博 士 論 文

Leveraging Systems Thinking to Complement Cyber Risk Management

Masato KIKUCHI

菊地　正人

情報セキュリティ大学院大学
情報セキュリティ研究科

情報セキュリティ専攻

２０２０年９月

Table of Contents

1 Introduction

1.1 Background

It is a tedious task to identify risks in cyberspace and treat them because cyberspace is a complex system and the scope is very broad. The interconnection of cyberspace and physical space means that cyber-attacks against cyberspace have an increasing impact on industries and society that increasingly rely on cyberspace. While interconnectivity within cyberspace increases efficiency, it reduces resilience to cyber-attacks.

1.2 Issues

There is a gap between the nature of risks in cyberspace and view of conventional risk management approaches about it. Conventional risk management approaches have difficulty in analyzing cyber risk and treating it appropriately.

1.2.1 View of Conventional Risk Management Approaches

1.2.1.1 Events and Causes

ISO 31000:2018 [1] is a representative risk management standard and defines risk as the effect of uncertainty on objectives. Conventional risk management approaches such as ISO 31000:2018 focus attention on individual events that affect the objective and their obvious causes as shown in Figure 1.

Figure 1. Causes, Events and Objective.

They tend to assume that causes are the proximate events immediately preceding the effect and large-scale effects can only be generated by large causes.

Conventional risk management approaches tend to see that the factors affecting the risk and their effect on the risk level are close in time and space and their relationship is linear because they tend to ignore feedback processes and associated delays. This occurs because conventional risk management approaches rely on our simplified cognitive maps of the causal structure of systems. Our mental models learn from experience. Consequences that are not close in time and space are often beyond our experience.

The factors affecting risks are risk sources, events and controls:

- Risk sources and events are the factors that increase the risks.
- Controls are the factors that decrease the risks.

1.2.1.2 Distance between the Risks and Their Factors

Conventional risk management approaches assume that the risk source produces a proportional effect on the risk level (linear relationship) because of the lack of consciousness of distance. This means, for example, conventional risk management approaches assume that a large increase in risk level can only be caused by large vulnerabilities nearby. Distance does not only mean physical distance but logical distance as well. If there are many interactions among entities such as network communications among thousands of devices or social interactions among thousands of people, there is a distance among them. Conventional risk management approaches assume that there is no implication of the feedbacks created by the state of the risk, because the increase in risk remains in proportion to the increase in risk source even as the state of risk changes as shown in Figure 2.

Figure 2. A Linear Relationship between Risk Source and Risk.

The behavior of the risk level over time can be drawn with a straight line if the risk level grows at a constant rate because the risk source produces a proportional effect on the risk level as shown in Figure 3.

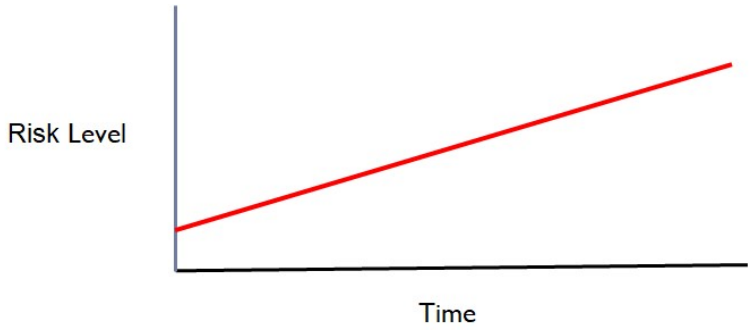

Figure 3. Linear Growth Behavior of Risk Level. (on assumption that original factors affecting risks grow at a constant rate)

There is a typical case of misperception of risk in linear terms caused by our simplified cognitive maps of the causal structure of systems. According to the research by Lammers et al. [2], people mistakenly perceive the coronavirus to grow in a linear manner, underestimating its actual potential for exponential growth and this prevents people from taking the measure such as social distancing to prevent the illness. Although many countries across the globe have introduced social distancing measures, sizeable opposition among politicians and the general population has delayed, prevented, or terminated early measures to increase social distancing. For example, toward the end of March 2020, a month in which, in the United States, the number of infections increased from a few dozen to 200,000 cases, one in four Americans opposed social distancing measures. A root cause is that people fail to recognize that the coronavirus can grow in an exponential manner, and, instead, erroneously perceive its growth in linear terms.

In their study, American participants were asked to guess the total number of coronavirus cases over specific period as shown in Figure 4.

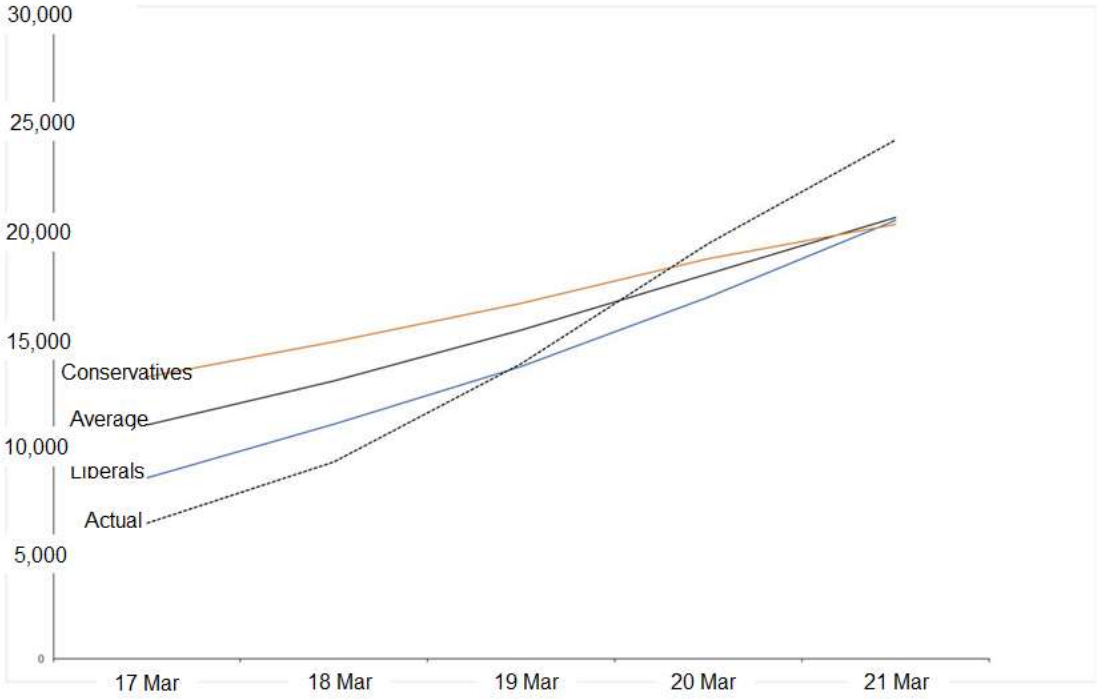

Figure 4. Perception and Actual of Total Number of Coronavirus Cases (Joris Lammers et al. PNAS 2020;117:28:16264-16266 [2]).

Participants, on average, show misperception of the virus's exponential growth in linear terms and underestimate the slope of the coronavirus growth curve over the period, falsely believing the number to be higher early in the week than it was. When making these guesses, many people erroneously think that the coronavirus cases have increased at a steady and constant pace. In reality, in the USA (as in almost all other countries) the number of corona patients doubles and keeps doubling every three days. Conservatives do so more strongly than liberals (continuous data split across the neutral midpoint, for presentation purposes).

This is a typical example that people, organizations and politicians tend to perceive the risk to grow in a linear manner, underestimating its actual potential for exponential growth and this prevents people from taking the appropriate measure to reduce the risk. In this case, the risk source is socializing with infected people without keeping distance and the risk is growth of coronavirus. People mistakenly perceive that socializing with infected people without keeping distance increases coronavirus in a linear manner because it generates an increase in number of infected people at a proportional rate as show in Figure 5. This means people perceive that the relationship between risk source and risk level is linear. In reality, socializing with infected people without keeping distance increases coronavirus in an exponential manner because it grows into large effect on the increase in number of infected people by cascading effects of a feedback loop as shown in Figure 6. This means the relationship between risk source and risk level is non-linear.

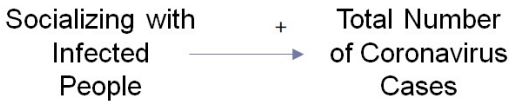

Figure 5. People's Perception about Linear Growth of Coronavirus.

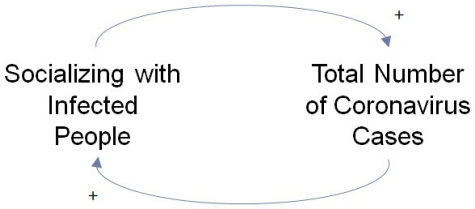

Figure 6. Reality about Exponential Growth of Coronavirus.

1.2.1.3 Time between the Risks and Their Factors

Conventional risk management approaches assume that the control instantly produces a proportional effect on the risk level (linear relationship) because of the lack of the consciousness of a delay. This means, for example, risk level exceeding an acceptable level can be reduced only by immediate implementation of controls with the same scale on the risk level exceeding an acceptable level. It is expressed as a balancing feedback loop between risk and control in Figure 7.

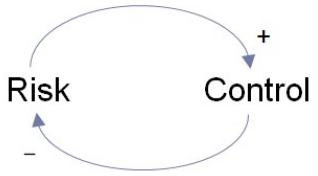

Figure 7. A Linear Relationship between Risk and Control.

When the relationship between the risk level exceeding an acceptable level and the implementation of controls is linear, the resulting behavior of risk level is goal seeking as show in Figure 8.

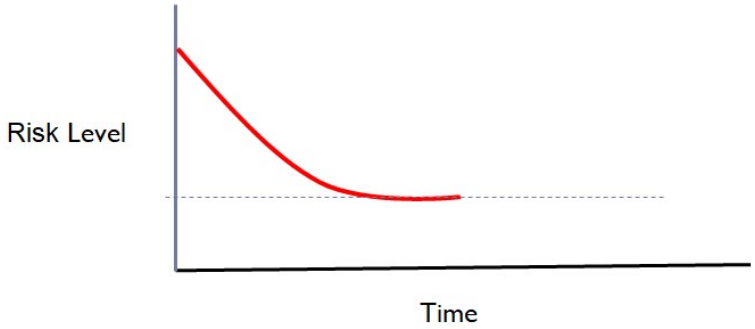

Figure 8. Goal Seeking Behavior of Risk Level.

Goal seeking behavior seeks equilibrium (acceptable risk level).

1.2.1.4 Equilibrium

Conventional risk management approaches are based on equilibrium assumption. This means that large-scale deviations from equilibrium (where risk level is at an acceptable level) can only be generated by large-scale causes that act with the same scale on the effect, that is, the outcome is a linear function of the cause.

When IT environment does not have global connectivity, interactions among devices are simple and it is not difficult for the conventional risk management approaches to predict their effects that are the outcome of a linear function of the cause. The consequences are close in time and space and can be predicted by experience from which the people can learn.

1.2.2 Nature of Risks in Cyberspace

1.2.2.1 Complex System

Cyberspace is a complex system. Management of risks in cyberspace is itself a complex process because it deals with cyberspace that is a complex system. Although conventional risk management approaches are well-established in the traditional IT environment, their direct translation to cyberspace is not straightforward because of the global connectivity of cyberspace, the large number of entities and their interactions.

According to Sterman [3], all behaviors of complex systems arise from the interaction of just two types of feedback loops, reinforcing feedback loops and balancing feedback loops. Reinforcing feedback loop amplifies whatever movement occurs, producing more movement in the same direction. Balancing feedback loop is always operating to reduce a gap between what is desired and what exists. The basic modes of behavior of complex systems are:

- Exponential growth, created by reinforcing feedback
- Goal seeking, created by balancing feedback
- Oscillation, created by balancing feedback with delays

Risks in cyberspace have these behaviors as they deal with cyberspace. Goal seeking behavior of the risks can be treated by conventional risk management approaches because its behavior is caused by the linear relationship between risks and their factors and seeks the state of equilibrium. However, exponential growth and oscillation behavior of the risks cannot be treated properly by conventional management approaches because they are caused by the non-linear relationship between risks and their factors and alters the state of equilibrium.

Especially in cyberspace, the factors affecting the risk and their effect on the risk level may not be close in time and space and their relationship may be drawn with curves (non-linear relationship) because the factors affecting the risk may not produce a proportional effect on the risk level.

1.2.2.1 Distance between the Risks and Their Factors

In cyberspace, small risk source can grow into large effect on level of the risks (non-linear relationship) by cascading effects through the global connectivity of cyberspace. This means, for example, a large increase in risk level in the premises of the organization may be caused by small vulnerabilities in the distant places such as systems operated by oversea business partners or PCs used at employee's home. There is an implication of the feedbacks created by the state of the risk, because the increase in risk is amplified with a transformation on a scale completely different from risk source as the state of risk changes. It is expressed as a reinforcing feedback loop between risk source and risk in Figure 9.

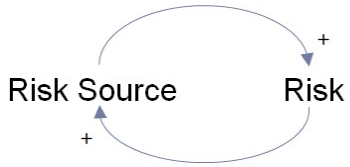

Figure 9. A Non-Linear Relationship between Risk Source and Risk.

The larger the risk, the greater its net increase because of larger risk source, further augmenting the risk and leading to ever-fast growth. For example, an increase in risk that devices in the premises of the organization are infected will generate an increase in infected devices in cyberspace (risk source), that further generates an increase in the risk.

The behavior of the risk level over time can be drawn with a curve if the risk level grows exponentially because the risk source grows into large effect on the risk level as shown in Figure 10.

