MILITARY-BASED CYBER RISK ASSESSMENT FRAMEWORK FOR SUPPORTING CYBER WARFARE IN THAILAND

Aniwat Hemanidhi & Sanon Chimmanee
Faculty of Information Technology
Rangsit University, Thailand

ahemanidhi@rta.mi.th; sanon.s@rsu.ac.th

ABSTRACT

Information Technology (IT) Risk Management is designed to confirm the sufficiency of information security. There are many risk management/assessment standards, e.g. IS0 27005:2011 and NIST SP 800-30rev1, which are mainly designed for general organizations such as governments or businesses. Cyber risk assessment focused on military strategy has been rarely studied. Hence, this paper presents an innovative cyber risk assessment conceptual framework named "Cyber Risk Assessment (CRA)" which is extended from previous work with Military Risk Evaluation (MRE). This proposed CRA is the collection and integration of both quantitative and qualitative data. The Vulnerability Detection (VD) tools in Network Risk Evaluation (the previous studies) were used for the quantitative data collection and the focus group in the MRE (the proposed method) was used to collect qualitative data, which enhance the general risk assessment standard to achieve the objective of the research. The complexity of cyberspace domains with a military perspective is thoughtfully contemplated into the cyber risk assessment for national cyber security. Results of the proposed framework enable the possibility of cyber risk evaluation into score for national cyber security planning.

Keywords: Cyber risk assessment, risk management, cyber security, cyber warfare, Network Centric Warfare.

Received: 2 December 2016 **Accepted**: 15 March 2017

INTRODUCTION

Risk management is a substantial solution to deal with IT risks. It integrates entire organization processes together. In accordance with ISO 31000:2009 (ISO, 2009), risk assessment is the core process within risk management. There are 3 phases in risk assessment including risk identification, risk analysis and risk evaluation. Typically, organizations manage risks with risk assessment process in order to modify risk treatment as satisfied by the risk criteria. Numbers of IT and computer security standards have been developed and updated continuously to manage information security, e.g. ISO/IEC 27000 Series (ISO/IEC, 2014) and NIST SP 800-82rev2 (NIST, 2015). Generally, information security management system (ISMS) standards, such as ISO 27001:2013 (ISO, 2013), will explain the information security terminology and risk management process but leave methodology open for organizations to choose the most appropriate one for themselves. However, main concerns of these standards remain business continuity and disaster recovery. Risk management standards for some specific types of organization may be available. For example, ISO 27799:2016 (ISO, 2016) provides implementation guidance for the controls that could be effectively used for managing health information security. Unfortunately, risk management for extremely dangerous threats that could be part of Cyber Warfare (CW), for example, Advance Persistent Threat (APT)/Nation state, is not completely clarified by these famous standards and frameworks.

Cyberspace is the latest domain within a military battlefield. It is a logical domain which is very sophisticated and difficult to control. Also, there are many uncertain stakeholders in cyberspace. General users around the world could elevate themselves as anonymous cyber criminals, terrorists and warriors at any time. Attackers can penetrate targets via the World Wide Web (WWW) using reconditely technical skills and supported tools. Regular IT equipment could be converted into cyber weapons instantaneously. For threat to the nation state or corporate espionage to gain more military or economic advantage, it is much cheaper and more efficient to conduct cyber operations than use traditional spies. Many organizations and countries are developing plans and capabilities to use the WWW to cause or increase the impact of terrorism and even full-scale wars (Andress & Winterfeld, 2011). One demonstration was the cyberattacks on Estonia in April and May 2007 by digital activists from the Russian diaspora (Herzog, 2011). This resulted in preventing Estonia public services from conducting their functions for two weeks.

Other serious examples are cyber attacking of Iran nuclear power plan by the American-Israeli Stuxnet virus in 2010 (Karnouskos, 2011), cyber

attacking of the computers of South Korean hydro and nuclear power operator suspected by North Korea in 2014, and hacking of Sony Picture Entertainment in November, 2014. In this century, threat spectrum becomes far more complicated and dangerous than ever. Modern military troops must be trained in both basic military operations and insidious cyber threats in multidimensional environments. Hence, this paper presents an innovative "Cyber Risk Assessment (CRA)" conceptual framework which intends to extend the previous Cyber Risk Evaluation (CRE) framework in order to fulfill risk assessment standards based on NIST SP 800-115 (NIST, 2008) and ISO 31000:2009 (ISO, 2009). Military Risk Evaluation (MRE) is presented based on Critical Security Metric (Sun, Jajodia, Li, Cheng, Tang, & Singhal, 2010) and Network Centric Warfare (NCW) (DOD, 2003). It is also extended to Risk Environment (RE) with additional likelihood of occurrence and magnitude of impact. In other words, the proposed CRA involves the collection and integration of both quantitative and qualitative data. The VD tools in Network Risk Evaluation (NRE) were used for the quantitative data collection, and the focus group in the MRE (the proposed method) was used to collect qualitative data. The outcome is Cyber Risk Assessment in military perspective, which is very useful for supporting cyber warfare.

LITERATURE REVIEW

Information and Asset Security have been developed continuously covering physical, communication, emission, computer, network, information and cyber security. No perfect solution could secure everything at the same time. The best security is perhaps to apply all of them together. Our research concentrates on the integration of network and information security that lead to cybersecurity in military concerns. Many concepts and research articles related to cybersecurity, cyber warfare, Network Centric Warfare (NCW), social network and SCADA were reviewed.

IT SECURITY AND RISK MANAGEMENT/ASSESSMENT STANDARDS

IT security relied on standards, protocols and procedures from numbers of vendors and related organizations. Many products from vendors are introduced to public companies and government agencies. Vulnerability Detection (VD) tools are prominent equipment used for scanning, detecting and analyzing vulnerabilities on each host. An important outcome is risk analysis for cyber

defense purposes. Security metrics and related standards are background features that significantly influence the results of VD tools. In one of our previous works (Chimmanee, Veeraprasit, Sriphrew, & Hemanidhi, 2012), we compared the scanning performance of two VD tools (NetClarity and Nessus). The result showed that each VD tool has unequal ability to detect hosts and vulnerabilities. Classification for the risk level of found vulnerabilities are also very diversified. The same vulnerability, as specified by the Common Vulnerabilities and Exposures list (The MITRE Corporation, 2017) from the U.S. National Vulnerability Database (NVD), detected from different VD tools, may be ranged at different risk levels. Thus, we proposed Network Risk Metric (NRM) to grade the different results from them (Hemanidhi, Chimmanee, & Sanguansat, 2012). In 2014, an additional open-source software-based VD tool, Retina, was applied. Unbiased Network Risk Evaluation (NRE) from NRM was presented (Hemanidhi, Chimmanee & Sanguansat, 2014). Later, with the original idea of "the same network infrastructure may have different IT risks depending on its attractive value", the authors introduced the Risk Environment (RE) and the Cyber Risk Evaluation (CRE) framework based on military operation, which were compiled from the integration of NRM and RE (Hemanidhi, Chimmanee & Kimpan, 2015). This paper presented only an abstract idea of the framework. Lastly, isolating from any standard, the authors demonstrated two case studies of the CRE framework (Hemanidhi, Chimmanee, Sanguansat & Nuchampun, 2015). Summary of previous works and literature reviews about IT security, Vulnerability Analysis, Risk management/assessment standards, and related articles are briefed in Table 1.

