Association for Information Systems
AIS Electronic Library (AISeL)

CONF-IRM 2015 Proceedings

International Conference on Information Resources Management (CONF-IRM)

5-2015

Cyber Defense Capability Model: A Foundation Taxonomy

Farzan Kolini
The University of Auckland, f.kolini@auckland.ac.nz

Lech Janczewski
The University of Auckland, lech@auckland.ac.nz

P30. Cyber Defense Capability Model: A Foundation Taxonomy

Farzan Kolini
The University of Auckland
f.kolini@auckland.ac.nz

Lech Janczewski
The University of Auckland
l.janczewski@auckland.ac.nz

Abstract

Cyber attacks have significantly increased over the last few years, where the attackers are highly skilled, more organized and supported by other powerful actors to devise attacks towards specific targets. To aid the development of a strategic plan to defend against emerging attacks, we present a high-level taxonomy along with a cyber defense model to address the interaction and relationships between taxonomy elements. A cyber-kinetic reference model which is used widely by U.S Air Force is adopted as a baseline for the model and taxonomy development. Asset, Cyber Capability, and Preparation Process are the three high-level elements that are presented for the cyber defense capability model. The Cyber Capability, as the focal point of the study, uses three classifiers to characterize the strategic cyber defense mechanisms, which are classified by active, passive and collaborative defense. To achieve a proper cyber defense strategy, the key actors, assets and associated preparation procedure are identified. Finally, the proposed taxonomy is extensible so that additional dimensions or classifications can be added to future needs.

Keywords

Cyber Security, Cyber Defense Model, Taxonomy, Cyber Actor, Cyber Attack, and, Active Defense, and Passive Defense

1. Introduction

The expansion of cyberspace usage over the past two decades, resulted in access to the internet for almost every location on the globe (Choucri et al. 2014). Since 2000, by technological enhancement in Information Technology (IT) and improvement in internet networks, the overall number of internet users has been dramatically increased by 673 percentages to 2.8 billion users (Global Internet Report 2014). Modern societies are highly dependent on IT and notably on the internet for survival. IT and information systems will facilitate innovation, product and services, and communication for the modern economies. According to the Global IT Report, The productivity promised by ICT for some nations is estimated to reach up to 10% of their GDP by 2015 (Klimburg 2012).

Increased reliance on ICT and information systems leads to increase in emerging risks and cyber attacks. Cyber attacks are now becoming more sophisticated in terms of impact and scale. A large-scale cyber attack spreads in a matter of seconds, leading to substantial damage to individuals, corporations, and nation-states. Recently, other cyber actors such as criminals, hacktivist, whistleblowers, and cyber fighters became more engaged in the events that take place in cyberspace. However, the key dilemma for the governments and organization s is to recover from a cyber incident in a timely manner while minimizing the adverse impact. The ultimate goal for every nation is to safeguard its sovereignty, economy and critical assets against any national threat(Klimburg 2012).In order to mitigate cyber attacks, nation states need to assess their cyber capabilities and preparation procedures while identifying the key actors and the critical assets associated with them. This approach is very similar to McCumber Cube Model, which refers to confidentiality, integrity, and availability of information systems through technology, human factors and, policy and procedures (McCumber 2004).

In conjunction with McCumber's security model, this Study seeks to illustrate a model for cyber defense capability which can be used to prepare and respond to cyber threats. For this reason, the main pillars of the current study, cyber defense capability model, are derived from Cyber/Kinetic inference model, which is demonstrated by U.S Air force during the advanced course in Engineering Cyber Defense Exercise. The rest of the proposed model is based on previous studies that are relevant to this setting or covering the defense mechanisms that are already in place or would be applicable.

Moreover, the proposed model offers a new taxonomy at a strategic level to assist the users to adopt an appropriate defense strategy during cyber incidents. Although a considerable number of extant literatures proposed a tactical or operational level taxonomies to classify attacks, vulnerabilities or intrusions, to our best knowledge, this is the only study that attempts to elucidate the synergy and interaction between various cyber defense capabilities.

The paper starts by presenting the previous taxonomies on cyber attacks and defense in Section 2.The following section presented the groundwork for the taxonomy by illustrating the cyber capability reference model. Section 4 discussed the criteria for an acceptable taxonomy, while the proposed taxonomy and the breakdown of the cyber defense capabilities are discussed in Section 5. Finally, the conclusion and the future study is presented in Section 6.