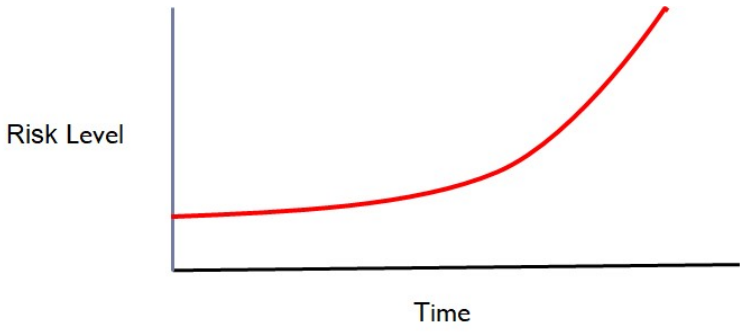

Figure 10. Exponential Growth Behavior of Risk Level. (on the assumption that original factors affecting risks grow at a constant rate)

1.2.2.1 Time between the Risks and Their Factors

In cyberspace, the control may not produce a proportional effect on the risk level (non-linear relationship) because of the delay in the implementation of controls. Complexity of the interconnections in cyberspace may cause the delay of effects of the controls. This means, for example, risk level exceeding an acceptable level cannot

be reduced by implementation of controls with the same scale on the risk level exceeding an acceptable level. It is expressed as a balancing feedback loop with a delay between risk and control in Figure 11.

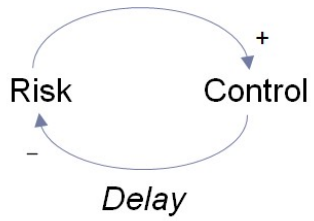

Figure 11. A Non-Linear Relationship between Risk and Control.

If there is a delay in the implementation of controls, the controls have different effect on risk level in the short-term and the long-term. The delay causes the implementation of controls to continue even after the risk level is supposed to be reduced to the acceptable level, forcing the risk level to decline too much, and triggering too much reduction of implementation of controls. The resulting behavior of risk level is oscillation as show in Figure 12.

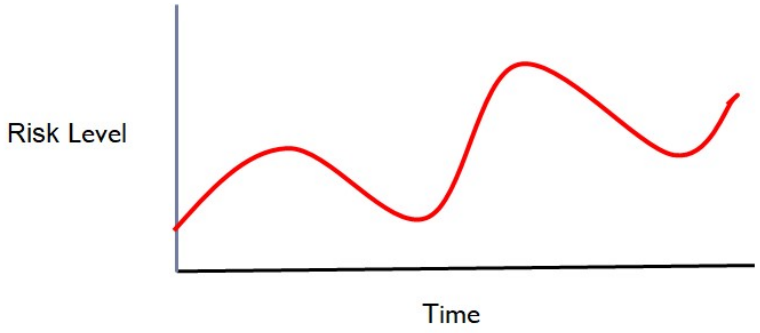

Figure 12. Oscillation Behavior of Risk Level.

Oscillation behavior constantly overshoots equilibrium (acceptable risk level).

1.2.2.2 Equilibrium

In cyberspace, oscillation and exponential growth behaviors overshoot equilibrium. The entities in cyberspace are tightly coupled and interact strongly with one another. Their actions feedback on themselves and alter the state of equilibrium. The tiny initiating events cause transformation on a scale completely different from their own and their effects are not proportional to their causes, that is, the outcome is a nonlinear function of the cause. This emergent property of cyber risk is not considered by conventional risk management approaches.

1.2.3 Summary

Because conventional risk management approaches assume that the factors affecting the risk and their effect on the risk level have linear relationships, they have difficulty in analyzing the effects on the cyber risk level that may have non-linear relationships

with the factors affecting the cyber risk and treating cyber risk appropriately. The behavior of cyber risk level predicted by conventional risk management approaches can differ from the real situation because they do not concern the implications of the feedbacks among the factors affecting the risk and their effect on the risk level. Interrelationships among the factors may not be in linear cause effect chains but in feedback loops and they may allow cyber risk to exhibit behavior that couldn't be observed in its constituent parts.

1.3 Objectives

The objective of the research is to propose the new models to complement conventional risk management approaches as stated in ISO 31000:2018 (Risk Management Standard) [1] and ISO/IEC 27005:2018 (Information Security Risk Management Standard) [4] to fill the gap between the nature of cyber risk and view of conventional risk management approaches about it leveraging systems thinking and system dynamics. The new models provide the ability to analyze the effects on the cyber risk level that may have non-linear relationships with the factors affecting the cyber risk and treat cyber risk appropriately. Among the basic modes of behavior of complex systems, exponential growth and oscillation behaviors are caused by the non-linear relationship between risks and their factors and cannot be treated properly by conventional management approaches. The new models analyze and treat these behaviors of cyber risk level.

System thinking can describe non-linear relationships between the factors and their effects that are not close in time and space in graphical causal presentation. System dynamics is based on systems thinking and can simulate the non-linear behavior of complex systems over time and provides an opportunity to experiment with solutions that control the behavior.

2 Previous Research

2.1 Introduction

Previous researches are reviewed from the two points of view: the factors affecting the management of cyber risk and application of systems thinking to the management of cyber risk and nonlinear effects.

2.2 Researches on the Factors Affecting the Management of Cyber Risk

2.2.1 Overview

Section 2.2 examines the previous researches on the factors affecting the management of cyber risk.

In order to manage cyber risk, there is a need to review the researches on what cyberspace is, how threats in cyberspace are categorized and how the conventional security risk management approach fits cyber risk.

First, the researches on threats in cyberspace are examined. Second, researches on securitization and its application to cyberspace are examined. Third, researches on risk management standards and their application to cyberspace are examined.

2.2.2 Threats in Cyberspace

2.2.2.1 Clark`s View of Cyberspace

Clark [5] made an important contribution to the definition of cyberspace as a hierarchical contingent system composed of:

- The people who participate in the cyber-experience—who communicate, work with information, make decisions and carry out plans, and who themselves transform the nature of cyberspace by working with its component services and capabilities (People Layer: e.g. actors, entities, users).
- The information that is stored, transmitted, and transformed in cyberspace (Information Layer: Information makes up interactions.).
- The logical building blocks that make up the services and support the platform nature of cyberspace (Logical Layer: This layer can be thought of as the ‘code' or protocols that give cyberspace its rules and structure for how it functions such as application, database and Web.).
- The physical foundations that support the logical elements. Cyberspace is a space of interconnected computing devices, so its foundations are PCs and servers, supercomputers and grids, sensors and transducers, and the Internet and other sorts of networks and communications channels (Physical Layer: e.g. PCs, servers and routers).

Clark argues that it is not the computer that creates the phenomenon we call cyberspace but the interconnection that makes cyberspace—an interconnection that affects all the layers in this model. Threats and vulnerabilities exist at all layers so that defense must similarly be based on an understanding of all these layers.

2.2.2.2 Kramer`s View of Cyberspace

Kramer et al. [6] introduces various definitions of cyberspace. These definitions suggest that cyberspace is more than computers and digital information and a key operational medium through which "strategic influence" is conducted. They also define the concept "cyberpower" as the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power. They argue that we are transforming how we exert influence and employ "smartpower" in the pursuit of strategic goals because of new forms of content and the connectivity that we use to transmit and exchange that content.

2.2.2.3 Appazov`s View of Cyberspace

Appazov [7] identifies anonymity, asymmetry and global reach as the key challenging features of cyberspace from a legal point of view. He thinks that those features are advantages of adversaries. For example, adversaries can conceal their identities (anonymity), a single adversary with the access to cyberspace can launch massive cyber-attacks due to the technologies (asymmetry) and the malicious actions of adversaries are borderless and unbounded by territorial jurisdiction (global reach).

Appazov also separates Cyber-Attacks into four categories: Cyberwarfare, Cyberespionage, Cyberterrorism, and Cybercrime. This categorization facilitates the development of national and international law governing the rights and duties of individuals and nations with respect to each category of activity with the exception of espionage and addresses the shortcomings of national and international legal frameworks.

2.2.2.4 Hansman`s Taxonomy of Cyber-Attacks

Hansman et al. [8] focus on the provisioning of a method for the analysis and categorization of both computer and network attacks, thus providing assistance in combating new attacks, improving computer and network security as well as providing consistency in language when describing attacks.

They propose to use the concept of dimensions that are a way of allowing for a classification of an attack to take a more holistic view of such an attack. The dimensions are attack vector, the targets of the attack, vulnerabilities, and possibility for an attack to have a payload or effect beyond itself. The attack vector is the method by which an attack reaches its target. They indicate that identification of attack vectors is very important because they provide the most accurate description of an attack. They also suggest that further dimensions could be added in the future such as propagation by replicating attacks and some form of visualization would be useful to help understand classifications better, and to correlate attacks.

2.2.2.5 Meyers` Taxonomy of Cyber-Attacks

Meyers et al. [9] argue that it is essential in constructing a defensive architecture to know who the adversaries are and what kinds of threats they are likely to attempt. They construct taxonomies of cyber adversaries and methods of attack, drawing from a survey of the literature in the area of cybercrime. For each of the adversary types, the corresponding skill level, maliciousness, motivation, and method are listed. They focus primarily on attacks in terms of their associated attack vectors because they think it is practically infeasible to encompass many dimensions in a single taxonomy.

2.2.2.6 Richberg's Threat Framework

Richberg [10] argues that there are so many cyber threat models. He proposes a common approach to threat framework that allows mapping of multiple models to a common reference than directly to each other. This approach categorizes threat activities, their objectives, actions and indicators through threat lifecycle and facilitates grouping and comparison of cyber threat activities seen from different perspectives.

2.2.2.7 Hutchins' Cyber Kill Chain Model

Hutchins et al. [11] argue that conventional network defense tools focus on vulnerability component of risk, and traditional incident response methods make assumption that response should happen after the point of compromise. They propose an intelligence-driven approach that addresses the threat component of risk to study intrusions from the adversaries' perspective. Their cyber kill chain model describes phases of intrusions, mapping information that objectively describes an intrusion to defender courses of action. Definitions for cyber kill chain phases are as follows:

- Reconnaissance - Research, identification and selection of targets.
- Weaponization - Coupling a remote access trojan with an exploit into a deliverable payload such as PDF and Microsoft Office documents.
- Delivery - Transmission of the weapon to the targeted environment. Typical delivery vectors include email attachments and websites.
- Exploitation - After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability.
- Installation - Installation of a remote access trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.
- Command and Control (C2) - Once compromised hosts establish the C2 channel, intruders have "hands on the keyboard" access inside the target environment.
- Actions on Objectives - Typically, this objective is data exfiltration which involves collecting, encrypting and extracting information from the victim environment; violations of data integrity or availability are potential objectives as well.

These cyber kill chain phases are shown in the Figure 13.

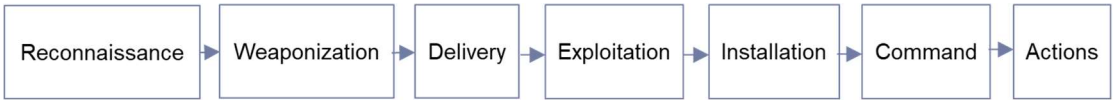

Figure 13. Cyber Kill Chain Phases

A kill chain is an end-to-end process to target and engage an adversary to create desired effects and any one deficiency will interrupt the entire process. They encourage defenders to move their detection and analysis up the kill chain and more importantly to implement courses of actions across the kill chain. They also insist that analyzing multiple intrusion kill chains over time will identify commonalities, overlapping indicators and adversaries' intent.

2.2.3 Securitization and Cyberspace

2.2.3.1 Buzan's Securitization

In their book [12], Buzan et al. describe securitization theory. Securitization is a process by which an issue is presented as an existential threat to a designated referent object, and the special nature of security threats justifies the use of extraordinary measures to handle them. Referent objects are seen to be existentially threatened and have a legitimate claim to survival. Sectors are identified as specific types of interaction of threats and referent objects. Securitizing actors securitize issues by declaring something – referent object – existentially threatened.

They mention that levels of analysis are used extensively to locate the actors, referent objects, and dynamics of interaction that operate in the realm of security. Levels are locations where both outcomes and sources of explanation can be located and may suggest causal explanations from one level to another. The five most frequently used levels of analysis are as follow:

- International systems, meaning the largest conglomerates of interacting or interdependent units that have no system level above them. Currently, this level encompasses the entire planet.
- International subsystems, meaning groups of units within the international system that can be distinguished from the entire system by the particular nature or intensity of their interactions with or interdependence on each other. Subsystems may be territorially coherent, in which case they are regional such as ASEAN.
- Units, meaning actors composed of various subgroups, organizations, communities, and many individuals and sufficiently cohesive and independent to be differentiated from others and to have standing at the highest levels (e.g. states, nations, transnational firms).
- Subunits, meaning organized groups of individuals within units that are able to affect the behavior of the unit.
- Individuals, the bottom line of most analysis in the social sciences.

They note that security complex is designed for political and military sectors in the context of states level and dominated by regional dynamics and explains distinct and stable patterns of security interaction between actors. Cybersecurity discourse moves seamlessly among internal, private, public and public authority sphere, and between economic and political-military security. RAND's scenario [13] shows the example of such a cybersecurity discourse.

2.2.3.2 Hansen's Hyper-Securitization

Hansen and Nissenbaum [14] adopt the framework of securitization theory to cybersecurity and theorize cybersecurity as a distinct sector with a particular constellation of threats and referent objects. Network security and individual security are significant referent objects, but that their political importance arises from connections to the collective referent objects of the state, society, the nation, and the economy. These referent objects are articulated as threatened through three distinct forms of securitizations: hypersecuritization, everyday security practices, and technonifications. Key to understanding the potential magnitude of cyber threats is the networked character of computer systems.