Table 1

Summary of Previous Works and Literature Reviews about IT Security, Vulnerability Analysis, Risk Management/Assessment Standards, and Related Articles

Domains	**Topics**	**References**	**Contributions/Explanations**
Vulnerability analysis	ITU-T X.805	(Cho et al., 2005)	Vulnerability analysis method for developing security framework of NGN infrastructure and services.
Vulnerability analysis	CVSS Version 2.0 (Supersedes CVSS v1.0:2004)	(Mell et al., 2007)	A complete guide to the CVSS Version 2.0, an open framework for communicating the characteristics and impacts of IT vulnerability.

(continued)

Domains	Topics	References	Contributions/Explanations
Risk management	Enterprise level IT risk management (Basis of enterprise risk assessment model)	(Aziz and Hashim, 2008)	Presents a framework that organizes IT risks into five categories: infrastructure development and support, operations and maintenance of business process, office level support, software development, and outsourcing management.
IT security	ISO/IEC 27004:2009	(ISO/IEC, 2009)	Information security management - measurement
Risk management	ISO/IEC 31000:2009	(ISO/IEC, 2009)	Risk management - principles and guidelines
Vulnerability analysis	Fuzzy heuristic design for diagnosis of web-based vulnerabilities	(Subramanian et al., 2009)	Proves that appropriate metrics are needed to grade the various vulnerabilities from different scanners.
IT security	ISO/IEC 27003:2010	(ISO/IEC, 2010)	ISMS implementation guidance
IT security	Automatic security analysis system using security metrics	(Sun et al., 2010)	Security metric collection, management, and visualization for scalable and automatic security analysis. Four critical metrics are described: service, location, role, and asset.
Vulnerability analysis	Fuzzy classification metrics for scanner assessment and vulnerability reporting	(Loh et al., 2010)	Metrics for web application scanner assessment and vulnerability reporting.

Table 1

Summary of Previous Works and Literature Reviews about IT Security, Vulnerability Analysis, Risk Management/Assessment Standards, and Related Articles

Domains	Topics	References	Contributions/Explanations
IT security	Security metrics: A brief survey	(Purboyo et al., 2011)	Identifies many open problems in security metrics area.

(continued)

Domains	Topics	References	Contributions/Explanations
IT security and risk management	ISO/IEC 27005:2011 (Supersedes ISO/IEC 27005:2008)	(ISO/IEC, 2011)	Information security risk management
Vulnerability analysis	NetClarity auditor and Nessus comparison for vulnerability detection on Rangsit university network	(Veeraprasit et al., 2012)	Compares performance of hardware-based and software-based vulnerability detection tools upon network of an educational institution.
Vulnerability analysis	A performance comparison of VD between NetClarity auditor and open source Nessus	(Chimmanee et al., 2012)	Compares performance of two VD tools in 3 categories: searching ability, scanning time and the ability of detection.
IT security and risk management	COBIT 5	(ISACA, 2012)	A business framework for the governance and management of enterprise IT.
Risk management	NIST SP 800-30rev1 (Revision 1)	(NIST, 2012)	Guidance for conducting risk assessment of federal information systems and organizations.
Risk management	Risk evaluation by VD tools for IT Department of the Royal Thai Army	(Hemanidhi et al., 2012)	Proposed unbiasedly Network Risk Evaluation (NRE) to a military IT unit.
IT security	ISO/IEC 27001:2013 (Supersedes ISO/IEC 27001:2005)	(ISO/IEC, 2013)	ISMS - Requirements
IT security	ISO/IEC 27002:2013 (Supersedes ISO 27002:2005)	(ISO/IEC, 2013)	Code of practice for information security management
Risk management	Network Risk Evaluation from security metric of vulnerability detection tools	(Hemanidhi et al., 2014)	Introduced NRM for grading distinctive results of various vulnerability detection tools. The outcome is an unbiased NRE for overall network.
Risk management	Cyber Risk Evaluation (CRE) framework based on risk environment of military operation	(Hemanidhi et al., 2015)	Proposed new idea of risk evaluation under military operation environment. Methodology concept is loosely designed.

(continued)

Domains	Topics	References	Contributions/Explanations
IT security	ISO/IEC 27000-Series (ISO27k) (4th ed.) (Supersedes ISO/IEC 27000 (3rd ed.):2014)	(ISO/IEC, 2016)	ISMS - Overview and vocabulary *The first standard of this series is ISO/IEC 17799:2000
IT security	ISO 27799:2016 (Supersedes ISO 27799:2008)	(ISO, 2016)	Health informatics - Information security management in health using ISO/IEC 27002

NETWORK CENTRIC WARFARE (NCW), MILITARY OPERATION AND OTHER TOPICS RELATED TO CYBER WARFARE

It is not only the U.S. that is awake about the new form of war in cyberspace domain. After the cyberattack on Estonia in April 2007, the North Atlantic Treaty Organization (NATO) has become a conscious region started to prepare for the possibility of forthcoming cyberwar. The Science and Technology Committee (STC) of the NATO Parliamentary Assembly have continuously managed to conduct conferences on cyber security matter since 2009. On November 23, 2014, the STC stated that cyber security is a crucial international concern. The STC pointed out the wide divergence of cyber security capabilities among their members. Attacking on allies with weak cyber security capabilities can lead to severe effects on all nations. The NATO defense planning process is developing an integration of cyber defense capabilities among their members (Vitel, 2014). In fact, it is hard to demarcate the boundary of cyberwar, cyberterrorism, and cybercrime. Ophardt (2010) pointed out that cyberwar is challenging the traditional concepts of territory. Cyber aggression by non-state collective actors could turn into sociological cybercrime or cyberwar. The International Criminal Court (ICC) should be part of a solution to address these cyber threats and the new international legal framework must consider the power of sociological forces in cyberspace. Critical examples of cyber warfare are as follows.

Supervisory Control and Data Acquisition (SCADA)

Traditionally, SCADA is implemented to manage Power/Nuclear Plants. On December 22, 2014, the Wall Street Journal reported that computers at South Korea's nuclear-plant operator of the Korea Hydro & Nuclear Power Co Ltd. (KHNP) had been hacked since December 15, 2014 (Kwaak, 2014). The

U.S. not only accused North Korea for this cyber attack but also the previous hacking of the Sony Picture Entertainment earlier in November, 2014. Even if these circumstances remain unclear but main digital evidences pointed to North Korea, which admitted to forming a hacker team. The U.S. and South Korea need to observe North Korea's cyberwarfare capabilities seriously since them. This is a clear example that cyber warfare incidents threaten the national security of a state.

Online Social Networks (OSNs)

In the last decade, Thailand was confronted with waves of political difficulties that led to tremendous political changes. Social networks have been utilized by various groups to gain both tangible and intangible power from human assets. The Royal Thai Ministry of Defense is a core executive of the Council of Ministers that needs to cooperate with the government to cease protestors' intimidated activities. The Royal Thai Armed Forces found itself in a cumbersome status of how to manage the balance between the stability of the government and the liberty of the Thai citizens in a democracy. Notwithstanding, many websites and networks of the Royal Thai Armed Forces became cyber attacking targets (from various groups of protestors) via the Internet.