2. Review of Previous Taxonomies

Fred Cohen's (1997) early work has identified 94 different computer attacks and techniques under a single classification. Although the findings could help security experts to protect computers and Information Systems (IS), the taxonomy is almost a repository or database for different kinds of attacks. Lindquist and Johnson (1997) have introduced a new concept which is called the dimension of classification which is used to classify specimens based on specific attributes. Therefore, they have suggested that all the computer attacks can be classified into two dimensions, according either the intrusion technique or intrusion result.

Howard (1998) has presented a process-based taxonomy that classified security incidents according to a series of computer attacks and events. The proposed taxonomy divided computer

attacks into five series of steps that can be taken by an attacker to compromise networks or information systems. Although the study offered a practical baseline for cyber attacks, it failed to provide enough insight towards the motives and objectives of the attacks. Hansman and Hunt (2004) suggested an overarching taxonomy that classified computer and network attacks into f attack vector, target, vulnerability and payload. Although the taxonomy can be used widely at an operational level, blended or mixed attacks such as Advances Persistent Threats (APT) cannot be categorized properly in taxonomy.

Simmons et al. (2009) suggested a cyber attack taxonomy which called AVOIDIT (Attack Vector, Operational Impact, Defense, Information Impact and Target). Distinct from the previous studies, it was able to encompass the blended attacks like Stuxnet. As a tactical taxonomy, AVOIDIT can be used by the security managers during the security management processes or in development of information security policies. In spite of the usefulness and insight, the taxonomy is not comprehensive enough to be used for high-level defense strategies that safeguard critical infrastructure against cyber threats.

Killouri et al. (2004) declared that the previous studies are mostly attack-centric taxonomies that widely can be used by the attackers rather than the system defenders. Hence, they offered a taxonomy that could predict whether an intrusion detection system (IDS) can detect all related attacks in a particular attack class. The focal point of the study was to signify that the defense-centric taxonomy offers greater benefit and flexibility for IS defenders rather than attack-centric taxonomies. Kjaerland (2005) has studied the cyber intrusions on commercial and government sectors. Kjaerland perceived attack and defense-centric taxonomies can be used as complementary to estimate the severity of attacks or the suitability of the defense controls.

Scott and Angelos (2013) proposed an extensible taxonomy that could classify events and associated impacts by demonstrating the interaction between actors, vector, and types of attacks. By using this taxonomy, the end user can cross-tabulate all cyber events that pertain to a particular actor or all the attacks that are using a similar attack vector. Understanding these relationships and links can help the end user to develop a cyber strategy program.

In much of the previous literature, security taxonomies were divided into three general categories: attack, vulnerability, and intrusions. These are subjected to be technical taxonomies which can be used at the operational level by cyber security analysts during risk assessment, mitigation, and control programs. Mirkovic and Reiher (2004) have created a taxonomy of DDOS attacks for classifying threats and defense related to DDOS. Zhu, Cebula and Young (2010) have suggested a taxonomy for attacks and vulnerabilities that target SCADA systems. Khattak, Ramay et al. (2014) have proposed a taxonomy of botnet behavior, detection and defense to classify the characteristics of the botnet threat. Hoque, Baishya et al. (2014) have presented a taxonomy of network tools and systems that could be used to conduct cyber attacks. Loukas, Gan et al. (2013) developed a taxonomy of attack and defense mechanisms that could be applied to emergency management. All these taxonomy may help the cyber defenders to understand how cyber intrusion can be triggered.

In contrast, some recent studies have attempted to illustrate a series of cyber activities, events or incidents that are relatively associated with each other, so the various categories can interact,

link, and collaborate to describe the cyber threat. These studies go beyond the context of phenomena by looking at the motivation, relationships, interaction and impacts of cyber attacks. These taxonomies can be counted for strategic taxonomies that can be called in the planning of cyber strategies (Scott and Angelos, 2013 and Uma and Padmavathi, 2013).

3. Cyber Defense Reference Model:

The U.S Air Force research laboratory has presented a cyber-kinetic reference model that can be used during cyber attacks (Mudge and Lingley 2008). This study has adopted this reference model -with slight changes in the order-to demonstrate the cyber defense capabilities (See Figure 1). We perceive that the proposed model can describe the interaction between cyber defense capabilities and preparation processes that are required to protect the assets. It is closely matched with research objectives by accommodating previous study shortcomings. First, this model can mitigate cyber attacks that end in cyber-physical loss. Second, defense capabilities are strategy-driven controls that can be called to defend or respond to cyber threats; thus the depicted model can also be used as a tool during the planning for a cyber defense strategy. Third, cyber security is achieved by interaction and synergy between capabilities, cyber processes and critical assets, which is essential to safeguard against a sophisticated blended attack. Moreover, the proposed model can provide enough insight to illustrate and respond to blended and complex cyber attacks. Furthermore, it can provide an opportunity for defenders to respond to a physical impact that is associated with a cyber attack. Figure 1 depicts the proposed cyber-kinetic reference model.