Hyper-securitizations distinguish themselves from regular securitizations by their instantaneity and inter-locking effects that tie in referent objects from a wide range of sectors (societal, financial, military etc.) by linking them through an almost domino-like sequence to the consequences of a damaged network. Everyday security practices construct various threats that towards the entire network, thus, to a larger extent, to society. Technifications concerns the role of technical, expert discourse within cyber securitization.

2.2.4 Risk Management and Cyberspace

2.2.4.1 ISO Risk Management Standards

ISO provides a risk management standard called ISO 31000:2018 and an information security risk management standard called ISO/IEC 27005:2018.

ISO 31000:2018 [1]:

- provides guidelines on managing risk faced by organizations;
- provides a common approach to managing any type of risk including cyber risk and is not industry or sector specific; and
- provides principles, framework and processes of risk management that consists of risk identification, risk analysis, risk evaluation and risk treatment.

ISO/IEC 27005:2018 [4]:

- provides guidelines for information security risk management in an organization;
- is based on the asset, threat and vulnerability risk identification method; and
- inherits processes of risk management defined by ISO 31000.

There are other ongoing ISO activities to develop new standards concerning cyber security.

2.2.4.2 NIST Cybersecurity Framework

President issued Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, in February 2013. The Order directed NIST to work with stakeholders to develop a voluntary framework (Cybersecurity Framework) – based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure.

Cybersecurity Framework [15] consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk. The framework puts more focus on the later stages of risk management processes such as risk treatment consists of detect, respond and recover functions.

2.2.5 Achievements

There are some established definitions of cyberspace. Interconnectivity rather than computers and digital information is highlighted as a key element of cyberspace. This key element of cyberspace provides people the ability to influence events in operational environments. Adversaries take advantage of it to attack the organizations through cyberspace while the organizations take advantage of it to create an organization value through cyberspace. The features derived from interconnectivity of cyberspace such as anonymity, asymmetry and global reach are advantages of adversaries.

There are some established ways to categorize cyber-attacks. There is one way of categorization to address the shortcomings of national and international legal frameworks. Another way of categorization is to provide assistance in combating the attacks and providing consistency in language when describing attacks. One of the most thorough taxonomy consists of four dimensions: attack vector, the targets of the attack, vulnerabilities, and payloads. Another taxonomy focuses on adversaries and attack vector. Taxonomies develop into a common threat framework progressively and allows mapping of multiple taxonomies to a common reference. There is a kill chain approach to describe phases of intrusions from the adversaries' end-to-end process perspective. It allows defenders to move their detection up the kill chain and analyze multiple intrusion kill chains over time to identify adversaries' intent.

It is successful to identify and locate cybersecurity as a particular sector on the broader terrain of securitization theory by recognizing that potential magnitude of cyber threats is mainly caused by the networked character of computer systems. Cybersecurity is theorized as a sector where multiple discourses among the state, society, the nation, and the economy may be found.

Conventional risk management approaches as stated in ISO 31000:2018 (Risk Management Standard) and ISO/IEC 27005:2018 (Information Security Risk

Management Standard) are already used for cyber risk management as well. Main processes of risk management such as risk identification, risk analysis, risk evaluation, and risk treatment defined in ISO 31000:2018 and inherited by ISO/IEC 27005:2018 are valid regardless of types of risks. More cyber risk-oriented framework called Cybersecurity Framework is also developed based on these existing standards. The framework puts more focus on the later stages of risk management processes such as risk treatment consists of detect, respond and recover functions.

The achievements of these researches are summarized as below:

- Identification of features of cyberspace
- Classification of threats in cyberspace
- Establishment of the theories on cyber security as a distinct sector with a particular constellation of threats and referent objects
- Application of generic risk management approach to information security risk taking account of cyberspace

2.3 Researches on the Application of Systems Thinking to the Management of Cyber Risk

2.3.1 Overview

Section 2.3 examines the previous researches on the application of systems thinking to the management of cyber risk.

In order to manage cyber risk, there is a need to review the researches on how systems thinking can be applied to cyber risk and extreme events that are results of non-linear behavior of cyber risk.

2.3.2 Application of Systems Thinking to the Management of Cyber Risk and Extreme Events

2.3.2.1 Heylighen`s Research

Systems thinking is a way of helping a person to view complex systems. Heylighen [16] argues that complex systems such as the Internet have emergent properties that cannot be reduced to the mere properties of their parts. His explanation about the components of complex systems and their interactions is shown in the following sub-sections.

2.3.2.1.1 Agent

The complex systems consist of many parts that are connected via their interactions, both autonomous and to some degree mutually dependent. The components of a complex system are most commonly modeled as agents that react to a specific condition perceived in the environment by producing an appropriate action.

2.3.2.1.2 Propagation and Emergence

An action by one agent trigger further actions by one or more other agents, possibly setting in motion an extended chain of activity that propagates from agent to agent across the system. Such interactions are initially local: they start out affecting only the agents in the immediate neighborhood of the initial actor and there is no correlation between the activity in one region and the activity in another one. However, because all components are directly or indirectly connected, changes propagate so that far-away regions eventually are influenced by what happens here and now.

The outcome of interactions is not arbitrary, but exhibits a "preference" for certain situations over others. All interactions between all agents in the complex system will tend towards such a coherent, stable state, until they are all mutually adapted. This process generally accelerates because of a positive feedback.

Self-organization can be defined as the spontaneous emergence of global structure out of local interactions where "spontaneous" means that no internal or external agent is in control of the process. The structure emerging from self-organization can often be represented as a complex network such as the Internet. Complex networks tend to exhibit a number of specific features such as clustering and scale-free networks.

2.3.2.1.3 Clustering

Clustering means that when A is linked to B, and B to C, then the probability is high that A is also linked to C. In other words, two randomly chosen connections of B have a much higher than chance probability of being connected themselves.

2.3.2.1.4 Scale-Free Networks

The nodes of a complex network are strongly differentiated: something that happens to a hub will have a disproportionately large influence on the rest of the network, while something that happens to an ordinary node may have little or no consequences. This has great practical implications: an perturbation that appears in a hub (e.g. a central network server, a high-visibility web page, or a person who is known by many) may change the whole network in a short time, because it is immediately propagated far and wide. By identifying the hubs in a network, it becomes easier to manipulate its dynamics, for good or for bad. Obvious applications include the spread of computer viruses.

Whereas clustering tends to increase distances in a network, by creating locally connected clusters that have few links outside the cluster, the presence of hubs has the opposite effect. Because hubs have a very large number of links, they are likely to link into many different clusters, thus acting as shortcuts that reduce the distance between the clusters. But this also means that removing a hub may break the connections between otherwise remote regions of the network.

The more links an agent has, the larger its neighborhood, and therefore the larger the probability that it will receive even more links from within this neighborhood. Similarly, the larger the cluster, the more likely it is to receive random links from

outside, thus extending the neighborhood outwards and linking it into other clusters. This determines a positive feedback, which leads to an explosive growth in the number of links. The agents that happen to be in the center of such a quickly growing cluster will become the hubs of the network.

2.3.2.1.5 Non-Linearity

Processes in complex systems are often non-linear: their effects are not proportional to their causes. With amplification of positive feedback, initially small perturbations reinforce themselves so as to become ever more intense. The dynamics of complex systems typically exhibits a combination of positive and negative feedbacks, so that certain changes are amplified and others dampened. This makes the system's overall behavior both unpredictable and uncontrollable.

2.3.2.2 Research of McKelveya and Andriani

McKelveya and Andriani [17] argue that tiny initiating events often first appear as random, seemingly meaningless events that are easy to overlook, and yet they can spiral up into extreme events of disaster proportions. They note that if managers were to become more familiar with scale-free theories, they would better and sooner be able to see possible scale-free causal developments spiraling into extreme outcomes.

They drew on scale-free theories from complexity science that explain nonlinear dynamics. Even though the cause is the same at multiple levels, however, the consequence can be nonlinear; that is, nonlinear outcomes resulting when a single event out of myriad very small events gets amplified – for example, by positive feedback – to generate an extreme effect extending across multiple levels. Fractal structures emerge because, the same cause applies at multiple levels. While incubation tiny initiating events are required as initiating events, disasters only happen if they scale up in size or consequence.

They state, in a linear world, such as the case with neoclassical economics and disciplines inspired by the equilibrium assumption, large-scale deviations from equilibrium (the normal state) can only be generated by large-scale causes that act with the same scale on the effect, that is, the outcome is a linear function of the cause. Instead, in a nonlinear world, the tiny initiating events cause transformation on a scale completely different from their own.

They observe that positive feedback underlies the Internet. Any time a system grows by adding nodes to an existing network, its growth will amplify historically generated imbalances among the links where older nodes will gain more links.

They argue that self-organization occurs when heterogeneous agents in search of improved fitness interconnect under conditions of exogenously or endogenously imposed adaptive tension. New order is an emergent outcome of the self-organizing process.

2.3.2.3 Trček's Research

Trček [18] suggests using system dynamics with a focus on risk management. He argues that although risk management is a well-established in many other areas, its direct translation to information systems is not straightforward because of the global connectivity of information systems, the large number of elements (e.g. thousands of software components), strong involvement of human factor, almost endless possible ways of interactions, etc.

He also argues that conventional risk management approaches have a lack of visibility of relationships between all related elements and proposes a new generic risk management model to identify these elements in graphical causal presentation. The elements include asset value, threat probability, risk, safeguards investments, current asset vulnerability, and months of exposure period.

The model enables quantitative treatment, together with simulations on how the elements influence oscillation behavior of information security risk level, by use of system dynamics and supports and improves decision making in information systems security. The simulations are basic and oscillation behavior of information security risk level is extremely influenced by the way in which the model is initialized and the model is over-reactive to the changes of elements.

2.3.2.4 Gros´s Research

Groš [19] argues that the information system is a complex system in which interconnections between its components play an important role, that risk management process is itself a complex process because it deals with complex system. Although interconnections between components allow complex systems to exhibit behavior that couldn't be observed in its constituent parts, he observes that the conventional risk management approaches are based on reductionist approach that decomposes a system into its basic components, analyzes them separately and, based on those analyses, predict the behavior of the system as a whole and can differ from the real situation.

He proposes a novel risk management process that takes into account complexity. It focuses on the interconnections and dependencies between resources that are anything, material or non-material that takes part in the information system. Dependencies between resources allow threat sources to spread and to reach other resources and each resource is treated as a source of a threat and has a set of vulnerabilities. This method still has difficulty in determining the exact interaction between resource dependency and controls and how threats spread through the system.

2.3.2.5 Research of Branagan et al.

Branagan et al. [20] argue that complex systems may be defined by the fact that the system behavior is emergent. The macro level behavior of the system is dependent on the interactions between its various components at a level lower than that at which the

behavior is observed. It is impossible to predict the macro level behavior of these systems by observation of the behavior at this macro level, particularly with the limited volume of historical data available.

They think that interdependencies result from coupling between systems by the implementation of communication network such as the Internet and such interdependencies can rapidly increase the overall system complexity. A local system is aware of its immediate coupled neighbors and the potential threat it poses to them and vice versa. Security events may present a significant magnification of risk when transmitted to distant coupled systems which, could in turn, feedback to the originating system. They highlight that the speed of coupling effects is widely recognized as a cyber security problem, computer viruses and worms for example, can spread faster than remedial efforts and risk scenarios for any one of local systems may depend on risk scenarios of all coupled systems.

They explore the use of simulation methods to explore the nature of system behavior where experimentation on the system itself is infeasible. They are based around the exploration of the causal chains starting from some unavoidable threat and terminating at some unacceptable impact and the predicted behavior of a complex system may offer a solution.

Their proposed threat network model is based on two key concepts. First, a threat event encodes a threat acting on some entity in the system of concern. Second, a threat propagation encodes the propagation of threats through the system. Given the probability of threats, and that of propagation between threat events, the static probability threat networks estimates the probability of consequential impacts. It is possible to trace backwards, i.e. from the undesirable impact to determine the range of threats associated with such an outcome. For example, local threat events such as injection of a virus into a network may have disproportionate effects on the macro level of the system behavior and the simulation provides an opportunity to experiment with countermeasures that reduce the probability of specific threat propagations.

Given some good graphical representation of threat event and threat propagation probabilities, the model may allow the risk assessor to identify critical events, and propagations, and to explore the sensitivity of the final outcome to those identified critical parameters. However, the model assumes that all events take place instantaneously and has difficulty in providing a scenario where events are set in a temporal sequence.

2.3.2.6 Research of Saunders et al.

Saunders et al. [21] argues that currently, risk assessment in IT security has been limited to static analysis and modeling.

They propose a system dynamics framework that is capable of moving beyond traditional risk assessment models. The system dynamics simulation provides a graph showing behavior over time and depicts the relationships among the variables of threats, attacks, and budget over a specific period. By viewing these relationships it can hypothesized as to what possible modifications may be beneficial to the system.

There is a lack of validation of the effectiveness of this proposed model against more traditional methods such as Cost Benefit using Annual Loss Expectancy.

2.3.3 Achievements

Previous researches successfully verify that complex system has the unique properties that the Internet has. Key property is identified as emergent property that cannot be reduced to the mere properties of their parts. Interconnections between components allow complex systems to exhibit this property. One example of emergent property is propagation where an action by one agent trigger further actions by one or more other agents, possibly setting in motion an extended chain of activity that propagates from agent to agent across the system. There are also self-organization property and scale-free networks. Self-organization is defined as the spontaneous emergence of global structure out of local interactions and exhibited by the Internet. In scale-free networks, computer viruses spread as an example that tiny initiating events can spiral up into extreme events of disaster proportions. These properties explain nonlinear dynamics and are generally accelerated by a positive feedback.

