to be disseminated. This activity retrieves the requested CTI from the CTI repository if there is a request for specific intelligence, or forward a CTI that the system needs to broadcast and appends receiver data like the format it uses and the IP address of the receiving network.

• Activity A62, National Cyber Threat Early Warning Broadcast, is responsible to broadcast cyber threat warning into open channels.

• Activity A63, CTI Format Encoding, is the activity to encode the disseminated CTI using the CTI format that the receiving party understand. Not to be confused with activity A52 which deals with hardware specific automation format, this activity deals with the format in threat intelligence information sharing/exchange.

• Activity A64, Compression, Encryption and Signing, is the activity that ensures trust, confidentiality and nonrepudiation in the CTI dissemination activity.

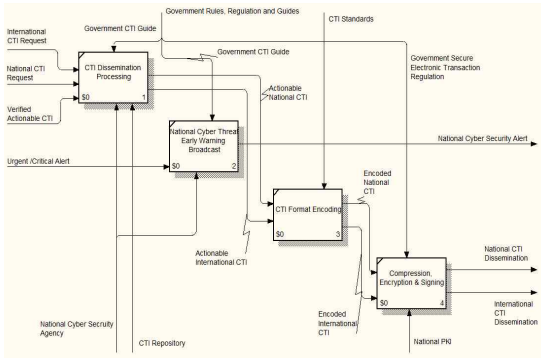

Fig. 12. A6 Diagram: CTI Dissemination.

5. CONCLUSIONS

A study of a nationwide CTI information exchange management system is a proof-of-concept study in designing and planning a strategic information management system at a country scale.

In this paper, we discuss a concept of a nationwide CTI information sharing platform that could be used to detect and mitigate cyber security risk on a national scale to prevent a national cyber incident and provide a cyber threat early warning. And we propose business process reengineering model for the Cyber Threat Intelligence (CTI) information exchange system on a national scale. The paper will use the IDEF0 method to reengineer the business processes of CTI to better suite a nationwide environment to help the government protect its national assets for a better national cybersecurity posture.

This paper also proves that by using business process modeling method with IDEF0, it is possible to depict the complex nature of implementing cyber

threat intelligence information sharing and analysis on a national scale. IDEF0 is powerful tool for that it can simplify the complex task of the intelligence life cycle and provide us with a model that could guide us to develop the system based on its operational activities and needed control and mechanism resource. With the activities, input, output, control and mechanisms in the IDEF0 diagram of the nationwide CTI information exchange defined, the diagrams could be used as a blueprint to guide the technical design of the nationwide CTI.

REFERENCES

[1] A.K. Sood and R.J. Enbody, "Targeted Cyberattacks: A Superset of Advanced Persistent Threats," *IEEE Security and Privacy*, Vol. 11, No. 1, pp. 54-61, 2013.

[2] *Advanced Persistent Threats: A Decade in Review*, Technical Report of Command Five Pty Ltd, 2011.

[3] K. Geers, D. Kindlund, N. Moran, and R. Rachwald, *World War C: Understanding Nation-State Motives behind Today's Advanced Cyber Attacks*, Technical Report of FireEye, 2014.

[4] D. Kushner, "The Real Story of Stuxnet," *IEEE Spectrum*, Vol. 50, No. 3, pp. 48-53, 2013.

[5] B. Schneier, Phishing Has Gotten Very Good, https://www.schneier.com/blog/archives/2013/03/phishing_has_go.html (accessed Nov., 15, 2016).

[6] R.L. Trope and S.J. Humes, "By Executive Order: Delivery of Cyber Intelligence Imparts Cyber Responsibilities," *IEEE Security and Privacy*, Vol. 11, No. 2, pp. 63-67, 2013.

[7] Y.R. Pramadi, Y. Rosmansyah, and M.G. Park, "A Study on Cyber Threat Intelligence Information Exchange System," *Proceedings of the 5th Japan-Korea Joint Workshop on Complex Communication Sciences*, pp. 156-159, 2016.