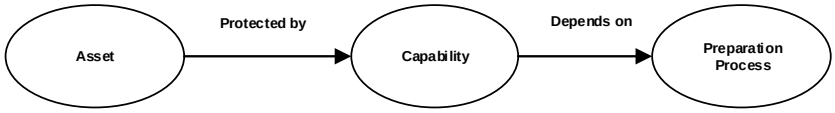

Figure 1: Cyber-Kinetic Reference Model

4. Criteria for an Acceptable Taxonomy

The requirement for an acceptable taxonomy has been demonstrated comprehensively in previous literature. Hansman and Hunt (2004), and Lindquist and Johnson (1997) enumerated several characteristics for a good taxonomy like, accepted, comprehensible, exhaustive, repeatable, unambiguous, useful and mutually exclusive.

Pertinent to taxonomy evolution, Igure et al (2008) has conducted a comprehensive survey on available taxonomies between 1984 and 2005, in contrast with the extant literature they perceived that taxonomy's classes do not need to be mutually exclusive for the following reasons. First, to produce a greater coverage. Second, a vulnerability which cannot be detected under one category might be discovered under a second category. Moreover, with the advent of blended attacks which are using multiple attack vectors, classification of a threat or vulnerability under one category cannot provide a comprehensive understanding of the links between attackers, vectors, targets and the impacts of the attack.

5. Cyber Capability Defense Model and Taxonomy

The primary objective of this study was to provide a taxonomy that could differentiate between the various types of defensive mechanisms that could be used to mitigate or respond to cyber attacks.

It also assists the users to link and transit between dimensions and sub-categories to apply appropriate defense mechanisms in order to cope with the ever-changing nature of cyber attacks. Applying an appropriate defense strategy requires the identification of all the key actors in the cyberspace. The actors are an intrinsic part of cyber incidents whether for being accountable as the attack perpetrator or assisting the attacked parties to repel or respond to cyber attacks. Therefore, unlike the previous studies, the proposed taxonomy has attempted to identify all involved players in cyberspace.

Figure 2 provides an overview of proposed taxonomy, which is divided into three distinct dimensions: asset, capability and preparation processes. Since this taxonomy is designed to be expandable, the additional dimensions or categories can be added to satisfy the future needs.

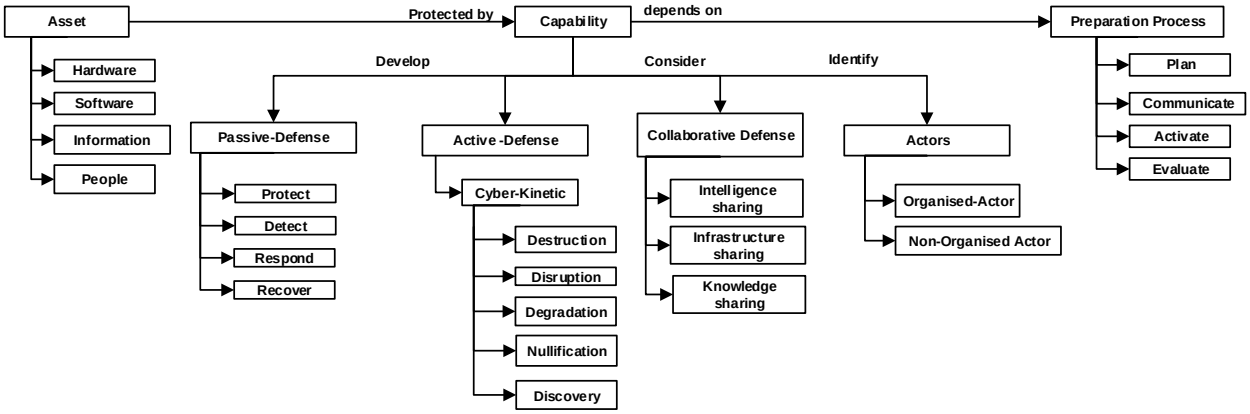

Figure 2: Cyber Capability Defense Model and Taxonomy Overview

5.1 Assets

Asset can be defined as resources valuable to governments, organizations and individuals (ISO 2012) that are related to cyberspace. Assets possess tangible or intangible value that is needed to be protected against cyber threats.