There are attempts to propose a new generic risk management model to identify related elements in graphical causal presentation to address a lack of visibility of their relationships. These models also enable simulations on how the elements influence behavior of information security risk level and what possible modifications may be beneficial to the risk level.

There is also an attempt to propose a novel risk management process that takes into account complexity. It focuses on interconnections between resources that allow threat sources to spread.

There is a finding that security events may present a significant magnification of risk when transmitted to distant coupled systems and the speed of coupling effects is recognized as a cyber security problem. This behavior is explored by threat network model that are based on two key concepts – a threat event and a threat propagation and allow the risk assessor to identify critical events, and propagations, and to explore the sensitivity of the final outcome to those identified critical parameters.

The achievements of these researches are summarized as below:

- View of the Internet as a complex system that has propagation and emergent behaviors
- View of the spread of computer viruses based on scale-free theories and coupling effects of systems in the Internet
- View of interrelationships among the factors affecting the information security risk in graphical causal presentation
- Basic simulation on how non-linear behavior of information security risk level is influenced by the factors affecting the information security risk over time
- Modelling of threat networks that provide graphical representation of threat event and threat propagation probabilities by application of systems thinking

2.4 Limitations

Previous researches identify that interconnectivity are key elements of cyberspace and generate emergent behaviors. However, they do not succeed in analyzing how they generate emergent behaviors. For example, cybersecurity located as a particular sector on the securitization theory considers that potential magnitude of cyber threats is mainly caused by the networked character of computer systems. However, it does not provide a practical mean to analyze how this symptom occurs, particularly, through propagation dimension and scale-free theories.

Previous researches also establish some ways to categorize cyber threats and they provide common languages about cyber threats to be treated. However, they see cyber threats in liner cause effect chains and do not consider feedback loops among them that generate emergent behaviors.

Although conventional risk management approaches define risk management processes that can be applied to any type of risks, there is a lack of detailed methods to analyze the emergent behaviors of cyber risk.

Regarding the simulation of the generic risk management model on how the related elements influence behavior of information security risk level, it is extremely influenced by the way in which the model is initialized and the model is over-reactive to the changes of elements. The simulation also does not take into account business environments such as business growth and corresponding risk appetite.

Attempt of risk management process to take into account complexity by focusing on interconnections between resources has difficulty in determining how threats spread through the system. Threat network model that explores the effects of threat events and threat propagations on the risk assumes that all events take place instantaneously and has difficulty in providing a scenario where events are set in a temporal sequence.

The limitations of previous researches are summarized as below:

- Propagation dimension and scale-free theories are not practically considered for cyber-attacks analysis.
- Simulation of threat networks assumes that all threat events take place instantaneously and does not take into account a scenario where threat events are set in a temporal sequence.
- Simulation of non-linear behavior of risk level is over-reactive to the changes of the factors affecting the risk.
- Simulation of non-linear behavior of risk level does not take into account business environments such as business growth and corresponding risk appetite.

2.5 Further Exploration

Analysis and treatment of non-linear behavior of risk level in previous researches have limitations and they need to be addressed by further researches. The limitations and the corresponding further exploration are shown in Table 1.

Table 1. Limitations and Further Explorations

Limitations	**Further Exploration**
Propagation dimension and scale-free theories are not practically considered for cyber-attacks analysis. Simulation of threat networks assumes that all threat events take place instantaneously and does not take into account a scenario where threat events are set in a temporal sequence.	Application of propagation dimension and scale-free theories to cyber-attacks analysis
Simulation of non-linear behavior of risk level is over-reactive to the changes of the factors affecting the risk.	Application of systems thinking and system dynamics to model non-linear behaviors of cyber risk level over time
Simulation of non-linear behavior of risk level does not take into account business environments such as business growth and risk appetite.	Comprehensive simulation of non-linear behaviors of cyber risk level taking into account business environments over time

3 Conventional Risk Management Approaches and Cyber Risk

3.1 Introduction

View of conventional risk management approaches is reviewed and a case study is introduced. Based on them, the limitations of conventional risk management approaches are described.

3.2 View of Conventional Risk Management Approaches

ISO 31000:2018 [1] is a representative risk management standard in the world and states:

- Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.
- Risk source is element which alone or in combination has the potential to give rise to risk.
- An event can be a risk source.

ISO/IEC 27005:2018 [4] is a representative information security risk management standard in the world and states:

- The estimated risk is a combination of the likelihood of an incident scenario (event) and its consequences.

Their relationships are shown in Figure 14.

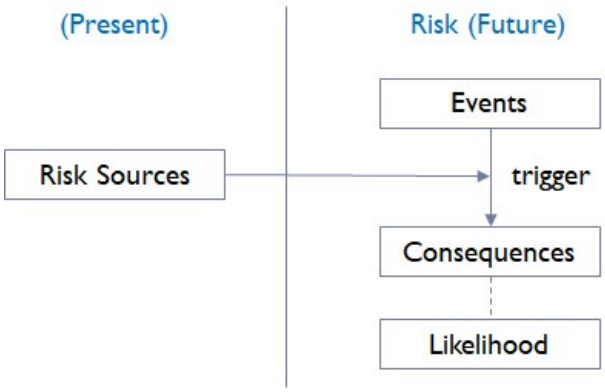

Figure 14. Risk Definitions in ISO 31000.

ISO 31000:2018 [1] also states:

- Control is measure that maintains and/or modifies risk.
- Options for modifying risk may involve: removing the risk source, changing the likelihood, and changing the consequences.

Their relationships are shown in Figure 15.

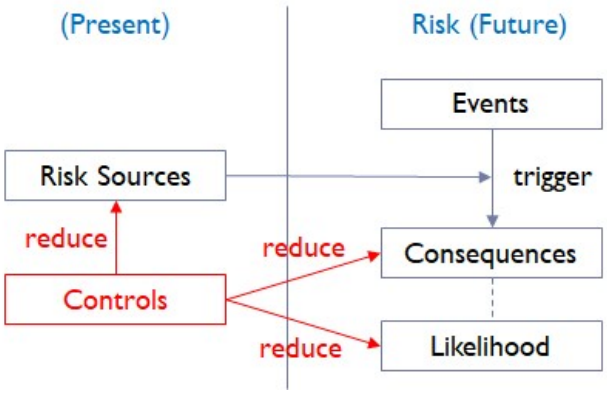

Figure 15. Control Definitions in ISO 31000.

Risk level is normally determined by a linear equation such as a combination of the likelihood of an incident scenario (event) and its consequences that are influenced by risk sources. As a result, the relationship between the factors affecting the risks and their effect on level of the risks can be drawn with a straight line (linear relationship) because the factors affecting the risks produce a constant proportion (liner behavior).

For example, a change affecting risk sources produce a proportional effect on the risk level through a corresponding change in likelihood of an event or its consequences. A change affecting controls also produce a proportional effect on the risk level through a corresponding change in likelihood of an event or its consequences.

3.3 Case Studies of Conventional Risk Management Approaches

3.3.1 Virus Infection Case

As a case study, a conventional risk management approach is applied to virus infection. Regarding risk sources of virus infection, the conventional risk management approach may:

- focus on an execution of malicious program on a computer (a snapshot of risk) and addresses it within an organization; and
- overlook the propagation of malicious program through cyberspace (a pattern of change of risk) and neglect to address the reinforcing feedback loop that shows non-linear outcomes of increasing number of infected computers connected to cyberspace.

The conventional risk management approach may view risk sources of virus infection as shown in Figure 16.

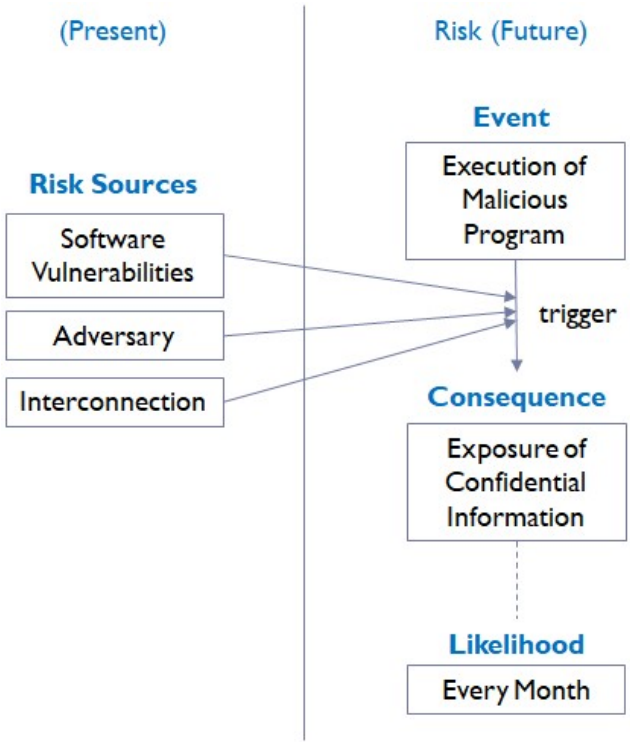

Figure 16. View of the Conventional Risk Management Approach about Risk Sources of Virus Infection.

For example, the conventional risk management approach may view that an increase in number of software vulnerabilities produce a proportional effect on the risk level through a corresponding increase in likelihood of an event: execution of malicious program. However, the risk level may increase exponentially by a large-scale effect of propagation of malicious program through cyberspace that produce an exponential effect on the consequence.

Regarding the controls for virus infection, the conventional risk management approach may:

- focus on a snapshot of risk and may implement excessive controls comparing it with a normal cyber risk appetite; and
- overlook the longer-term patterns of change of risk and neglects to address the real causes of those patterns: the implementation of controls may not produce a constant reduction of the level of cyber risk and their effects on cyber risk level may be different in the short-term and the long-term because of the time taken to implement controls (delay).

The conventional risk management approach may view the controls for virus infection as shown in Figure 17.

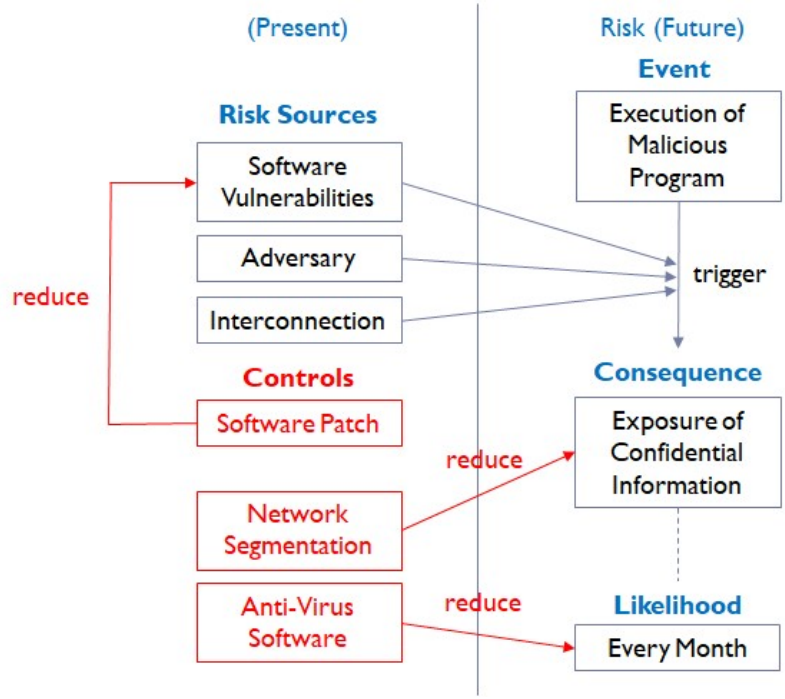

Figure 17. View of the Conventional Risk Management Approach about Controls for Virus Infection.

For example, the conventional risk management approach may view that an increase in controls such as applying software patches to devices produces a proportional effect on the risk level through a corresponding decrease in likelihood of an event: execution of malicious program. However, the risk level may fluctuate by different effects of the implementation of controls in the short-term and long term on the risk level by the delay of their implementation.

3.4 Limitations of Conventional Risk Management Approaches

3.4.1 Overview

As entities become more interconnected in cyberspace, management of cyber risk becomes more complex and dynamic and requires to see the patterns of change in cyberspace. Although conventional risk management approaches are well-established, their direct translation to cyberspace is not straightforward because of the global connectivity of cyberspace, the large number of entities and their interactions. The entities in cyberspace are tightly coupled and interact strongly with one another. Their actions feedback on themselves and alter the state of cyberspace, triggering others to act.

Conventional risk management approaches focus on events - snapshots of isolated parts of cyberspace and tends to ignore feedback processes and associated delays. Sterman [3] argues that ignorance of feedback processes occurs because of two basic and related deficiencies in our mental models. First, our cognitive maps of the causal

structure of systems are vastly simplified compared to the complexity of the systems themselves. Second, we are unable to infer correctly the dynamics of all but the simplest causal maps.

Our mental models learn from experience. Consequences that are not close in time and space are often beyond our experience. For example, through our experience, encouraging people to travel increases sales of travel industry. However, in the modern world where interactions of entities (people in this case) are complicated because of extensive connectivity (by various transport in this case) and, under the outbreak of coronavirus, the more people are encouraged to travel, the more infection spreads, and coronavirus grows in an exponential manner. Like the case in the research by Lammers et al. [2], the government may mistakenly perceive that travel just increases infections in a linear manner, underestimating its actual potential for exponential growth, and may try to encourage people to travel to increase sales of travel industry. As a result, exponential growth of coronavirus may force the government to put the restriction of travel to prevent infections from spreading, people's concern of infection during travel grows, and eventually sales of travel industry may decline. In reality, the root cause of decline of sales of travel industry is not an obvious thing like a decrease in travel but a lack of isolation of infected people in this circumstance. This failure to identify the root cause occurs because the government focuses on events. If the government identifies the feedback underlying the events, they can identify the correct root cause as well.