Thailand has 28 million Facebook users (the 9th position worldwide). Yet another 30 million LINE users rank Thailand as the 2nd LINE community in the world after Japan. From the Thailand Internet user profile 2015 (ETDA, 2015), 81.2% of Thai people access the Internet via smart phones 5.7 hours a day and 82.7% of smart phone use is for communication over famous social networks such as Facebook (92.1%) and LINE (85.1%). Sharing information through the social media in Thailand is extremely quick. Therefore, information operation and cyberwar via social network on mobile devices are critical in Thailand. According to Singer (2015), ISIS uses the social media as a weapon. Protestors in Thailand use OSNs to share information against the government. At any stage, it is possible that terrorists could impersonate themselves as members of protestors and mislead the group into their courses. Thus, OSNs gain implicit cyber power to menace the national security. The contribution of the proposed framework is displayed by its capabilities in assessing cyber risk from the cognitive and information domains of NCW. Summary of the literature review about NCW, Military Operation, and other topics related to cyber warfare are in Table 2.

Table 2

Summary of the Literature Reviews about Network Centric Warfare (NCW), Military Operation, and Other Topics Related to Cyber Warfare

Domains	Topics	References	Contributions/Explanations
Military	FM 34-130	(DOA, 1994)	Intelligence preparation of the battlefield. The battlefield environment, effects and threat evaluation are defined.
Network centric	Network Centric Warfare (NCW)	(DOD, 2003)	Description of NCW and its three domains: Physical, information and cognitive.
Cyber	Cyber warfare and the crime of aggression	(Ophardt, 2010)	The need for individual accountability on future battlefields.
Military	JP 3-0 (Joint operation)	(DOD, 2011)	Guidelines for the Armed Forces in joint operations across the range of military operation. 3 levels of war are described including strategic, operational and tactical level.
Cyber	Cyber warfare	(Andress & Winterfeld, 2011)	Techniques, tactics and tools for security practitioners.
Cyber	Revisiting the Estonian cyber attacks: Digital threats and multinational.	(Herzog et al., 2011)	A summation of the cyberattacks on Estonia in April and May 2007 by digital activists.
SCADA	Stuxnet worm impact on industrial cyber-physical system security	(Karnouskos, 2011)	Investigation on the Stuxnet worm which could be used as a potential cyber weapon targeting to attack critical system infrastructures, e.g. SCADA.
Military	ADRP 3-0	(DOA, 2012)	Unified land operations. Description of the army operational concept and combat power.

(continued)

Domains	Topics	References	Contributions/Explanations
Information operation	FM 3-13	(DOA, 2013)	Inform and influence activities. Information environment is described and categorized into 3 dimensions of NCW.
SCADA	The real story of Stuxnet [Online]	(Kushner, 2013)	Cyber worm designed to modify the execution code in PLCs of the Siemens SCADA systems.
Cyber	Cyber space and Euro-Atlantic security	(Vitel, 2014)	Informing concern of cyber threats against all countries that rely heavily on computer networks and systems.

Table 2

Summary of the Literature Reviews about Network Centric Warfare (NCW), Military Operation, and other Topics Related to Cyber Warfare

Domains	Topics	References	Contributions/Explanations
Cyber	Joint publication 3-13 (Incorporating change 1)	(DOD, 2014)	Information operations: Cyberspace is identified as a global domain and recognized as a new military battlefield.
SCADA	South Korea Nuclear Plant Operator Hacked [Online]	(Kwaak, 2014)	Critical cyber attacking that threatens the national cyber security.
Cyber	Cyber risk evaluation (CRE) framework for network centric warfare	Hemanidhi et. al., 2015)	Introduced CRE that integrates risks from NRM and RE together. No risk management standards are applied.
SCADA	NIST SP 800-82rev2 (Revision 2)	(NIST, 2015)	Guide to Industrial Control Systems (ICS) security including SCADA Systems
OSNs	Terror on twitter: How ISIS is taking war to social media and social media is fighting back	(Singer et al., 2015)	OSNs as potential weapons for terrorist.
SCADA	A review of cyber security risk assessment methods for SCADA systems	(Cherdantseva et al., 2016)	Twenty-four risk assessment methods developed for or applied in the context of a SCADA system.

PROPOSED FRAMEWORK

This paper presents a novel conceptual framework called "Cyber Risk Assessment (CRA)" which applied the mixed research method as explained by Creswell (2014). This framework was vertically divided into 2 major parts: Network Risk Evaluation (NRE) and Military Risk Evaluation (MRE). In the first part, quantitative data from NRE was analyzed from the vulnerability scanning of various VD tools using the testing and examination methodology. In the second part, qualitative data from MRE was gathered from discussions of military professionals and IT/Cyber specialists using the focus group methodology. Full details of this research methodology are described in the next section. This framework was designed with respect to the ISO 31000:2009 standard, therefore, both NRE and MRE were horizontally differentiated into 3 phases including cyber risk identification, cyber risk analysis, and cyber risk evaluation. The entire conceptual CRA framework is shown in Figure 1. Quantitative data from NRE is the upper part while qualitative data from MRE is the lower part.

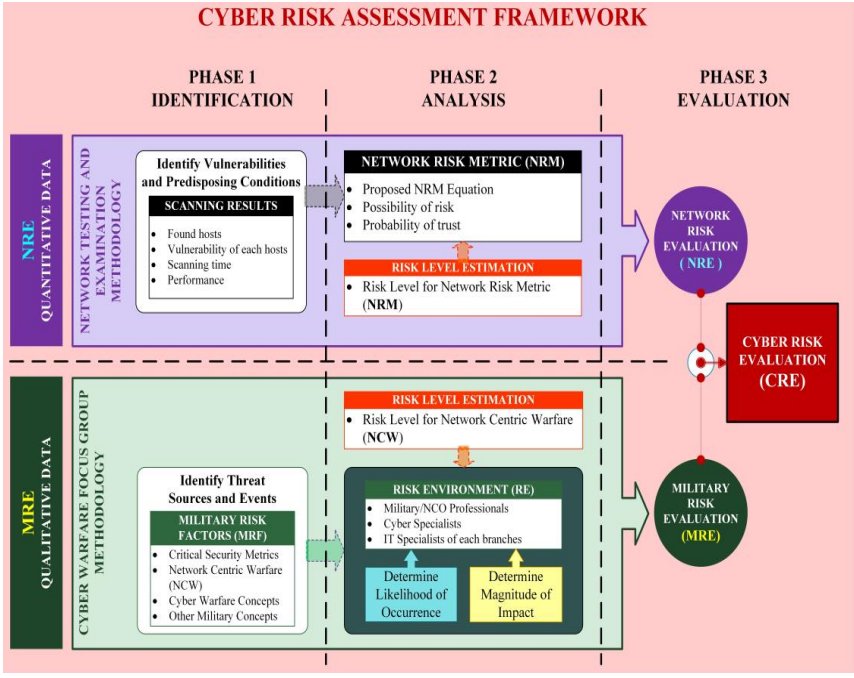

Figure 1. Cyber risk assessment (CRA) conceptual framework.