5.1.1 Hardware

A hardware asset is defined by any technological equipment that facilitates a service or value to the end users. Hardware are used to transfer, store, process, control or present the information or services to the users. Computers, network equipment, IT Infrastructure, SCADA systems and fibre cables are examples of hardware assets.

5.1.2 Software

A software asset refers to IT application, software or database that is widely used by individuals, organizations or governments.

5.1.3 Information

An information asset refers to information processed, stored and transported by internetworked information systems (ISACA 2014).

5.1.4 People

People relate to human factors of cyberspace who are often targeted as the principals of cyber attacks. People are actively interacting with cyberspace through seeking or facilitating particular services (Von Solms and Van Niekerk 2013).

5.2 Capabilities

Cyber capabilities are defined by the ability of a cyber defender to prepare, prevent, detect and respond to a cyber attack (Jordan and Hallingstad 2011).The capabilities are very complex, technical, strategic and operational abilities of a defender to confront a cyber threat. This notion requires the development of strategic tools for active and passive defense and collaboration with other key players.

5.2.1 Passive Defense (PD)

PD (See Figure 3) refers to all the measures and controls that could be used passively to protect, detect, respond and recover to the cyber threat. PD will provide a vehicle to focus on making cyber assets more resistant or resilient to cyber attacks (Denning 2014).

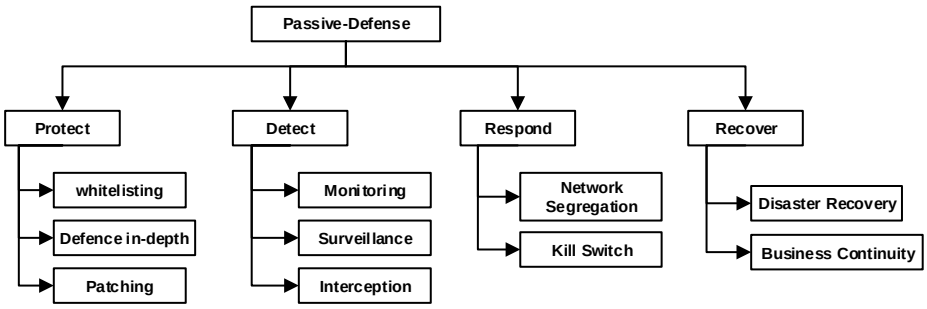

Figure 3: Passive Defense Classification

Protect

Protect refers to prepare and implement the proper safeguards to ensure the delivery of service assets (NIST, 2014). Cyber security protection can be achieved by using whitelisting techniques, defense-in-depth mechanisms or patching processes. Antivirus software, firewalls, access controls, penetration testing, audits are examples of system protection.

Detect

Detect refers to developing and implementing processes and activities to discover the occurrence of cyber events (NIST, 2014).In this stage, it is assumed that an undesirable event has happened in our systems. Detection can be achieved through monitoring and surveillance mechanisms or technologies. Intrusion Detection Systems (IDSs), Security Incident Event Management (SIEM), data and voice surveillance are techniques and technologies that can be applied for this purpose.

Respond
Respond refers to developing and implementing the activities to respond to a detected cyber event (NIST, 2014).A successful response will contain the effect and impact of cyber attack. For instance, Network segregation and Internet kill switch are the technical solutions; often by autocratic governments; to respond or to mitigate the severe impact of cyber threats.

Recover
Recovery refers to developing and implementing activities or processes that restore the compromised or degraded services to its normal operation (NIST, 2014).Business continuity and Disaster recovery are the programs that can be used to minimize the disruptive effect of cyber incidents.

5.2.2 Active Defense (AD)
AD(See Figure 4) refers to a real-time capability to minimize the impact of the cyber attacks (Rosenweig, 2014). AD may use some types of offensive ability to discover, destruct, disrupt, degrade or nullify incoming cyber threats. Denning (2014) perceived that all of the safeguards in AD are analogous to air and missile defense aims to shoot down or deflect the attacker's missile or rocket.