Conventional risk management approaches distract the organizations from seeing the long-term patterns of change that lie behind the events and from understanding the causes of those patterns. The long-term patterns of change provide clues to the structure that explains what event trends are and why. Although events are the most visible aspect of cyberspace, they are not always the most important.

The limitations of conventional risk management approaches are summarized as a lack of consideration of:

- Emergent properties of risk
- Dynamics of risk
- Visibility of the interrelationships among the factors affecting the risks

3.4.2 Lack of Consideration of Emergent Properties of Risk

As Groš [19] suggests that majority of today's analysis of systems is based on the reductionist approach, conventional risk management approaches are also based on it and decompose risk into its basic factors in a linear relationship, analyzes them separately and, based on those analyses, predict the behavior of the risk as a whole.

Conventional risk management approaches assume that there is no implication of the feedbacks created by the state of the risk, because the increase in risk remains in proportion to the increase in risk source even as the state of risk changes as shown in Figure 18.

Figure 18. A Linear Relationship between Risk Source and Risk.

Risk source and risk may not be in a linear relationship but in a feedback loop as shown in Figure 19, and they may allow cyber risk to exhibit behavior that couldn't be observed in its constituent parts. There is an implication of the feedbacks created by the state of the risk, because the increase in risk is amplified with a transformation on a scale completely different from risk source as the state of risk changes. It is expressed as a reinforcing feedback loop between risk source and risk.

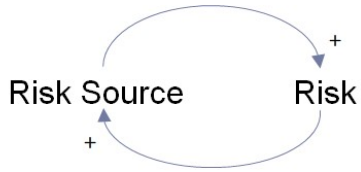

Figure 19. A Non-Linear Relationship between Risk Source and Risk.

The behaviors predicted by conventional risk management approaches can differ from the real situation because they do not concern the implications of the feedbacks.

In a linear world, such as the case with conventional risk management approaches based on equilibrium assumption, large-scale deviations from equilibrium (the normal state) can only be generated by large-scale causes that act with the same scale on the effect, that is, the outcome is a linear function of the cause. Instead, in a nonlinear world such as cyberspace, the tiny initiating events cause transformation on a scale completely different from their own and their effects are not proportional to their causes [17]. This emergent property of cyber risk is not considered by conventional risk management approaches.

3.4.3 Lack of Consideration of Dynamics of Risk

Sterman [3] argues that dynamics are what appears to be unchanging is, over a long-time horizon, seen to vary.

Conventional risk management approaches focus on a snapshot of risks and finds their causes and the low leverage that is close to the risks in time and space. It may overlook the longer-term patterns of change of risks and the causes of those patterns and neglects to find the high leverage that is not close to the risks in time and space.

Sterman [3] argues that people use various cues to causality including temporal and spatial proximity of cause and effect, temporal precedence of causes, covariation, and similarity of cause and effect. These heuristics lead to difficulty in complex systems where cause and effect are often distance in time and space, where actions have multiple effects, and where the delayed and distant consequences are different from and less salient than proximate effects (or simply unknown).

Conventional risk management approaches tend to point to specific events to explain the risk without seeing the structures underlying these events because they see the world as a sequence of events. It overlooks the long patterns of the risk and react to the events. As a result, it focuses on low leverage that may reduce the risk in the short run and often increase it in the long run.

Conventional risk management approaches have a lack of visibility of non-linear relationships between all related factors because they assume that the factors affect the behavior of the other factors instantly. In reality, the factor can affect only the future behavior of the other factors and there are always delays in affecting. Foresight is essential when there are long delays because responding to the cyber risk only when it becomes obvious is to miss an important opportunity to prevent emerging cyber risk from appearing.

3.4.4 Lack of Consideration of Visibility of the Interrelationships Among the Factors Affecting the Risks

Conventional risk management approaches have a lack of visibility of the dynamic interrelationships among the factors affecting the risks [18]. Without the visibility of the dynamic interrelationships among the factors affecting the risks, it is difficult for the organizations to:

- identify the real causes of risks; and
- know just where to work to address them.

The emergent properties of risks cannot be reduced to the mere properties of their parts. Visibility of the dynamic interrelationships among various factors at a level lower than that at which the behavior is observed leads to identification of the real causes of risks.

4 New Models for Cyber Risk Management

4.1 Requirements

4.1.1 Overview

The models need to be able to analyze and treat non-linear behaviors of cyber risk level to fill the gap between the nature of risks in cyberspace and view of conventional risk management approaches about it.

The models need to address the limitations of conventional risk management approaches considering:

- Emergent properties of risk that cannot be observed in its constituent parts with a focus on the interrelationships among the factors affecting the risks
- Dynamics of risk presented by the dynamic simulations that explore the nature of behaviors of cyber risk level over time
- Visibility of the dynamic interrelationships among the factors affecting the risks by use of graphical causal presentation

4.1.2 Cyber Risk Analysis

Analysis of non-linear behaviors of cyber risk level needs to provide useful information on how that pattern of the behaviors occurs.

Analysis of non-linear behaviors of cyber risk level needs to identify:

- Underlying causes of non-linear behaviors of cyber risk level at a level at which patterns of behavior can be changed
- Interrelationships and delays among the factors affecting the cyber risks that allows cyber risk level to exhibit non-linear behaviors

Specifically, the model needs to take into account:

- How the factors affecting the cyber risks can reinforce or balance each other through feedback loops.
- How propagation and scale-free causal development spirals into extreme events in cyberspace as an emergent property of cyber risk level.
- How business environments such as business growth and corresponding risk appetite change over time.
- How the dynamic interrelationships among the factors affecting the risks occur through graphical causal presentation.

4.1.3 Cyber Risk Treatment

Treatment of non-linear behaviors of cyber risk level needs to provide useful information that can be used to determine how that pattern of the behaviors might be influenced.

Treatment of non-linear behaviors of cyber risk level needs the simulations that:

- explore how the factors affecting the cyber risks influence non-linear behaviors of cyber risk level over time; and
- predict non-linear behaviors of cyber risk level and provides an opportunity to experiment with risk treatment decisions that control the behaviors.

The simulations explore the nature of behaviors of cyber risk level where experimentation on the cyber risk level is infeasible.

4.1.4 Model Validation

While it is not easy to prove that the model meets these requirements, it can be justified through the successful application of this model to actual cases in dynamic simulation.

4.2 Methodologies

4.2.1 Overview

Systems thinking can describe non-linear relationships between the factors and their effects that are not close in time and space in graphical causal presentation. It helps the model to consider emergent properties of cyber risk and visibility of the dynamic interrelationships among the factors affecting the cyber risk. Systems thinking can be applied to develop the Feedback Loop Diagram for cyber risk analysis to identify the structure underlying non-linear behaviors of cyber risk level.

System dynamics is based on systems thinking and can simulate the non-linear behaviors of cyber risk level over time and provides an opportunity to experiment with solutions that control the behaviors. It helps the models to consider dynamics of cyber risk. System dynamics can be applied to develop the Stock and Flow Diagram for cyber risk treatment to simulate the structure underlying non-linear behaviors of cyber risk level.

System thinking and system dynamics address the limitations of conventional risk management approaches.

4.2.2 Systems Thinking

4.2.2.1 Concept

Meadows [22] explains that a system is a set of things – people, cells, molecules, or whatever – interconnected in such a way that they produce their own pattern of behavior over time.

Groš [19] explains that the general features of any complex system are:

- The system has internal structure.
- The system has behavior that is not observed in its constituent parts.
- System adapts to inputs and evolves.
- There is uncertainty in the system.

Heylighen [16] argues that cyberspace is a complex system that emerges from interactions of various autonomous entities and exhibits propagation and scale-free features. Cyber risk management is itself a complex process because it emerges from cyberspace.

McNamara [23] argues that systems thinking is a way of helping a person to view complex systems from a broad perspective that includes seeing overall structures and patterns in systems:

- to identify the real causes of issues; and
- to know just where to work to address them.

Systems thinking can describe cyber risks in a rich language with a focus on interrelationships rather than linear cause-effect chains, and patterns of change rather than snapshots. It helps the organizations facing many urgent cyber risks to see the structure underlying the patterns of change of the cyber risks and find the most effective controls. It is difficult for the organizations to see the structure unless they look for long-term behavior rather than short-term events. It provides the organizations the way to see the snapshot of cyber risk as parts of trends. Heylighen [16] argues that the emergent properties of risks cannot be reduced to the mere properties of their parts but the interrelationships among various factors at a level lower than that at which the behavior is observed.

4.2.2.2 Structure and Behavior

Sterman [3] argues that the behavior of a complex system arises from its structure. Senge [24] argues that structure influences behavior over time and addresses the underlying causes of behavior at a level at which patterns of behavior can be changed.

View of systems thinking about the patterns of change of the cyber risk level is shown in Figure 20.

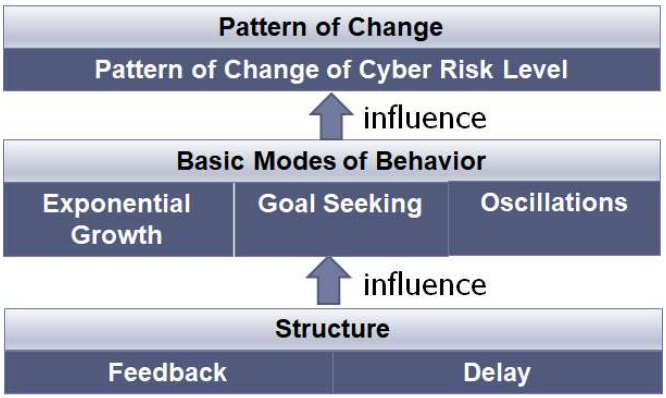

Figure 20. View of Systems Thinking about Cyber Risk.

The structure consists of the feedbacks and delays. Seeing circles of influence rather than straight lines is important for the organizations to see the real cyber risk.

Sterman [3] argues that all dynamics of complex systems arise from the interaction of just two types of feedback loops, reinforcing feedback loops and balancing feedback loops. All dynamics arise from reinforcing feedback loop amplifies whatever movement occurs, producing more movement in the same direction. In the situation where cyber risk is growing, reinforcing feedback loop is working. Balancing feedback loop is always operating to reduce a gap between what is desired and what exists. In the situation where cyber risk is being kept at an organization's acceptable level, balancing feedback loop is working. Reinforcing feedback loop consists of risk sources drives cyber risk level and balancing feedback loop consists of controls constrains it.

Feedback loop may contain delays that are interruptions in the flow of influence which make the consequences of actions occur gradually. Feedbacks with delays may not matter in the short term but the long term. Delays are strong determinants of behavior. Changing the length of a delay may make a large change in the behavior of the complex systems.

Behaviors of the complex systems often arise as the relative strengths of the specific type of feedback loop. Sterman [3] argues that the basic modes of behavior of complex systems are identified along with the feedback structures generating them. These modes are:

- Exponential growth, created by reinforcing feedback
- Goal seeking, created by balancing feedback
- Oscillation, created by balancing feedback with delays

Exponential growth arises from reinforcing feedback. The larger the quantity, the greater its net increase, further augmenting the quantity and leading to ever-fast growth.

Goal seeking arises from balancing feedback. Every negative loop includes a process to compare the desired and actual conditions and take corrective action. Large gaps

between desired and actual states tend to generate large responses while small gaps tend to generate small responses.

Oscillation arises from balancing feedback with delays. The state of the system constantly overshoots its equilibrium state, reserves, then undershorts, and so on. The delays cause corrective actions to continue even after the state of the system reaches its goal, forcing the system to adjust too much, and triggering a new correction in the opposite direction.

These basic modes of behavior are common to large variety of situations.

4.2.2.3 Root Cause and Leverage

Underlying causes of behavior are identified by finding the structure that is responsible for it. Observation of basic modes of behaviors leads to the identification of the corresponding structure. For example, if exponential growth is observed, reinforcing feedback is dominant. Then the hypothesis is made where reinforcing process is and examined by the simulation. High leverage that leads to significant improvement of the behaviors with a minimum of effort may be found there. Identifying where delays occur in systems is also important to understand the behavior of the systems. Changing the length of a delay may utterly change the behavior.

In systems thinking, the structure rather than the individual factor is responsible for the cyber risk.

4.2.2.4 Diagram

Feedback Loop Diagram shows how changes in one element A have an impact on another element B, and then on the original element A as shown in Figure 21.

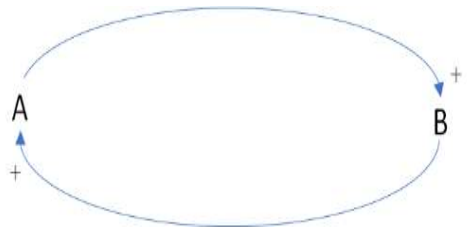

Figure 21. An Example of Feedback Loop Diagram.

Arrows indicate the direction of causal influences. Signs at arrow heads (+ or -) indicate the polarity of the relationship. A positive polarity, indicated by +, means an increase in the independent variable increases the dependent variable (and a decrease decreases). Negative signs mean an increase (decrease) in the independent variable decreases (increases) the dependent variable.

4.2.3 System Dynamics

System dynamics [25] based on systems thinking is an approach to understanding the non-linear behavior of complex systems over time using stocks, flows, feedback loops, table functions and delay.

- Stocks represent quantities of tangible and/or intangible entities that have incoming and/or outgoing flows. Stocks change over time through the actions of the flows. The symbol for a stock is a rectangle.
- Flows are equivalent to valves, that is a device the setting for how much quantity may flow into or out of a stock in a given time period.
- Cloud is a metaphysical flow and indicates a boundary.
- Converters are constants or calculations based on other entities.