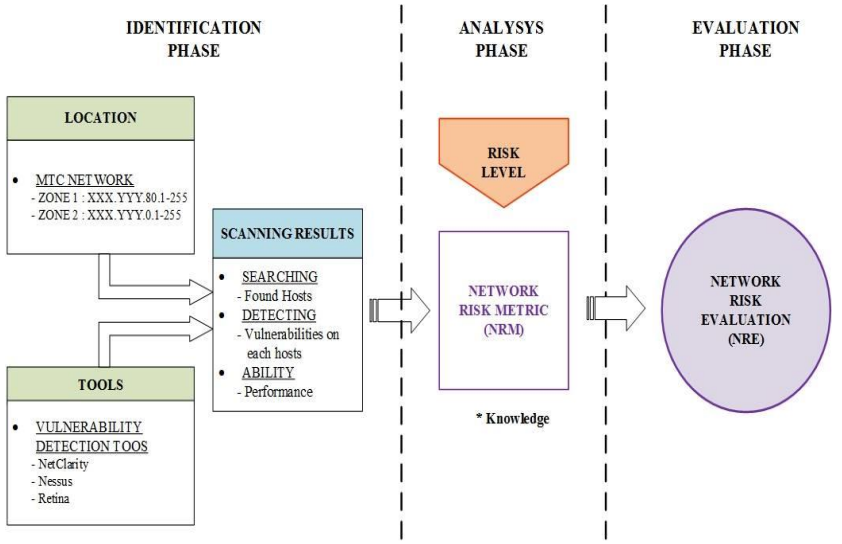

Figure 2. Network risk evaluation (NRE) concept.

PART 1: NETWORK RISK EVALUATION (NRE)

As mentioned above, each major part will be separated into 3 phases including cyber risk identification, analysis and evaluation. The general concept of NRE is shown in Figure 2.

NRE Phase 1: Cyber Risk Identification

Basically, risk identification is to identify risks from the sources, targets, events, causes and potential consequences. It would include identification of assets, threats, existing controls, vulnerabilities and consequences. There are several types of vulnerabilities, for instance, vulnerabilities from the strategic level (policy, plan, procedure, and so on), human vulnerability (training, awareness, responsibilities, and so on), vulnerabilities from techniques and physical vulnerabilities. In the first phase of NRE, we focused on technical vulnerability identification because it is the most prominent technique that many organizations choose to scan their networks and vulnerabilities of each host. It consists of two factors: location and tools as shown in Figure 2. Location represents the network where several VD tools are implemented. Tools are types of vulnerability detection, e.g. NetClarity, Nessus and Retina. The main purpose of this phase was to identify hosts and their vulnerabilities.

NRE Phase 2: Cyber Risk Analysis

In this phase, scanning results from phase 1, including the number of found hosts and vulnerabilities of each host, were graded through a mathematical algorithm called "Network Risk Metric (NRM). NRM was proposed for non-biased network risk evaluation of the overall network from various VD tools. The outcomes of the NRM were inputs for NRE in the cyber risk evaluation phase. Note that, from our perspective, types of network equipment have different levels of attraction to attackers. In this article, only generic ideas and algorithms are addressed by the following Eq. (1-5). Full explanation and examples of NRM can be found in our previous article at IEEE ACDT 2015 publication (Hemanidhi et al., 2014).

Differentiate Server-Client Risk

There were 5 steps in this phase. We differentiated computers of the network into two groups: server (*s*) and client (*c*). More groups are possible depending on classification of the network administrator. The "Cut-off" value *f* to limit diffusion of data was calculate from Eq. (1).

$$f_{s,c} = \frac{\sum_{i \in s,c} \sum_{l=1}^{L} n_{i,l}}{LH_{s,c}} \tag{1}$$

where L is the number of risk level, $i \in \{Server(s), Client(c)\}$, and $n_{i,l}$ is number (value) of detected vulnerabilities in each risk level *l.* Four risk levels identified by NetClarity were applied including low, medium, high and serious/ critical. Definition of each risk level can be found in the NACwall appliances user guide (NetClarity, 2011). Then we normalized all detected vulnerabilities of each risk level by appropriate cut-offs. The new "Cut-off Normalize Table" was then created from Eq. (2) as follows,

$$\bar{n}_{i,l}^{(s,c)} = \begin{cases} ln_{i,l} & , n_{i,l} \leq f_i \\ lf_{s,c} & , n_{i,l} \leq f_i \end{cases} \tag{2}$$

Then, $\bar{n}_{i,l}^{(s)}$ and $\bar{n}_{i,l}^{(c)}$ was weighted by weighted value (ω_L) in which L = *{Serious(4), High(3), Medium(2), Low(1)}*. The new weighted value of vulnerability for each server host $\acute{n}_{i,l}^{(s)}$ and client host $\acute{n}_{i,l}^{(c)}$ was derived from Eq. (3) as follows:

$$n'^{(s,c)}_{i.l} = \omega_L \times \bar{n}^{(s,c)}_{i.l} \tag{3}$$

The outcome was the new weighted value of vulnerability for each group. The new "Weighted Normalized Table" was then created. The normalized risk for server $R_i^{(s)}$ and client $R_i^{(c)}$ was calculated from Eq. (4).

$$R_i^{(s,c)} = \frac{\sum_{l=1}^{L} n'_{i.l}}{\sum_{l=1}^{L} l \cdot f_i} \times 100 \quad (4)$$

The relative risk for server group and client group ($\overline{R}_{s,c}$) was estimated from Eq. (5).

$$\overline{R}_{s,c} = \frac{\sum_{i \in s,c} R_i^{(s,c)}}{H_c} \quad (5)$$

These relative risks were initial values to evaluate the mean of overall risk for each type of host.

NRE Phase 3: Cyber Risk Evaluation

Finally, in the last phase of NRE, products from NRM were graded through Eq. (6-8). The neutral risk evaluation from various VD tools was invited. The first step of this phase was to find the "Probability of Trust", $P_{i,j}(T)$, which is related to the ratio of the detected host's type. Its simple equation is shown in Eq. (6).

$$P(T)_{i,j} = \frac{H_i}{\sum_{\forall i,j} H_{i,j}} \quad (6)$$

; $i \in \{s,c\}$ and $j \in \{NetClarity, Nessus, Ratina\}$

Then we offered the "Possibility of Risk", $P(R)_{i,j}$, which detected those vulnerabilities that might be exploited. This was made by applying the "Probability of trust" to the relative risk of the server and the client as shown in Eq. (7).

$$P(R)_{i,j} = \overline{R}_{i,j} \times P_{i,j}(T) \quad (7)$$

Finally, the "Total estimated risk", for each type of host, in percentage, was calculated by adding all possibilities of risk together as shown in Eq. (8).

$$Total\ estimated\ risk\ (\%)^{(s,c)} = \sum P(R)_{i,j} \times 100 \quad (8)$$

The total estimated risk represents the final overall risk for each type of host from our proposed "Network Risk Metric (NRM)". This is our "Network Risk Evaluation (NRE)" which is not biased to any vendor or standard institution.

PART 2: MILITARY RISK EVALUATION (MRE)

To evaluate risk in the military perspective, it is important to understand the basic background of military operation and its related topics. In the Cyberwar and the NCW concept (DOD, 2003), there were 5 war-fighting domains including land, sea (maritime), air, space and cyberspace. The first four domains could be considered as physical domains since military objects could be specified by location, direction, distance, weight, size, and so on. However, the fifth domain, cyberspace, is a global domain within the information environment comprising the interdependent network of information technology infrastructures, including the Internet, telecommunication networks, computer systems and embedded processors and controllers (Andress & Winterfeld, 2011). This domain is very extensive covering both physical and logical factors. Theories, strategies, doctrines and tactics that shape the domain and cyberwar are really needed. The general concept of MRE is shown in Figure 3.