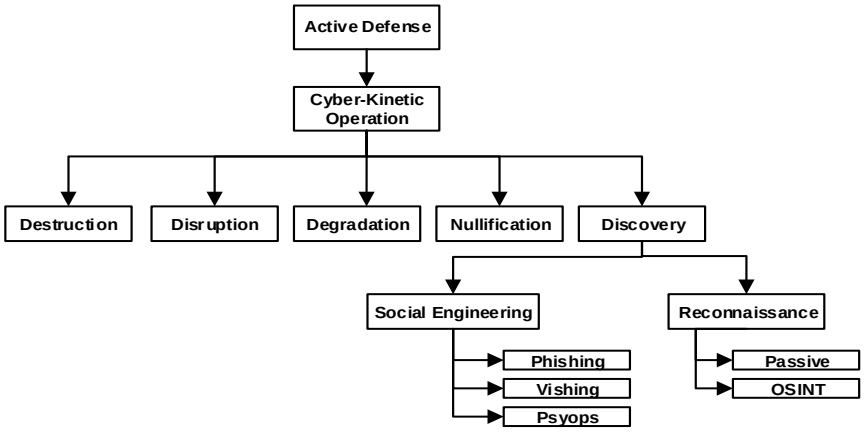

Figure 4: Active Defense Classification

Cyber-Kinetic (Cyber Adjunct to Kinetic) Operation:
The intent of cyber-kinetic is to defend against kinetic effects of cyber attacks through an active defense operation. Cyber adjunct to kinetic operation can be classified as the following:

- Destruction- Destruction occurs when the IT hardware or equipment is modified from their original stage; hence the damaged devices are malfunctioned or not function properly. s. Stuxnet worm, Siberian pipeline sabotage or operation Orchard are examples of destruction operation by means of cyber kinetic capabilities (Clarke and Knake 2011).
- Disruption- Disruption refers to a kind of denial of service or unauthorised usage of resources in which the target's resources are fully exhausted, consumed or unavailable to the legitimate users.
- Degradation- Degradation of service occurs when the required services are falling outside predetermined service level, so the legitimate user will experience the lower quality of service (QOS).

- Nullification- Nullification refers to the ability of an entity to nullify a cyber attack by using electronic or cyber capability (Andress and Winterfeld 2011).
- Discovery- Discovery is the ability of an entity to discover valuable information about the target from various sources. Social engineering and Reconnaissance are the methods that can control human behaviour to acquire useful information about a prospective target. Phishing, Vishing, Psychological operation (Psyops) and Open source Intelligence (OSINT)) are the common types of discovery operation.

5.2.3 Collaborative Defense

Collaborative defense, see Figure 4, is the ability of a defender to rely on the support of organizations, international bodies or other nations to stop a cyber attack. Collaborative defense can be achieved by operational cooperation of different actors against a common cyber event. (Klimburg 2012)

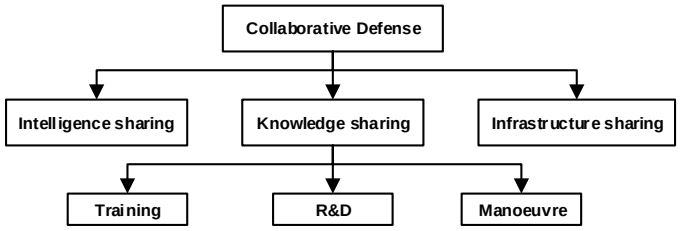

Figure 5: Collaborative Defense Classification

Intelligence Sharing

Intelligence refers to the collected information that are analysed and contextualized; so it can be used by policy makers for efficient decision-making on matters of interest. Intelligence sharing can be an asymmetric operation that one party may share more information than their counterparts. It also helps involved parties to achieve superiority in cyberspace (Rovner, Mahoney et al. 2013). Echelon operation, Magic Lantern and Five Eye (FVEY) operations are sitting in this setting (Andress and Winterfeld 2011, Janczewski 2014).

Infrastructure Sharing

Infrastructure sharing is a strategy that used to share infrastructure to drive innovation, reducing the cost and increasing the security safeguards (Hathaway 2014).

Knowledge Sharing

Knowledge sharing programs can help cyber allies to achieve higher skills and experiences. Cyber coalitions can exchange their knowledge and experiences in training and awareness programs, research and development projects, and cyber exercises. The US Cyber Storm III exercise and NATO Cyber Sea maneuver are falling into this section (Klimburg 2012).

5.2.3 Actors

Actors are the entities that are interacting and participating in cyber activities (See Figure 6).