Figure 22 shows the Stock and Flow Diagram converted from the example of Feedback Loop Diagram shown in Figure 21 by use of system dynamics.

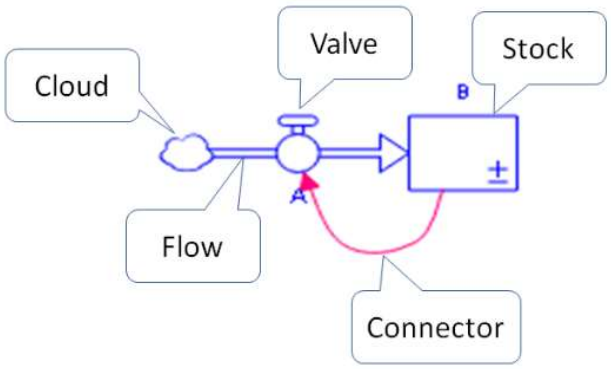

Figure 22. An Example of Stock and Flow Diagram.

A feedback loop is formed when changes in stock have an impact on the flows into or out of the same stock. A feedback loop is a closed chain of causal connections from a stock, through a set of decisions that are dependent on the level of the stock, and back again through a flow to change the stock.

If the stock represents cyber risk level, it can be hypothesized that the organizations monitor cyber risk level in the stock and make decisions to lower the cyber risk level or to keep it with acceptable ranges. The organizations regulate the cyber risk level in the stock by manipulating flows. Incoming flows are the risk sources to increase the cyber risk level and outgoing flows are the controls to decrease the cyber risk level.

System dynamics is a tool that can quantify the behavior of the structure. The values of the variable stocks and flows are computed each period through simultaneous difference equations. Different “runs” with different initial conditions of the simulation are performed. These values for each run are collected. Output from a simulation is analyzed statistically to discover recurring trends.

4.3 Contributions

The new models are developed to meet the requirements described in section 4.1 using the methodologies described in section 4.2. They analyze and treat non-linear behavior of cyber risk level to complement conventional risk management approaches.

At an organization level, a new model called Dynamic Cyber Risk Model (DCRM) is developed to analyze and treat oscillation behavior of cyber risk level. DCRM Feedback Loop Diagram is developed for cyber risk analysis to identify the real causes of fluctuation of cyber risk level that leads to the implementation of excessive controls. DCRM Stock and Flow Diagram is developed by conversion of DCRM Feedback Loop Diagram for cyber risk treatment to get useful information to determine where to work to address the causes.

This view of DCRM is shown in Figure 23.

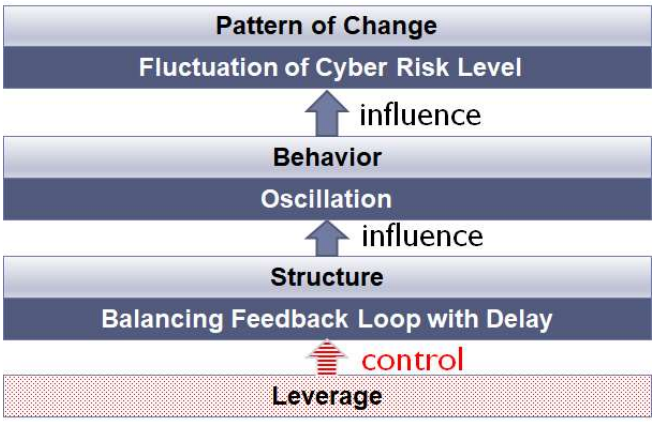

Figure 23. View of DCRM about Cyber Risk.

Using DCRM, information security governance team of the organization can find the appropriate approach to optimize the balance of the cyber risk level and cost of controls at an organization level with the guidance on avoiding the implementation of excessive controls while accepting cyber risk level exceeding cyber risk appetite to some extent for a certain period of time.

At an individual cyber-attack level, a new model called Power of Cyberspace Model (POCM) is developed to analyze and treat exponential growth behavior of cyber risk level. POCM Feedback Loop Diagram is developed for cyber risk analysis to identify the real causes of an extreme effect of cyber-attack on cyber risk level. POCM Stock and Flow Diagram is developed by conversion of POCM Feedback Loop Diagram for cyber risk treatment to get useful information to determine where to work to address the causes.

This view of POCM is shown in Figure 24.

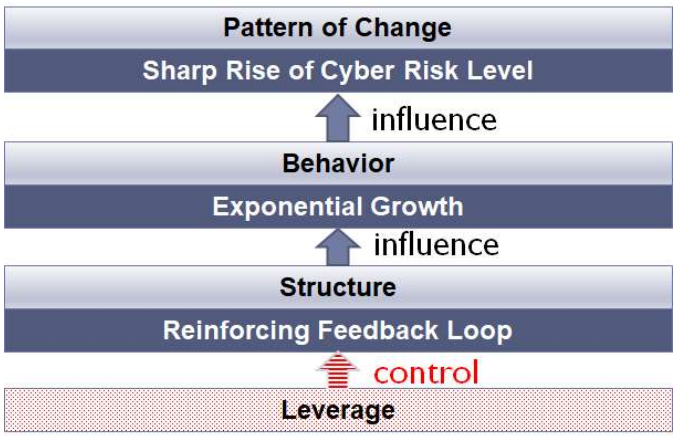

Figure 24. View of POCM about Cyber Risk.

Using POCM, information security management team of the organization can find the appropriate approach to effectively reduce the extreme impact of the specific cyber-attack on the organization with the guidance on the treatment of infected devices.

5 Dynamic Cyber Risk Model (DCRM)

5.1 Background

Corporate Value-Based Cyber Risk Model was developed by Ohki et al. [26]. The objective of the model is the quantification of the risks that arise from dependence of business on cyberspace (cyber risk). In this model, "Cyber Risk Level" is identified and calculated from four components. They are "Corporate Value", "Cyber Ratio", "Target Ratio" and "Protection Ratio". Calculation steps are as below:

1. "Corporate Value" is calculated by sum of "Asset Value", "Process Value" and "Capability Value". "Asset Value" is past value accumulated in the asset and shown in balanced sheet. "Process Value" is current value created from business processes. "Capability Value" is source of future competitiveness and utilizes resource-based view.
2. "Cyber-Accessible Corporate Value" is calculated by multiplying "Corporate Value" by "Cyber Ratio". "Cyber Ratio" is the ratio of corporate assets, processes and capabilities that are accessible from cyberspace.
3. "Cyber-Targeted Corporate Value" is calculated by multiplying "Cyber-Accessible Corporate Value" by "Target Ratio". "Target Ratio" is the likelihood that cyber-attacks occur.
4. "Cyber Risk Level" is calculated by multiplying "Cyber-Targeted Corporate Value" by (1 – "Protection Ratio"). "Protection Ratio" is the likelihood that the implementation of controls prevents cyber-attacks from occurring.

This calculation is summarized in Figure 25.

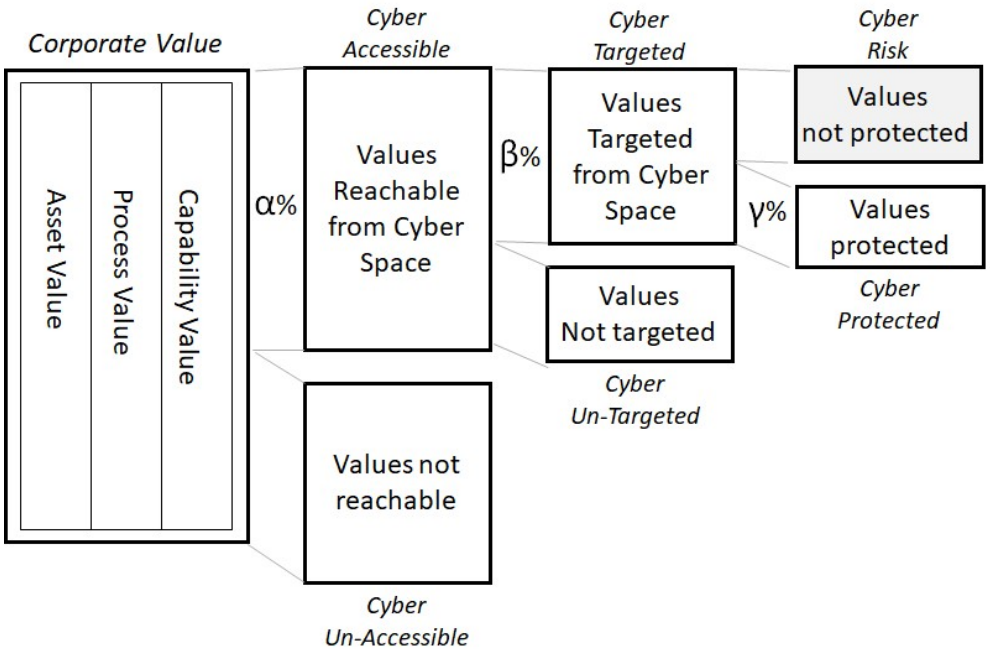

Figure 25. Corporate Value-Based Cyber Risk.

The ratios used in the calculation are summarized in Figure 26.

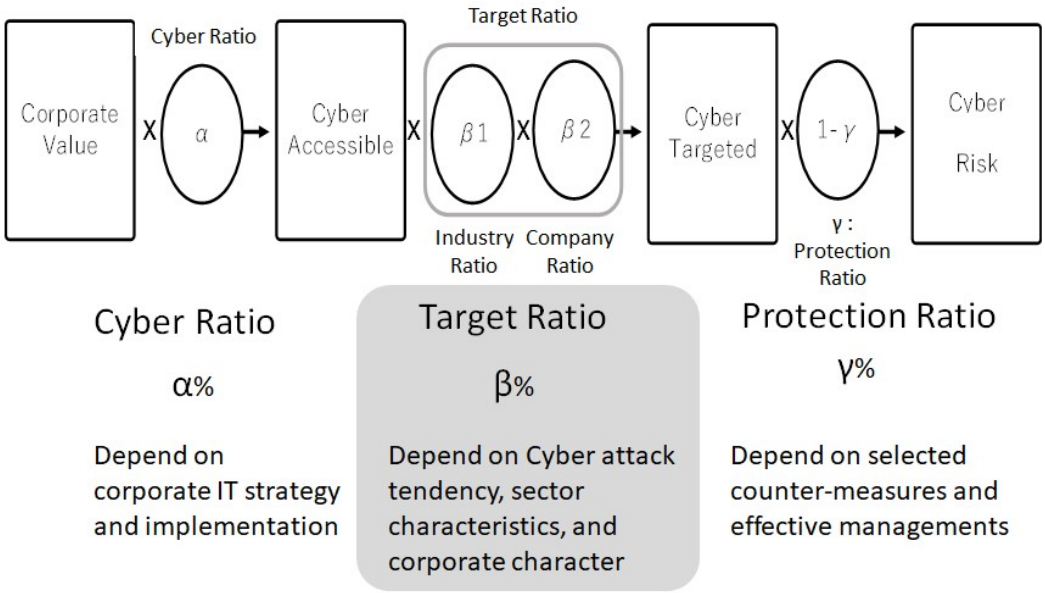

Figure 26. Ratios.

Although the Corporate Value-Based Cyber Risk Model successfully analyzes "Cyber Risk Level", it focuses on a snapshot of cyber risks. The model has a difficulty in analyzing patterns of change of "Cyber Risk Level" where effects of controls on "Cyber Risk Level" is different in the short-term and the long-term. Without considering real causes of these patterns of change, there are some possibilities that excessive controls may be implemented. To solve this issue, DCRM is created by application of systems thinking to the Corporate Value-Based Cyber Risk Model.

5.2 Concept

DCRM uses graphs of behavior of "Cyber Risk Level" to understand trends over time, rather than focusing attention on individual factors affecting the "Cyber Risk Level".

For example, it helps the organizations to see how the implementation of controls influences the "Cyber Risk Level" over time through their interrelationships and delays (structure) and to gain insight into the leverage. It is assumed that interrelationships exist among "Cyber-Accessible Corporate Value", "Target Ratio " and "Protection Ratio" that compose "Cyber Risk Level" defined in Corporate Value-Based Cyber Risk Model.

Using DCRM, organizations can analyze how oscillation behavior of "Cyber Risk Level" occurs (cyber risk analysis) and get useful information to find how that behavior might be influenced (cyber risk treatment).

This view of DCRM is shown in Figure 27.

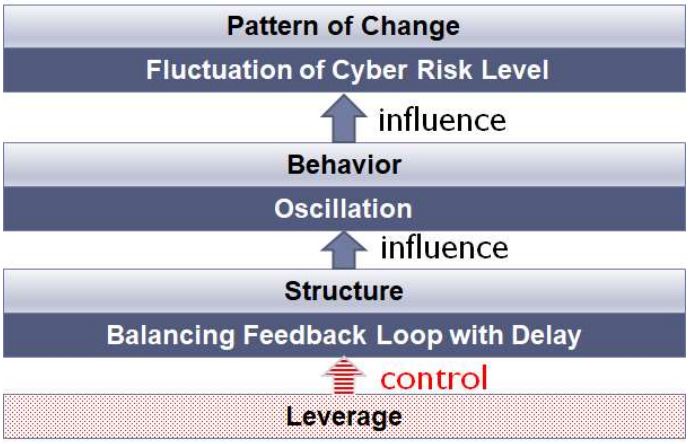

Figure 27. View of DCRM about Cyber Risk.

Oscillation behavior of "Cyber Risk Level" is created by the structure that includes balancing feedback loop among the factors affecting the cyber risk and results in a fluctuation of "Cyber Risk Level". Treatment of a fluctuation of "Cyber "Risk Level" requires addressing the structure underlying oscillation behavior of "Cyber Risk Level".