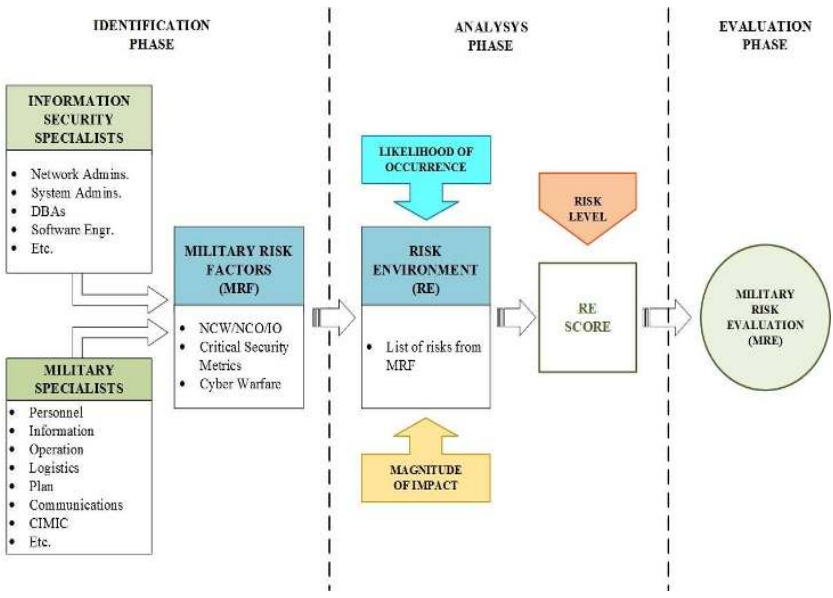

Figure 3. Military risk evaluation (MRE) concept.

MRE Phase 1: Cyber Risk Identification (Military Risk Factor: MRF)

In the first phase of MRE, Cyber Risk Identification, risk factors and their related consequences subjected to military operation must be identified. To obtain this information, in-depth interviewing with military professionals and information security specialists are motivated. The outcome is called "Military Risk Factors (MRF)" which could send significant affects to military cyber warfare. Contents of MRF are categorized and filled into an appropriate cell of the crossed table between NCW domains and criticality in security metric. Four criteria of criticality in security metric (Sun et al., 2010) including service, location, role and asset lie in rows. Three key domains of NCW (DOD, 2003), including physical, information and cognitive are in columns. The contents of MRF are shown in Table 3.

Table 3

Military Risk Factor (MRF) from Critical Security Metric and Network Centric Warfare (NCW) Integration

	Physical	**Information**	**Cognitive**
Service	Government Private sector Military	Protocol system Social media	Intention, spirit, awareness, health, concern, believe, training, etc.
Location	Land, maritime air, space, mobile	Network Cyberspace	Goal, target, direction surveillance, recon-naissance, etc.
Role	Defensive Offensive	Monitoring, collecting, creating, processing, storing, sharing, exchanging	Chain of command, command and control, leadership, unity, process, defense, attack
Asset	Personnel, hardware, network infrastructure	Software Intellectual properties	Doctrine, tactics, knowledge, experience, etc.

MRE Phase 2: Cyber Risk Analysis (Risk Environment: RE)

The second phase of MRE, from ISO 31000:2009 (ISO/IEC, 2009), each risk incident based on MRF from the first phase was scored based on their likelihood of occurrence and magnitude of impact. Firstly, the focus group, composed of military/NCW professionals and IT/Cyber specialists, was

motivated. Secondly, each risk incident was rearranged into a 3x4 table called "Risk Environment" (RE) matrix as shown in Figure 4. Note that, the RE matrix has the same structure of the MRF table in which 4 criteria of criticality in security metric lie in rows while 3 domains of information environment in the NCW are in columns. Lastly, the focus group discussed each incident in details and quoted the score of each incident applied with the risk level in Table 5. For example, if we want to analyze risk environment of a military network affected by the public electric service infrastructure in a state of cyberwar, within the Location-Physical cell, the risk level would be analyzed from likelihood and impact if related the land location of electric plants is physically attacked. Risk Environment subjected to the MRF was considered under the likelihood of occurrence and the magnitude of impact. More explanations about RE Matrix and risk level are as follows.

Impact \ Likelihood		Physical		Information		Cognitive	
Risk Environment (RE)		Likelihood		Likelihood		Likelihood	
	Service	Impact	*Government Private Sector Military*	Impact	*Protocol System Social Media*	Impact	*Intention, Spirit, Awareness, Health, Concern, Believe, Training, etc.*
	Location	Impact	*Land, Maritime Air, Space, Mobile*	Impact	*Network Cyberspace*	Impact	*Goal, Target, Direction Surveillance, Reconnaissance, etc.*
	Role	Impact	*Defensive Offensive*	Impact	*Monitoring, Collecting, Creating, Processing, Storing, Sharing, Exchanging*	Impact	*Chain of Command, Command and Control, Leadership, Unity, Process, Defense, Attack*
	Asset	Impact	*Personnel, Hardware, Network Infrastructure*	Impact	*Software Intellectual Properties*	Impact	*Doctrine, Tactics, Knowledge, Experience, etc.*

Figure 4. Risk environment (RE) matrix subjected to likelihood of occurrence and magnitude of impact.

For each incident, relevant vulnerabilities and their corresponding threats were considered. The appropriate row was identified by the risk environment impact while the column was identified by the likelihood of the threat incident. Table 4 is for mapping MRF with the likelihood of occurrence and the magnitude of impact against RE.

Table 4

Likelihood and Impact on Risk Environment (RE)

Likelihood and Impact on Risk Environment		Likelihood of incident				
		Normal (0)	Low (1)	Medium (2)	High (3)	Very High (4)
Risk Environment Impact	Normal (0)	0	1	2	3	4
	Low (1)	1	2	3	4	5
	Medium (2)	2	3	4	5	6
	High (3)	3	4	5	6	7
	Very High (4)	4	5	6	7	8

Each risk result was measured on a scale of 0 to 8 that was evaluated against the risk acceptance criteria. It was mapped to the overall risk rating as described in Table 5.

Table 5

Risk Level of Risk Environment (RE) for Network Centric Warfare (NCW)

Risk Level	Description
Normal (0-1)	Less important impacted environment – no unusual activity exists beyond the normal concern or no damage to the network centric domain, i.e. normal probing of the network, low risk viruses.
Low (2)	Slightly more important than a low-level impacted environment. The potential exists for malicious cyber activities. No significant impact has occurred.
Medium (3-5)	Significant risk due to increased hacking, virus, or other malicious activity in cyber environment which compromises systems or diminishes service. For example, important vulnerability that may be easy to exploit and allow an attacker to cause serious damage to the network. Significant impacts could happen within the cyber environment of NCW.
High (6)	High risk of increased hacking, virus or other malicious cyber activity which targets or compromises core infrastructure, causes multiple service outages, multiple system compromises or compromises critical infrastructure. High level of damage or disruption or potential for severe damage within the cyber environment of NCW
Severe/ Critical (7-8)	Severe risk of hacking, virus or other malicious activity resulting in wide-spread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors. Severe level or wide spread level of damage or disruption of critical infrastructure assets. Severe impacts to the cyber environment of NCW.