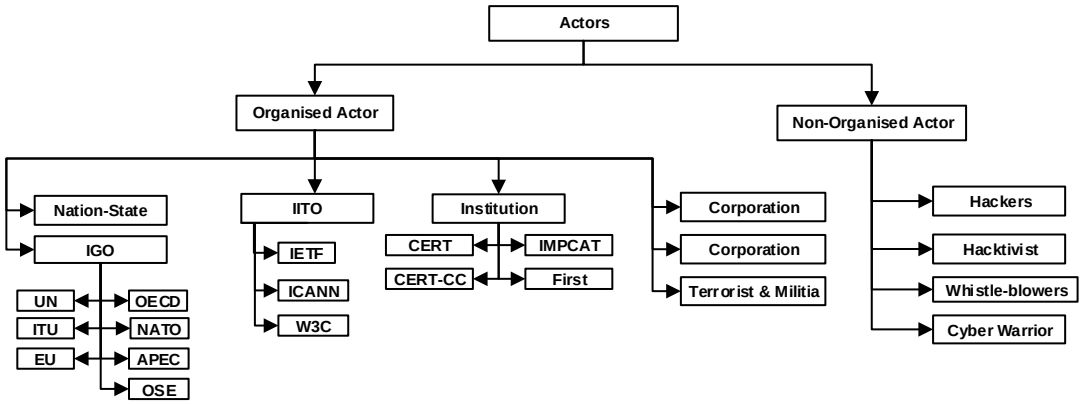

Figure 6: Actor Classification

Organized Actor

Any actors with a basic command structure, resources, funds, vision and objectives are counted as organized actors (Bruderlein 2000).

- Intergovernmental Organization (IGO) - Many IGOs (see Table 1) are focusing on international cyber security issues. IGOs vary significantly in size, scope, expertise and legitimacy (Kahn, McConnell et al. 2011).

IGOs	Liability	Cyber Activity	Members
United Nations (UN)	International treaty based with legal authority	Policy maker , Disputes, and Reports	193 countries
International Telecommunication Union(ITU)	Treaty based organization	Coordination ,Guidelines, technical standards and education	193 countries and 700 companies
European Union (EU)	Governing body	Legislation, policy maker	28 countries
North Atlantic Treaty Organization (NATO)	Treaty based organization	Guidelines, education, cyber/military Prevention and Response cooperation	33 countries
Organization for Economic Co-operation and Development(OECD)	International Forum	Publications and reports	34 countries
Asia-Pacific Economic Cooperation(APEC)	International Forum	Publications and reports	21 countries
Organization for Security Co-operation in Europe (OSCE)	Regional Security Organization	Training , workshops and reports	57 countries 11 partners

Table 1: IGOs and Related Cyber Activities

- International Internet Technical Organization (IITO)-IITO are managing and developing standards, protocols and technical documents (Kahn, McConnell et al. 2011).
- Institution- Institutions is a structure or mechanism with a particular behaviour. In the cyber domain, institutions are created in response to imminent cyber threats. These institutions are funded national authority with international scope; however they are not in a form of IGOs (Choucri et al. 2014).

IITO	Structure	Cyber Activity
Internet Corporation for Assigned Names and Numbers(ICANN)	Non-Profit corporation	Manage IP addresses and DNS
Internet Engineering Task Force (IETF)	Non-Profit corporation	Design and develop technology, protocols and guideline
The World Wide Web Consortium (W3C)	Committee	Web Standards

Table 2: IITOs and Related Activates

Institutions	Scope	Cyber Activity
Computer Emergency Response Team Coordination Centre (CERT – CC)	International	Coordination of global CERT
Asia Pacific(AP)-CERT	Regional -Asia	Asian Regional coordination
TF-CSIRT	Regional -Europe	European regional coordination
Forum of Incident Response and Security Teams(FIRST)	International	Forum and Information sharing
International Multilateral Partnership Against Cyber Threat(IMPACT)	International	Global threat response centre

Table 3: Institutions and Related Activates

- Criminals- Cyber criminals are the enterprises that seek to achieve financial gain through illegal activities. As cyber criminals become more decentralised, they become more organized and gain more technical knowledge and resources.
- Terrorists and Militia groups – Cyber terrorists can impose a permanent cyber threat to the government and populace by attacking networks, information systems and infrastructure that are using internetworked information systems (Kallberg and Thuraisingham 2013).

Non-Organized

Any actors without the basic requirements of organized actors can be defined as non-organized actors.

- Hackers- Hackers are often individuals who exploit vulnerabilities in a computer or system networks. Hacker's motivations are varied broadly from reputation to financial gains. Hackers' morals or ethics are the metrics that are classified as Black Hat, White Hat, and Grey Hat, etc.
- Hacktivists -Hacktivists are often politically motivated individual hackers that attack specific targets to achieve ideological goals.
- Whistleblowers- Whistleblowers are mainly individuals that are exposing and leaking misconducts or illegal activities occurring in governments, organizations, etc. The recent revelation of Snowden is an example of this activity.
- Cyber Warrior-Cyber fighters are nationally motivated citizens that are acting against other political parties that are opposing them.