5.3 Cyber Risk Analysis

5.3.1 Overview

DCRM Feedback Loop Diagram is developed by application of systems thinking to the Corporate Value-Based Cyber Risk Model for cyber risk analysis to identify the real causes of fluctuation of "Cyber Risk Level" that leads to the implementation of excessive controls.

Development of DCRM Feedback Loop Diagram requires the identification of the factors and their relationships in the context of analysis of oscillation behavior of "Cyber Risk Level".

5.3.2 Development of DCRM Feedback Loop Diagram

5.3.2.1 Identification of the Factors Related to Analysis of Cyber Risk Level and Their Relationships

The following factors affecting "Cyber Risk Level" are identified as components of Corporate Value-Based Cyber Risk Model:

- Cyber-Accessible Corporate Value
- Target Ratio
- Protection Ratio

An increase in “Cyber-Accessible Corporate Value” generates an increase in “Cyber Risk Level”. According to ISO/IEC 27005:2018 [4], the estimated risk is a combination of the likelihood of an incident scenario (event) and its consequences. An increase in “Cyber-Accessible Corporate Value” increases the consequences of an incident and then becomes one of the factors to increase “Cyber Risk Level”. An increase in “Target Ratio” increases the likelihood of an incident and then becomes one of the factors to increase “Cyber Risk Level”.

According to ISO 31000:2018 [1], control is measure that maintains and/or modifies risk. An increase in “Protection Ratio” means an increase in likelihood that the implementation of controls prevents cyber-attacks from occurring then it becomes one of the factors to decrease “Cyber Risk Level”.

These factors and their relationships are drawn in DCRM Feedback Loop Diagram as shown in Figure 28.

Figure 28. DCRM Feedback Loop Diagram – First Step.

5.3.2.2 Identification of the Factors Related to Cyber-Accessible Corporate Value and Their Relationships

The following factors are identified to complement “Cyber-Accessible Corporate Value”:

- Targeted Cyber-Accessible Corporate Value
- Cyber-Accessible Corporate Value to be Created

“A proposal of cyber security risk modeling based on corporate values for business executives” by Ohki et al. [26] mentions that the mission of business executives is increasing corporate value.

If “Cyber-Accessible Corporate Value” does not reach the target (“Targeted Cyber-Accessible Corporate Value”), business activities are conducted to fill the gap (“Cyber-Accessible Corporate Value to be Created”).

An increase in “Cyber-Accessible Corporate Value” caused by business activities fills the gap and “Cyber-Accessible Corporate Value to be Created” decreases. On the other hand, an increase in “Targeted Cyber-Accessible Corporate Value” increases the gap and “Cyber-Accessible Corporate Value to be Created” increases.

These factors and their relationships are added to DCRM Feedback Loop Diagram as shown in Figure 29.

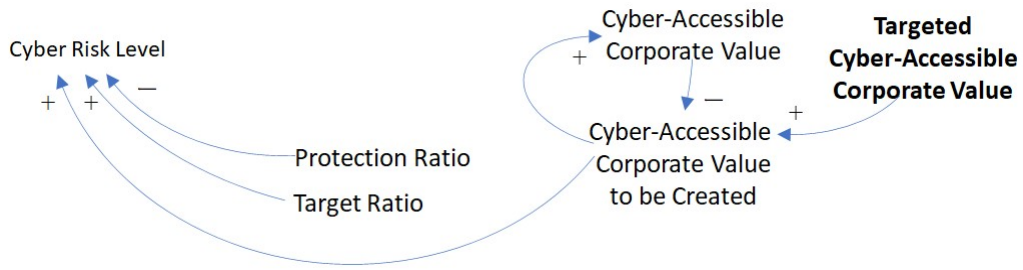

Figure 29. DCRM Feedback Loop Diagram – Second Step.

5.3.2.3 Identification of the Factors Related to Classification of Cyber Risk Level and Their Relationships

The following factors are identified to classify "Cyber Risk Level":

- Level of New Cyber Risk
- Level of Residual Cyber Risk

"Cyber Risk Level" is generated by a specific business cycle as shown in Figure 29 and it is categorized as "Level of New Cyber Risk". "Level of New Cyber Risk" is accumulated over time and it is categorized as "Level of Residual Cyber Risk".

These factors and their relationships are added to DCRM Feedback Loop Diagram as shown in Figure 30.

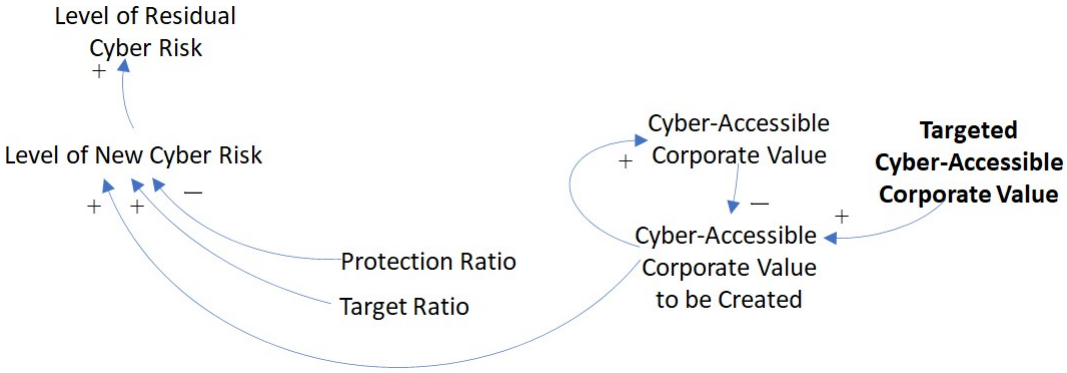

Figure 30. DCRM Feedback Loop Diagram – Third Step.

5.3.2.4 Identification of the Factors Related to Evaluation of Cyber Risk Level and Their Relationships

The following factors are identified to evaluate "Cyber Risk Level":

- Cyber Risk Appetite
- Level of Cyber Risk to be Treated

Business executives choose to reduce “Level of Residual Cyber Risk” exceeding “Cyber Risk Appetite”. “Level of Residual Cyber Risk” exceeding “Cyber Risk Appetite” is called “Level of Cyber Risk to be Treated”. According to ISO/IEC 27005:2018 [4], level of risks should be compared against risk evaluation criteria and risk acceptance criteria. An increase in “Level of Residual Cyber Risk” becomes one of the factors to increase “Level of Cyber Risk to be Treated” while an increase in “Cyber Risk Appetite” becomes one of the factors to decrease “Level of Cyber Risk to be Treated”.

These factors and their relationships are added to DCRM Feedback Loop Diagram as shown in Figure 31.

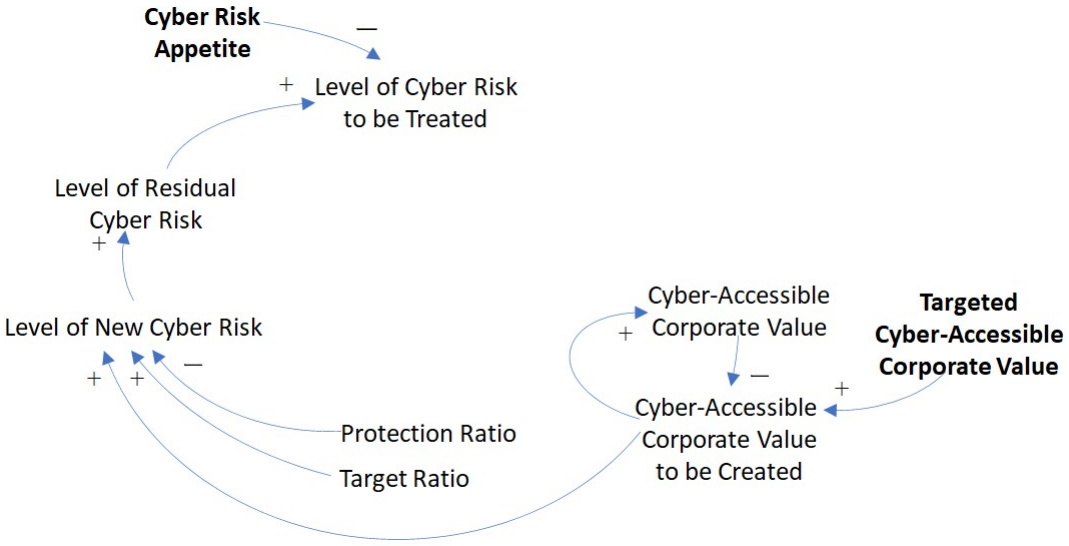

Figure 31. DCRM Feedback Loop Diagram – Fourth Step.

5.3.2.5 Identification of Factors Related to Treatment of Cyber Risk Level and Their Relationships

The factors are identified to treat cyber risk level with controls as shown in Table 2:

Table 2. Factors and Status of Controls

Factors	**Status of Controls**
Level of Cyber Risk to be Treated	Not yet implemented
Level of Cyber Risk under Treatment	Under implementation
Level of Cyber Risk Treated	Implemented

“Level of Cyber Risk to be Treated” is “Level of Residual Cyber Risk” exceeding “Cyber Risk Appetite”. It normally takes some time to reduce “Level of Cyber Risk to be Treated” by the implementation of controls. Therefore, treatment of “ Level of Cyber Risk to be Treated” has three stages: “to be Treated”, “under Treatment”, and “Treated”. “Level of Cyber Risk to be Treated” is the Level of Cyber Risk that needs to be treated but not yet done so. “Level of Cyber Risk under Treatment” is the Level

of Cyber Risk that needs to be treated and under treatment by the controls. "Level of Cyber Risk Treated" is the Level of Cyber Risk that is already reduced by the implemented controls. Table 2 shows these factors that show "Level of Cyber Risk to be Treated" in each stage in association with the status of controls. There is a delay from "under Treatment" to "Treated" stage. It indicates the time taken to implement controls.

An increase in "Level of Cyber Risk to be Treated" is a cause of an increase in " Level of Cyber Risk under Treatment" that is a cause of an increase in "Level of Cyber Risk Treated" with a delay. An increase in "Level of Cyber Risk Treated" is a cause of a decrease in "Level of Cyber Risk under Treatment", "Level of Cyber Risk to be Treated" and "Level of Residual Cyber Risk".

These factors and their relationships are added to DCRM Feedback Loop Diagram as shown in Figure 32.

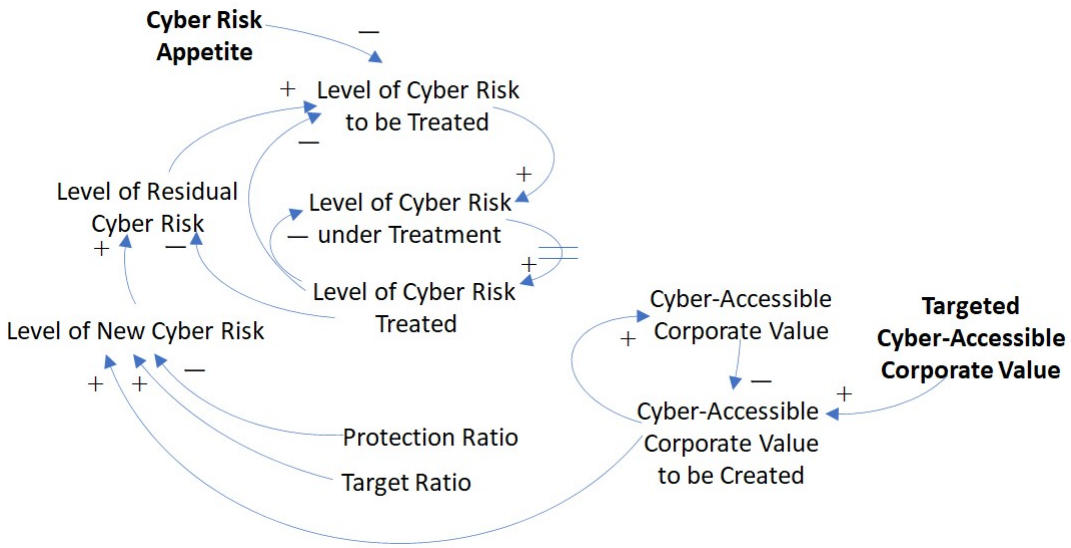

Figure 32. DCRM Feedback Loop Diagram – Final Step.

5.3.2.6 Completion of Development of DCRM Feedback Loop Diagram

The complete DCRM Feedback Loop Diagram is developed as shown in Figure 32. It incorporates all factors and their relationships in the context of analysis of oscillation behavior of cyber risk level.

5.3.3 Scenario from DCRM Feedback Loop Diagram

A particular pattern of change of cyber risk level expected by the structure is identified by DCRM Feedback Loop Diagram. It is explained as below:

- Because of the delay, the implementation of controls does not produce a constant reduction of the "Level of Residual Cyber Risk". (non-linear relationship).

- The “Level of Residual Cyber Risk” sometimes unexpectedly rises in the short-term because effects of controls on “Level of Residual Cyber Risk” is different in the short-term and the long-term.
- If such a “Level of Residual Cyber Risk” is compared with a normal “Cyber Risk Appetite”, there are some possibilities that excessive controls may be implemented, and productivities and usability of controls may be undermined.

5.4 Cyber Risk Treatment

5.4.1 Overview

DCRM Stock and Flow Diagram is developed by application of system dynamics for cyber risk treatment to get useful information to determine where to work to address the causes of fluctuation of cyber risk level that leads to the implementation of excessive controls. DCRM Stock and Flow Diagram is simulated to determine how oscillation behavior of cyber risk level might be influenced.

Development of DCRM Stock and Flow Diagram requires the conversion of DCRM Feedback Loop Diagram.