MRE Phase 3: Cyber Risk Evaluation

From the previous cyber risk analysis phase, scoring of risk incidents in RE Matrix was evaluated in 2 steps. The first one was to find the average of all available REs from each domain (column) of the NCW. Was possible that the scoring value of some cells in the RE matrix remain "NIL" rather than "Zero". The second step was to find the mean of all three results from the first step. Let RE be an *m* x *n* matrix in which *m* represents 4 members of the critical security metrics and *n* represents 3 members of the NCW. Therefore, RE is a 3 x 4 matrix by nature. The definition of RE matrix is defined with Eq. (9).

$$RE = \left(re_{i,j}\right)_{m*n} \tag{9}$$

; $re_{i,j}$ *is the entry, the i*-th row *j*-th column of the RE matrix

; $m = |\{Service, Location, Role, Asset\}| = 4$

; and $n = |\{physical, information, cognitive\}| = 3$

In the first stage, the average of each NCW domains (av_j) was calculated from Eq. (10).

$$av_j = \left(\frac{1}{l}\right) * \sum_{i=1}^{m} \left(re_{i,j}\right) \text{where } re_{i,j} \neq NIL \tag{10}$$

; $l = |re_{i,j}|$ where $re_{i,j} \neq NIL$

MRE is the mean of the three NCW domains from the second stage as shown in Eq. (11).

$$\text{MRE} = \left(\frac{1}{n}\right) * \sum_{k=1}^{n} (av_k) \tag{11}$$

; $k \in \{physical, information, cognitive\}$

Finally, the Cyber Risk Evaluation (CRE) is the mean between the NRE and MRE. It should be noted that, although NRM and RE were evaluated separately, their outcomes were integrated in the CRE phase for the concluding result. NRM was evaluated by a mathematical equation called NRE. RE was evaluated from the average of risk levels from the likelihood of occurrence and magnitude of impact from the cyber risk analysis phase.

METHODOLOGY

This research used the mixed-method approaches by procedures of the overall purposed framework. It is the integration of quantitative data using the Vulnerability Assessment (VA) from NRE (previous proposed study) and quantitative data using the focus group from MRE which is the proposed method in this article. Three methods were used to gather the outcome of each major step: (a) experiment, (b) in-depth interview, and (c) focus groups.

Quantitative Methodology: Experiment

In our previous work, NRE was collected from two former phases, identification and analysis. These was done by applying a real experiment to the target networks. In NIST SP 800-115 (NIST, 2008), there are three types of information security assessment methods including testing, examination and interviewing. In the identification phase, VD tools were connected to test all target networks for hosts and vulnerabilities scanning. In the analysis phase, testing outcome from the first phase was examined by NRM and a series of mathematical equations which were already notified in our previous work. In short, quantitative methodology from experimental designs (Creswell, 2014, P.41) were used to evaluate network risk by applying network testing and the examination approach (NIST, 2008).

Qualitative Methodology: Best Practice with In-Depth Interviewing and Focus Group

To evaluate military risk in cyber warfare, the qualitative method is more suitable for data inquiry. Two approaches of qualitative methodologies were selected.

Standard and Best Practice Review with In-Depth Interviewing

Many standards, best practices, and military publications related to information and cyber security were reviewed. The initial framework was designed with the integration of the NCW concept. Afterwards, in-depth interviewing with groups of military specialists who have knowledge in Information/Cyber System Security, NCW, and CW were employed. The interview session took place at the Royal Thai Army HQ, Bangkok, Thailand, in September 2014. It took three hours approximately. The moderator scoped topics to match the research objectives in NCW and CW. The participants quoted comments and discussed in detail openly. The summary of the knowledge from in-depth

interviewing was used to update the major contents in the initial framework, as shown in Table 6. The proposed framework is the outcome of the review of the articles and the in-depth interview.

Table 6

Phases, Questions, Quoted Comments and Topics

Phases	**Questions**	**Quoted comments**	**Topics**
Military risk identification (MRI)	How could we identify cyber threats?	From many factors that depended on sources and events, e.g. Critical Security Metrics, NCW, CW, military factors, etc.	Military risk factors (MRF)
	What are the military risks in cyberspace?	Any figure and action that could affect military operations in cyberspace (every level: strategic, operational, and tactical).	Lists of military risks in cyberspace
Military risk analysis	How could we integrate these complex data for analyzing?	Concentrate on analyzing military risks in Network Centric Warfare (NCW) domains that crossed with critical risk metrics.	Risk Environment Matrix (RE Matrix)
	What should be the most appropriate way to analyze these contents?	Some ideas of risk management standard would do. Here is ISO 31000:2009. Likelihood/Impact for each military risk in RE matrix will be scored by related specialists and professionals.	Risk Level Estimation
Military risk evaluation	How could we evaluate results from the analysis?	Total score of each cell in RE Matrix will be calculated mathematically with the proposed equations.	MRE Equations.

In the identification phase, threat sources and related environment, known as Military Risk Factors (MRF), were defined. Afterwards, they were rearranged and placed in the most appropriate cell of the RE matrix for analyzing. Significant contents on the corresponding risk acceptance criteria were initiated as shown in Table 3 of the proposed framework section. In the analysis phase, the likelihood of occurrence and the magnitude of impact for the corresponding contents in RE Metric were voted on a scale as explained in Figure 4. In this in-depth interviewing, the specialists agreed to measure the likelihood of occurrence and the magnitude of impact from 0 to 4 (normal to very high) as specified in Table 4. Then, the risk level was scaled from 0 to 8 as described in Table 5. Note that, the likelihood of occurrence, the magnitude of impact, and the risk level, could be defined as appropriate to the state of the

cyber environment concerned. Finally, in the evaluation phase, each domain of the NCW (Physical, Information, and Cognitive), subsequent to the critical risk metrics, was calculated through Eq. (9-11). The outcome of the military evaluation phase the Military Risk Evaluation (MRE). Hence, MRE and NRE from the network risk evaluation can be merged together mathematically. The mean value between MRE and NRE is Cyber Risk Evaluation (CRE) as explained in the previous section.

Focus Group

To implement this framework, two case studies were demonstrated: (a) affected from social network in Thailand and (b) affected from SCADA attack (Electricity) in Thailand. Quantitative methodology the was applied to the target network for the NRE. Then qualitative methodology using the focus group was deployed for the MRE. Experimental results are explained in the next section.

PARTICIPATION AND SAMPLING

9 specialists from government and non-government organizations participated in this study as shown in Figure 5. All of them had good background in IT/ Cyber Security, and strong knowledge in specific areas related to the research objectives as listed in Table 7.

Table 7

Participations in Specific Domain for the Focus Group Study of Cyber Risk Assessment (CRA) Conceptual Framework

Participants* **	**Experience/Knowledge in Specific Domain***									
	IT/Cyber security		**Cyber crime**		**Military/ NCW**		**SCADA**		**Social network**	
	Year	Skill**	Year	Skill**	Year	Skill**	Year	Skill**	Year	Skill**
Military Officials										
P1	5	2	5	2	10	3	2	2	5	3
P2	5	2	5	3	10	4	3	3	5	4
P3	10	4	7	3	10	5	4	3	10	4
P4	5	3	5	2	7	3	2	2	7	4
P5	10	3	5	3	7	3	3	3	7	3

(continued)

Participants***	Experience/Knowledge in Specific Domain*									
	IT/Cyber security		Cyber crime		Military/ NCW		SCADA		Social network	
	Year	Skill**	Year	Skill**	Year	Skill**	Year	Skill**	Year	Skill**
Police Officials										
P6	5	3	7	5	2	2	2	2	5	4
P7	3	3	5	5	2	2	2	2	5	4
Civilians										
P8	15	4	2	3	4	3	3	5	10	4
P9	20	4	10	2	2	2	20	5	10	3

Note. * In this paper, specific domains are SCADA and Social network.