[8] *IEEE Standard for Functional Modeling Language-Syntax and Semantics for IDEF0*, IEEE Standard 13201-1998, 1998.

[9] Information Systems Audit and Control Association, *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*, Rolling Meadows, IL 60008, USA, 2012.

[10] B.E. Grooms, *Joint Intelligence Preparation of the Operational Environment*, Joint Intelligence Organizations, USA, pp. 1-285, 2009.

[11] C. Johnson, L. Badger, and D.C. Waltermire, *NIST Special Publication 800-150, Guide to Cyber Threat Information Sharing (Draft)*, National Institute of Standards and Technology, 2014.

[12] C.S. Johnson, M.L. Badger, D.A. Waltermire, J. Snyder, and C. Skorupka, *Guide to Cyber Threat Information Sharing*, National Institute of Standards and Technology, NIST-SP 800-150, 2016.

[13] A. Liska, *Building an Intelligence-led Security Program*, Elsevier, Waltham, 2014.

[14] A. Kornmaier and F. Jaouen, "Beyond Technical Data-A More Comprehensive Situational Awareness Fed by Available Intelligence Information," *Proceedings of 2014 6th International Conference on Cyber Conflict*, pp. 139-154, 2014.

[15] K. Giles and W. Hagestad II, "Divided by a Common Language: Cyber Definitions in Chinese, Russian, and English," *Proceedings of 2013 5th International Conference on Cyber Conflict*, pp.1-17, 2013.

[16] S.Y. Kim, M.H. Kim, and M.G. Park, "A Study on the Information Security Control and Management Process in Mobile Banking Systems," *Journal of Korea Multimedia Society*, Vol. 18, No. 2, pp. 218-232, 2015.

[17] H. Dalziel, E. Olson, and J. Carnall, *How to Define and Build an Effective Cyber Threat Intelligence Capability,* Syngress, Waltham, 2015.

Yogha Restu Pramadi

He graduated with Bachelor of Education in Information Systems at the University of Indonesia in 2010.
He is a graduate student in School of Electrical Engineering and Informatics at the Institute Technology Bandung, Indonesia, and also a research member of the Software Engineering and Multimedia Information System (SEMI) Lab. as well as a dual degree graduate student of Pukyong National University, Rep. of Korea. His research interests are in Information Security, Software Security and Safety.

Yousep Rosmansyah

He graduated with Bachelor's degree in Electrical Engineering at the Institute Technology Bandung (ITB), Indonesia. He graduated with B.E. in Satellite Engineering and Ph.D. in Electrical Engineering at University of Surrey in England in 2003. He is a lecturer of School of Electrical Engineering & Informatics, Institute Technology Bandung since 1997. His interests are Mobile Application and Technology, Mobile Learning, and Wireless Sensor Networks.

Myong Hee Kim

She graduated with M.S. degree in Computer Science and Ph. D. in Information Systems from the Pukyong National University, Rep. of Korea. She was a Post Doctoral Researcher at the University of Colorado-Denver, USA. She is a lecturer of the Department of Information Systems, Graduate School, Pukyong National University. Also she was a lecturer of the Department of Computer Science and Engineering at the University of Colorado-Denver, USA. She served as an Assistant Faculty Consultant and an ICT Professional specialist for CPSC which is an Inter-Governmental International Organization for Human Resources Development in Asia and the Pacific Region.

Man-Gon Park

He is a head professor of the Dept. of IT Convergence and Application Engineering, Pukyong National University, Rep. of Korea since 1981. Also he was the president and chairman of the Korea Multimedia Society. He served as the Director General and CEO of the Colombo Plan Staff College for Technician Education (CPSC) from 2002 to 2007, which is an intergovernmental international organization of 29 member governments for Human Resources Development in Asia and the Pacific Region. His main areas of research are software reliability engineering, software safety and security engineering, BPR, Internet and web technology, multimedia information processing technology, and ICT-based HRD.