5.3 Preparation Process

The Art of War has given us the challenges to not rely on the likelihood of the enemy's not coming, instead on our readiness to receive them (Sun-tzu, Sawyer et al. 1994).The preparation process will help an entity to prepare and develop a cyber response plan prior to a cyber attack. Providing sufficient preparation will facilitate smooth execution of a cyber capability during a cyber attack. The image of cyberspace, threat and vulnerability is changing prominently over a period; hence developing a single defense strategy is not compelling, considering the complex nature and severe impacts of cyber attacks. While the need for multiple defense strategies is evident, the preparation phase will also facilitate a smooth transition to various cyber capabilities during a cyber attack.

5.3.1 Planning

The planning phase require to prepare an approach for a cyber defense plan prior to a cyber attack. The planning phase require to consider the worst case and best case attack scenarios to help the defenders to apply the most appropriate defense capabilities.

5.3.2 Communication

Communication Preparation require to establish a comprehensive plan to interact with all the required stakeholders during and prior to the cyber threat.

5.3.3 Activation

Developing a process to activate a cyber defense capability in a timely manner.

5.3.4 Evaluate

All the preparation procedures need to be continuously tested, evaluated and updated to ensure that they are enforced during cyber attack incidents. The evaluation can be performed through audits, maneuvers, exercise and previous experiences.

6. Conclusion and Future Work

The overall objective of development this taxonomy was providing all interested parties - researchers, business and government organizations- with a tool for an overall evaluation of their security status and quick finding of weak points of their cyber defense mechanisms. As we indicated in the introduction to this paper, our approach to the problem was taken from so-called McCumber Cube (2004). In this Cube, all security issues are grouped into small spaces and evaluated separately. We believe that the same approach should be used in researching security systems. Foundation stone of such method is based on the development of a useful taxonomy of cyber defenses capabilities. And it was the main objective of this research. The taxonomy has been introduced through a process of modification of a base cyber defense model, which can be used as a foundation for national cyber defense development.

We assume that this taxonomy and cyber defense process model will be useful to cyber defenders to grasp a better understanding of cyber defense capabilities that can be used to mitigate and respond to the cyber attacks. Governments and organizations can use the different categories of this taxonomy to build a robust and an effective cyber defense strategy to safeguard against the cyber threats. The proposed study also provides a valuable insight to cyber security controls and mechanisms that can be used to mitigate current cyber attacks.

We do not claim that this study has addressed all possible security controls; however, we perceive that the taxonomy can be used by the cyber security practitioners to facilitate cyber security implementation.

From the organization perspective, this study has classified various international agencies, organizations and authorities that can offer technical and logistical support to the nation states and cyber defenders. The proposed taxonomy is extensible; hence other scholars can add other dimensions or classifications to the current study. The Attacker's motivations are not addressed in this study so future research can focus on the motivational aspect of cyber attacks.

Finally, taxonomies need to get updated with the rapid speed of changes in technology, attack mechanism, regulation or attacker motivation. We will constantly try to track these changes and apply them to our taxonomy to make it current.

References

Andress, J. and S. Winterfeld (2011) *Cyber warfare: techniques, tactics and tools for security practitioners*, Elsevier.

Bruderlein, C. (2000) "The role of non-state actors in building human security." The case of armed groups in intrastate wars. Human security network Geneva.

Choucri, N., Madnick, S., & Ferwerda, J. (2014). Institutions for cyber security: International responses and global imperatives. *Information Technology for Development*, *20*(2), 96-121

Clarke, R. A. and R. K. Knake (2011*) Cyber war*, HarperCollins.

Cohen, F. (1997) "Information system attacks: A preliminary classification scheme." *Journal of Computers & Security*, (16)1, pp. 29-46.

Denning, D. E. (2014) "Framework and principles for active cyber defense." *Journal of Computers & Security*, (40), pp. 108-113.

Hachem, N., Ben Mustapha, Y., Granadillo, G. G., & Debar, H. (2011, May). Botnets: lifecycle and taxonomy. In *Network and Information Systems Security (SAR-SSI), 2011 Conference on*, IEEE, pp. 1-8

Hansman, S. and R. Hunt (2005) "A taxonomy of network and computer attacks." *Journal of Computers & Security*, (24)1, pp. 31-43.