** ***Skill: 5*** = *Excellent,* ***4*** = *Good,* ***3*** = *Median,* ***2*** = *Satisfactory, and* ***1*** = *Poor.*

*** ***P =*** *Participant*

Developing Questions

Well-known standards and best practices in information security and Enterprise Risk Management (ERM), e.g. ISO/IEC Series, NIST Series, COBIT 5 (ISACA, 2012), and COSO (Steinberg, Everson, Marten, & Nottingham, 2004), were seen to obtain questions for critical risk metrics. Military publications related to NCW and CW, e.g. Field Manual (FM) and Joint Publications (JP), were used to shape the general information security into military-based cyber security. The aims of developing questions were to guide and implicate the focus group with the research objective, and to stimulate discussion among them. Two significant outcomes from the questionnaire were then (a) to identify risks in cyberspace from multi dimensions and (b) to analyze cyber risks (likelihood and impact) and how they could affect national security in the military perspective. Examples of questions are shown in Table 8.

Table 8

Examples of Focus Group Session Questions (SCADA - Electricity)

Session Questions	Quote Comments	Risks (to target network*)	Risk Description	Code**
What are the critical risks to the SCADA system, in terms of service, that could affect national security?	*(Physical)* Control center of the SCADA network cannot maintain regular connection with its end-points, i.e. PLC, IED, RTU, etc.	Military's IT unit cannot maintain its Data Center (DC) and network service to the corresponding units. *Likelihood: 4* *Impact: 4*	Without public electricity, the power supply of the DC could prolong just for system backup and shut down safely.	*RS01*

(continued)

Session Questions	Quote Comments	Risks (to target network*)	Risk Description	Code**
What are the critical risks to the SCADA system, in terms of location, that could affect national security?	*(Information)* Telecommunication fraud. Endpoints of some SCADA sites might be tapped from attackers and could not communicate properly with the Distributed Control Server (DCS).	Military units in coincidental areas could not connect to the military DC. *Likelihood: 3* *Impact: 3*	The military C4I system is not in full control. Nevertheless, the core system is still functioning. Another communication network could compensate this risk in a level.	*RL02*
What are the critical risks to the SCADA system, in terms of role, that could affect national security?	*(Cognitive)* Significant effect on the on-going military operation, e.g. command and control system.	Military network could not support command and control system functionally. *Likelihood: 3* *Impact: 4*	Command and control play important roles in supporting commanders for decision-making. Unstable communication between the HQ and front-line base is a crucial damage.	*RR03*

Note. * The Military Technology Center Network
** ***Code: RS*** = Risk of Service, ***RL*** = Risk of Location, ***RR*** = Risk of Role, ***RA*** = Risk of Assets

Moderating

The focus group session was held in Bangkok, Thailand, in October 2015. A short briefing about cyber/information security, Network Centric Warfare (NCW), and Cyber Warfare (CW) was introduced in the beginning, followed by the significance of risk analysis and the proposed CRA conceptual framework. Two case studies, including Social Network and SCADA, were raised for cyber risk assessment. Risk incidents from the Cyber Risk Identification phase were investigated and amended. All risk incidents were scored based on their likelihood of occurrence and the magnitude of impact. Military Risk Evaluation (MRE) of both case studies were finally evaluated and integrated with Network Risk Evaluation (NRE) as designed by the proposed Cyber Risk Assessment (CRA) framework. This focus group interviewing was recorded on audio tape recorder to be transcribed later. The authors of this article are moderators and note takers of the focus group. Details of the case studies in SCADA and OSNs are way beyond this article. Therefore, they will be discoursed in future work.

Figure 5. Focus group on military based cyber risk assessment (CRA) framework for supporting cyber warfare in Thailand.

DISCUSSION ON FRAMEWORK

This article has demonstrated and proved that the proposed framework is suitable and covers all three domains of the Network Centric Warfare, namely physical, information and cognitive. Additionally, it is beneficial to the military strategy and systematic to all three levels of war in joint operations as described in Joint Publication 3-0 (DOD, 2011), including the Strategic, Operational and Tactical levels.

In the strategic level, the national cyber security community could utilize this framework as an innovative cyber risk assessment for full-scale national cyber risk management standard without lack of ICT perspectives from military services. The Royal Thai Ministry of Defense has recognized cyberspace as a military battlefield since 2015. This is the first cyber risk assessment framework proposed for national cyber security in the military perspective. In the operational level, ICT professionals, military experts and research communities can jointly learn about national cyber risks. Focus group discussion to identify and analyze cyber risks is an example of this collaboration. The outcome is best practices to secure ICT and cyber operation. This could be a great step to

enhance the cyber security rules and regulations of intermediate organizations responsible to the national cyber security globally. In the tactical/social level, subordinators and individuals will be aware of these dreadful threats through cyber security rules and regulation. ICT security baselines and/or guidelines should be provided to all members at this stage. They will learn how to use their ICT equipment properly and securely. Note that, military equipment, including vehicles, radars, and weapon systems, are commanded and controlled via ICT network infrastructure. Unlike basic ICT equipment in the data center, they are abandoned from famous ISMS standards because of their indirect impact on the business continuity. With the coming stream of cyber warfare, ISMS standards with military concerns must be seriously operated with respect to the NCW concept. This is a real critical circumstance for overall national cyber security which this proposed framework is designed with military concerns based on NCW.

CONCLUSION

IT security is very significant nowadays. Information is one of the most valuable properties that needs to be managed securely and effectively. Many information security and risk management standards are offered to provide procedures for the information system security of the organization. Risk assessment plays its crucial role as a core process in risk management. However, the thrill of dangerous cyber operation is growing continuously. Cyberspace was recognized as a new military battlefield in 2014. Cyberwar has become a new influential threat to national security. Unfortunately, current IT security and risk management standards are desired for general perspectives, especially for business continuity, rather than national security. Not only specific IT risk management standard, but also IT risk assessment methodology, is directly scoped for military operation. Therefore, this paper proposed an innovative idea of cyber risk assessment to improve national cyber security with specific intention to deliberate cyber warfare that could affect military operations. Activities on this logical domain can send significant impacts to actual the physical domain. The threat spectrum has also expanded from the basic concept to the most complicated operation. Network risk evaluation from primary standards does not fit well fit with cyber risk in military terms, hence, some risk management standards are developed for non-profit organization requirement but they do not yet consider the cyberwar environment.

In this article, we proposed a novel conceptual framework for Cyber Risk Assessment (CRA) which is well harmonized with NCW in the cyber warfare concept. With this framework, abstract notation from military risk environment

is parsed into a mathematical form that could be integrated with the technical notation from the network risk metric. The last outcome is called Cyber Risk Evaluation (CRE) subjected to a specific military environment. Our proposed CRA is now fulfilled from both quantitative and qualitative assessment. It is suitable for cyber risk assessment of both the common situation (e.g. normal activities) and uncommon condition (e.g. cyber terror and cyberwar). Risks that could significantly affect national cyber security are then investigated in-depth for the best preparation to countermeasure these terrifying threats in the future. All communities related to IT security could take the benefits of this finding from the planning processes to action. Details of both case studies in SCADA and OSNs will be elaborated in future work.

REFERENCES

Andress, J., & Winterfeld, S. (2011). *Cyber warfare: Techniques, tactics and tools for security practitioners.* USA: Syngress.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security on ScienceDirect,* 1-27.

Chimmanee, S., Veeraprasit, T., Sriphrew, K., & Hemanidhi, A. (2012). A performance comparison of vulnerability detection between NetClarity Auditor and Open Source Nessus. *Proceeding of the 3rd European Conference of Communications (ECCOM '12),* (pp. 280-285). Paris, France.

Cho, Y., Won, Y., & Cho, B. (2005). ITU-T X.805 based vulnerability analysis method for security framework of end-to-end network services. *Proceedings of the 4th WSEAS Int. Conf. on Information Security, Communications and Computers,* (pp. 228-292). Tenerife, Spain.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Thousand Oaks, CA: SAGE Publications, Inc.

Department of the Army (DOA). (2013). FM 3-13. *Inform and influence activities.* Washington DC, USA.

Department of the Army (DOA). (2012). ADRP 3-0. *Unified land operations*. Washington DC, USA.

Department of the Army (DOA). (1994). FM 34-130. *Intelligence preparation of the battlefield*. Washington DC, USA.

Department of Defense (DOD). (2003). Network-centric warfare. Washington DC, USA.: Office of the Secretary of Defense.

Department of Defense (DOD). (2006). Joint publication 3-13. *Information operations.* USA: DOD Publications.

Department of Defense (DOD). (2011). Joint publication 3-0. *Joint operations.* USA: DOD Publications.

Department of Defense (DOD) (2014). Joint publication 3-13. *Information operations*. (27 November 2012 Incorporating Change 1). USA: DOD Publications.

Electronic Transactions Development Agency (ETDA) (2015). *Thailand Internet user profile 2015.* Bangkok, Thailand: Ministry of Information and Communication Technology.

Hemanidhi, A., Chimmanee, S., & Kimpan, C. (2015). Cyber risk evaluation framework based on risk environment of military operation. *Asian Conference on Defence Technology (ACDT 2015) 2015.* (pp. 42-47). Hua Hin: doi: 10.1109/ACDT.2015.7111581

Hemanidhi, A., Chimmanee, S., & Sanguansat, P. (2012). Risk evaluation by vulnerability detection tools for IT department of the Royal Thai Army. *Proceeding of the 3rd European Conference of Communications (ECCOM '12)* (pp. 286-292). Paris, France: WSEAS Press.

Hemanidhi, A., Chimmanee, S., & Sanguansat, P. (2014). Network risk evaluation from security metric of vulnerability detection tools. *TENCON 2014 - 2014 IEEE Region 10 Conference* (pp. 1-6). Bangkok: doi:10.1109/TENCON.2014.7022358

Hemanidhi, A., Chimmanee, S., Sanguansat, P., & Nuchampun, W. (2015, November). Cyber risk evaluation framework for network centric warfare. *Journal of Converfence Information Technology (JCIT)*, 1-13.

Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational. *Journal of Strategic Security*, 49-60.

Information Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) (2014, January 1). *ISO/IEC 27000 (Information technology - Security techniques - Information security management systems - Overview and vocabulary)* (3rd ed.). Geneva: ISO/IEC.

Information Systems Audit and Control Association. (ISACA). (2012). *COBIT 5 (A business framework for the governance and management of enterprise IT).* Rolling Meadows, IL: ISACA.

International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2013). ISO/IEC 27001:2013 Information security standard. *Information security management system (ISMS).* UK: British Standard (BSi).

International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2011). ISO/IEC 27005:2011 *Information technology – Security techniques – Information security risk management* (2nd ed.). Geneva: ISO/IEC

International Organization for Standardization (ISO). (2016, Jul 1). ISO 27799:2016 *Health informatics - Information security management in health using ISO/IEC 27002* (2nd ed.). Geneva: ISO

International Organization for Standardization (ISO). (2009). ISO 31000:2009 *Risk management – Principles and guidelines.* Geneva: ISO.

Karnouskos, S. (2011). Stuxnet worm impact on industrial cyber-physical system security. *IEEE Proceeding of the 37th Annual Conference on IEEE Industrial Electronics Society (IECON 2011),* (pp. 280-285). Melbourne, Australia.

Kushner, D. (2013). IEEE SPECTRUM. *The Real Story of Stuxnet [Online]*. Retrieved from http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Kwaak, J. S. (2014). The Wall Street Journal. *South Korea nuclear plant operator hacked [Online]*. Retrieved from http://www.wsj.com/articles/south-korea-nuclear-plant-operator-hacked-1419237333

Loh, P. K. K., & Subramanian, D. (2010). Fuzzy classification metrics for scanner assessment and vulnerability reporting. *IEEE Transaction on Information Forensics and Security,* 5(4).

Mell, P., Scarfone, K., & Romanosky, S. (2007, June). *CVSS: A Complete Guide to the Common Vulnerability Scoring System Version 2.0.* Retrieved from The Forum of Incident Response and Security Teams (FIRST): https://www.first.org/cvss/v2/guide

National Institute of Standards and Technology (NIST) (2008). *NIST SPECIAL PUBLICATION 800-115 (Technical guide to information security testing and assessment).* Geithersburg, MD: Computer Security Division, Information Technology Laboratory.

National Institute of Standard and Technology (NIST) (2012). *NIST SPECIAL PUBLICATION 800-30rev1 (Information security guide for conducting risk assessments).* Gaithersburg, MD, US: Computer Security Division, Information Technology Laboratory.

National Institute of Standards and Technology (NIST) (2015*). NIST SPECIAL PUBLICATION 800-82r2* (*Guide to industrial control systems (ICS) Security).* Gaithersburg, MD: Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A.

NetClarity, Inc. (2011). *NACwall appliances user guide.* Bedford, MA, USA.

Ophardt, J. A. (2010). Cyber warfare and the crime of aggression: The need for individual accountability on tomorrow's battlefield. *Duck Law & Technology Review*, 1-28.

Singer, P., & Brooking, E. (2015, December 15). *Terror on twitter : How ISIS is taking war to social media—and social media is fighting back.* Retrieved from popular Science: http://www.popsci.com/terror-on-twitter-how-isis-is-taking-war-to-social-media

Steinberg, R.M., Everson, M. E. A., Martens, F. J., & Nottingham, L. E. (2004). *Enterprise risk management integrated framework.* USA: Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Subramanian, D., Le, H. T., & Loh, P. K. K. (2009, May 24-28). Fuzzy heuristic design for diagnosis of web-based vulnerabilities. *Fourth International Conference on internet monitoring and protection (ICIMP '09)* (pp. 103-108). Venice/Mestre: doi: 10.1109/ICIMP.2009.25.

Sun, K., Jajodia, S., Li, J., Cheng, W., Tang, W., & Singhal, A. (2010). Automatic security analysis using security metrics. *The 2011 Military Communications Conference – Track 3 – Cyber Security and Network Operations*, IEEE.

The MITRE Corporation. (1997-2017). *Common vulnerabilities and exposures*. Retrieved from Common Vulnerabilities and Exposures: https://cve.mitre.org/

Vitel, P. (2014, November 23). *Cyber space and Euro-Atlantic security.* France: Science and Technology Committee, NATO Parliamentary Assembly.