Harrison, K. and G. White (2011) "A taxonomy of cyber events affecting communities." System Sciences (HICSS), 2011 44th Hawaii International Conference on, IEEE.

Howard, J. D. and T. A. Longstaff (1998) "A common language for computer security incidents." Sandia National Laboratories.

Igure, V. and R. Williams (2008) "Taxonomies of attacks and vulnerabilities in computer systems." *Communications Surveys & Tutorials*, IEEE (10)1, pp. 6-19.

ISACA (2014*) Cybersecurity Fundamentals* USA.

ISO, B. (2012) “BS ISO/IEC 27032:2012 Information Technology Guideline for Cybersecurity.” British Standards Institute, London.

Janczewski, L. J. (2014) “3rd World War: Cyber War.” Proceeding of the “Informatics for the Future” conference, Warsaw, Poland.

Jordan, F. and G. Hallingstad (2011) “Towards Multi-National Capability Development in Cyber Defense.” *Information & Security: An International Journal*, (27)1, pp. 81-89.

Kahn, R. E., McConnell, M., Nye Jr, J. S., Schwartz, P., Daly, N. J., Fick, N., & Sharp, T. (2011). *America’s cyber future*. Technical report, Center for a New American Security.

Kallberg, J. and B. Thuraisingham (2013) “From Cyber Terrorism to State Actors’ Covert Cyber Operations.”

Kende, M. (2014). *Internet Society Global Internet Report 2014*. USA.

Khattak, S., Ramay, N. R., Khan, K. R., Syed, A. A., & Khayam, S. A. (2014). A taxonomy of botnet behavior, detection, and defense. *Communications Surveys & Tutorials*, IEEE, 16(2), pp. 898-924

Killourhy, K. S., et al. (2004) “A defense-centric taxonomy based on attack manifestations.” Dependable Systems and Networks, 2004 International Conference on, IEEE.

Kjaerland, M. (2006) “A taxonomy and comparison of computer security incidents from the commercial and government sectors.” *Journal of Computers & Security*, 25(7), pp. 522-538.

Klimburg, A. (2012) *National cyber security framework manual*, NATO Cooperative Cyber Defense Center of Excellence.

Lindqvist, U. and E. Jonsson (1997) “How to systematically classify computer security intrusions.” *Security and Privacy*, 1997. Proceedings, 1997 IEEE Symposium on, IEEE.

Loukas, G., et al. (2013) “A taxonomy of cyber attack and defense mechanisms for emergency management networks.” Pervasive Computing and Communications Workshops (PERCOM Workshops), 2013 IEEE International Conference on, IEEE.

McCumber, J. (2004) *Assessing and managing security risk in IT systems*: A structured methodology, CRC Press.

Mirkovic, J. and P. Reiher (2004) “A taxonomy of DDoS attack and DDoS defense mechanisms.” *ACM SIGCOMM Computer Communication Review*, 34(2), pp. 39-53.

Mudge, R. S. and S. Lingley (2008) “Cyber and air joint effects demonstration (caajed).” DTIC Document.

Neumann, P. G. and D. B. Parker (1989) “A summary of computer misuse techniques.” Proceedings of the 12th National Computer Security Conference, Baltimore, MD, USA.

Rosenzweig, P. (2014) “International Law and Private Actor Active Cyber Defensive Measures.” Stan. *J Int'l L*, 50, pp. 103-185.

Rovner, J., et al. (2013). *NATO Intelligence Sharing in the 21st Century*. Columbia School of International and Public Affairs.

Scott, D., Applegate and S. Angelos (2013) “Towards a Cyber Conflict Taxonomy.” 5th International Conference on Cyber Conflict, Citeseer.

Simmons, C., et al. (2009) “AVOIDIT: A cyber attack taxonomy.”

Sun-Tzu, et al. (1994) *Sun Tzu: The Art of War*, Westview Press.

Uma, M. and G. Padmavathi (2013) “A Survey on Various Cyber Attacks and their Classification.” *IJ Network Security* (15)5, pp. 390-396.

Von Solms, R. and J. Van Niekerk (2013) “From information security to cyber security.” *Journal of Computers & Security,* 38, pp. 97-102.

Zhu, B., Joseph, A., & Sastry, S. (2011). “A taxonomy of cyber attacks on SCADA systems”. In *Internet of things (iThings/CPSCom), 2011 international conference on and 4th international conference on cyber, physical and social computing*, pp. 380-388. IEEE.