5.4.2 Conversion of DCRM Feedback Loop Diagram into DCRM Stock and Flow Diagram

5.4.2.1 Overview

During the conversion of the DCRM Feedback Loop Diagram into the DCRM Stock and Flow Diagram by application of system dynamics, the factors shown in DCRM Feedback Loop Diagram are assigned to the stocks, flows and converters used in system dynamics while their relationships are kept.

5.4.2.2 Stocks

The following factors are quantities of entities that have incoming and/or outgoing flows. Therefore, they are assigned to stocks:

- Level of Residual Cyber Risk
- Level of Cyber Risk under Treatment
- Cyber-Accessible Corporate Value

In the Corporate Value-Based Cyber Risk Model developed by Ohki et al. [26], cyber risk level is expressed in amount of money. Because the main factors shown in DCRM come from the Corporate Value-Based Cyber Risk Model, cyber risk level in DCRM is also expressed in amount of money.

5.4.2.3 Flows

The following factors are incoming or outgoing flows for the stocks. Therefore, they are assigned to flows:

- Level of Cyber Risk to be Treated (Incoming flow for "Level of Cyber Risk under Treatment")
- Level of Cyber Risk Treated (Outgoing flow for "Level of Cyber Risk under Treatment")
- Level of New Cyber Risk (Incoming flow for "Level of Residual Cyber Risk")
- Level of Residual Cyber Risk Reduced (Outcoming flow for "Level of Residual Cyber Risk")
- New Cyber-Accessible Corporate Value Created (Incoming flow for "Cyber-Accessible Corporate Value")

5.4.2.4 Converters

The following factors are not stocks nor flows but constants or calculations based on other factors. Therefore, they are assigned to converters:

- Cyber Risk Appetite
- Targeted Cyber-Accessible Corporate Value
- Cyber-Accessible Corporate Value to be Created
- Protection Ratio
- Target Ratio

The following new factors are assigned to converters to determine where to work to address the causes of fluctuation of cyber risk level:

- Treatment Delay
- Treatment Ratio
- Cyber Risk Appetite Coefficient
- Targeted Cyber-Accessible Corporate Value Coefficient

"Treatment Delay" indicates the time taken to allow "Level of Cyber Risk under Treatment" to be "Level of Cyber Risk Treated" by completion of implementation of controls. "Treatment Ratio" indicates the ratio of "Level of Cyber Risk under Treatment" that becomes "Level of Cyber Risk Treated" by completion of implementation of controls. "Cyber Risk Appetite" is determined as the product of "Targeted Cyber-Accessible Corporate Value" by "Cyber Risk Appetite Coefficient". "Targeted Cyber-Accessible Corporate Value" is the product of "Cyber-Accessible Corporate Value" by "Targeted Cyber-Accessible Corporate Value Coefficient".

5.4.2.5 Completion of Conversion into DCRM Stock and Flow Diagram

The complete DCRM Stock and Flow Diagram is developed by conversion of DCRM Feedback Loop Diagram as shown in Figure 33. It incorporates all factors converted

and their relationships in the context of treatment of oscillation behavior of cyber risk level.

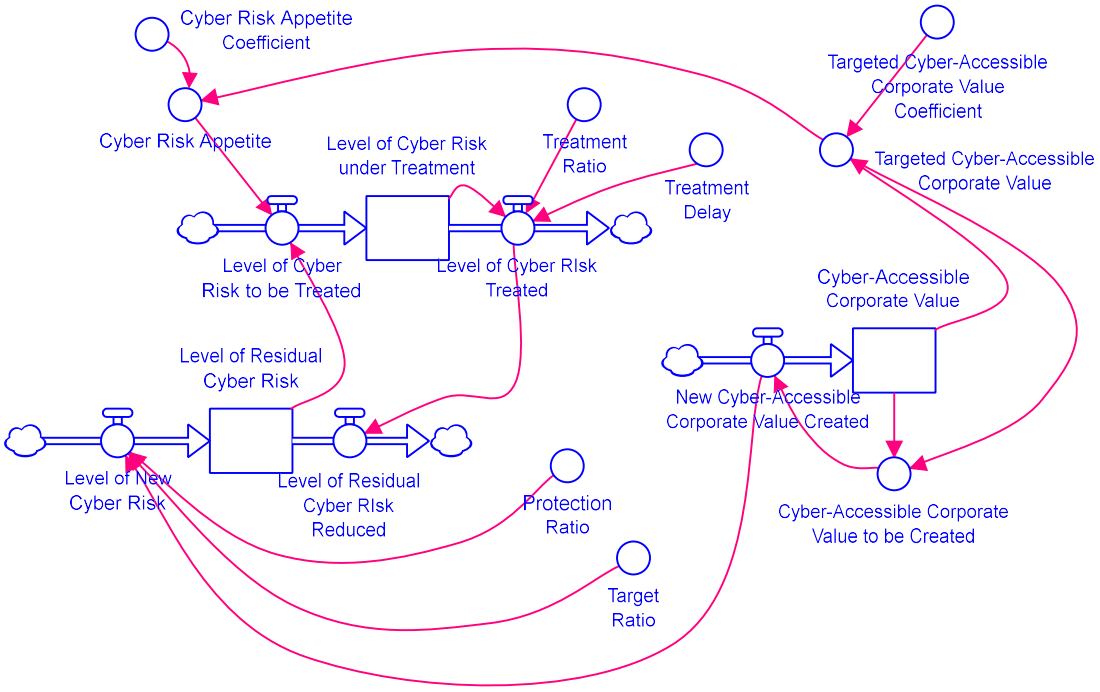

Figure 33. DCRM Stock and Flow Diagram.

5.4.3 Assumption of Simulation

5.4.3.1 Overview

The simulation of DCRM Stock and Flow Diagram needs to accord with reality. For the setting of environment in which the organization manages cyber risk, the values that faithfully represent reality are carefully chosen as shown in Table 3.

Table 3. Default Values of the Organization

Factors	Default Values
Targeted Cyber-Accessible Corporate Value Coefficient	1.1 (110%)
Cyber-Accessible Corporate Value	100 Billion Yen
Cyber Risk Appetite Coefficient	0.01 (1%)
Target Ratio	0.2 (20%)
Protection Ratio	0.6 (60%)
Treatment Ratio	1.0 (100%)1st Simulation
Treatment Delay	1.0 (1 Year Delay)2nd/3rd Simulation
Level of Residual Cyber Risk	2 Billion Yen
Level of Cyber Risk under Treatment	0 Yen

All those values remain unchanged during all simulations except “Cyber-Accessible Corporate Value”, “Level of Residual Cyber Risk” and “Level of Cyber Risk under Treatment”.

A change of “Cyber-Accessible Corporate Value” produce a proportional effect of the “Level of Residual Cyber Risk” during all simulations.

A change of “Treatment Delay” produces a disproportionate effect of the “Level of Residual Cyber Risk” during first simulation.

A change of “Treatment Ratio” softens a disproportionate effect of the “Level of Residual Cyber Risk” produced by “Treatment Delay” during second and third simulations.

5.4.3.2 Targeted Cyber-Accessible Corporate Value Coefficient

Compound annual growth rate (CAGR) of Nikkei average stock for 10 years from 2009 to 2018 is 10.02%. Therefore, “Targeted Cyber-Accessible Corporate Value Coefficient” is set to 1.1 and it is assumed that “Cyber-Accessible Corporate Value” grows by 10% every year. “Targeted Cyber-Accessible Corporate Value Coefficient” remains unchanged during simulation.

5.4.3.3 Cyber-Accessible Corporate Value

The unlisted technology companies whose value is more than $ 1 billion are called unicorn companies and widely noticed [27]. Because most asset of these companies are likely to be cyber-accessible, “Cyber-Accessible Corporate Value” of typical companies whose business are relying on cyberspace is set to 100 billion yen ($ 1 billion).

5.4.3.4 Cyber Risk Appetite Coefficient

According to the 23rd Corporate IT Trend Survey by JUAS [28], the companies invest around 1% of amount of sales in IT. Most IT investment is likely related to cyber risk treatment nowadays. Risk treatment normally requires balancing the risk level and cost of the risk treatment and investment in IT including security is made in proportion to risk appetite. Therefore, “Cyber Risk Appetite” is set to 1% of “Targeted Cyber-Accessible Corporate Value”. “Cyber Risk Appetite Coefficient” remains unchanged during simulation.

5.4.3.5 Target Ratio

According to IPA’s report [29], the likelihood that cyber-attacks occur is 19.3% so that “Target Ratio” is set to 20%. “Target Ratio” remains unchanged during simulation.

5.4.3.6 Protection Ratio

According to IPA's report [29], 22% of the organizations that receives cyber-attack suffer visible damage. Based on the assumption that the impact of the cyber-attack on information assets may not be visible and actual likelihood that information assets are not protected is 40%, "Protection Ratio" is set to 60%. "Protection Ratio" remains unchanged during simulation.

5.4.3.7 Treatment Ratio

"Treatment Ratio" is set to 100% during 1st simulation.

5.4.3.8 Treatment Delay

"Treatment Delay" is set to 1 Year Delay during 2nd and 3rd simulations.

5.4.3.9 Level of Residual Cyber Risk

"Level of Residual Cyber Risk" is set to 2 billion yen that is just above "Cyber Risk Appetite" initially to trigger risk treatment at the beginning of the simulation.

5.4.3.10 Level of Cyber Risk under Treatment

"Level of Cyber Risk under Treatment" is set to 0 yen based on that assumption that the company has not yet started any risk treatment before the beginning of the simulation.

5.4.4 First Simulation

5.4.4.1 Overview

Why oscillation behavior of cyber risk level occurs is simulated by DCRM Stock and Flow Diagram. In Figure 34, the simulation shows how the patterns of the "Level of Residual Cyber Risk" is influenced by changing "Treatment Delay" for 12 years as below:

- Run 1: 0.0 (0 Year Delay)
- Run 2: 0.2 (0.2 Year Delay)
- Run 3: 0.4 (0.4 Year Delay)
- Run 4: 0.7 (0.7 Year Delay)
- Run 5: 1.0 (1 Year Delay)

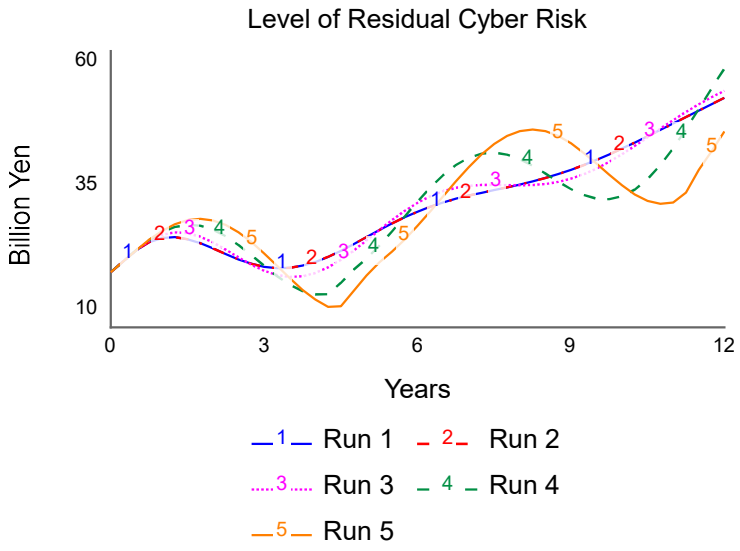

Figure 34. Patterns of Level of Residual Cyber Risk Influenced by Delay of Implementation of Controls.

This simulation is based on the assumption that any factors that are not related to cyber risks remain unchanged.

5.4.4.2 Calculation Settings

Values of variables are calculated at regular intervals. Interval is set to quarter by taking into account that accurateness of calculation and computational load. Shorter interval improves accurateness of calculation. Longer interval reduces computational load.

5.4.4.3 Initial Calculations

In the first round of the calculation, "Level of Residual Cyber Risk" exceeding "Cyber Risk Appetite" is assigned to "Level of Cyber Risk to be Treated".

In the second round of the calculation, "Level of Cyber Risk to be Treated" is added to "Level of Cyber Risk under Treatment" as the controls are under implementation and then "Level of Cyber Risk to be Treated" is reset.

In the third round of the calculation, if "Treatment Delay" is none, "Level of Cyber Risk under Treatment" is reduced and assigned to "Level of Cyber Risk Treated" while "Level of Residual Cyber Risk" exceeding "Cyber Risk Appetite" may be assigned to "Level of Cyber Risk to be Treated" if there is. If there is a "Treatment Delay", "Level of Cyber Risk under Treatment" averaged over the interval specified by "Treatment Delay" is reduced and assigned to "Level of Cyber Risk Treated". It takes into account that cyber risk level is reduced gradually at the interval specified by "Treatment Delay" from the outset of the implementation of controls in reality.

5.4.4.4 Way to Calculate "Level of Cyber Risk under Treatment"

"Level of Cyber Risk under Treatment" is calculated at the specific point, and then the implementation of the controls that reduces "Level of Cyber Risk under Treatment" to zero is initiated. "Level of Cyber Risk under Treatment" calculated at the specific point is reduced to zero when the implementation of the controls is completed after the time specified by "Treatment Delay" passes. It is based on the typical risk management processes where risk level is determined at the specific interval and then treated collectively. Although there are various types of controls to treat each cyber risk, and the time taken to implement these controls varies in reality, it is assumed that the time taken to implement the controls collectively for cyber risk level determined at the specific interval is specified by "Treatment Delay" in the simulation. It makes it easier to see the impact of the time taken to implement the controls on the patterns of the "Level of Residual Cyber Risk". If the time taken to implement the controls varies greatly, its impact on the patterns of the "Level of Residual Cyber Risk" may be smaller.

5.4.5 Second and Third Simulations

5.4.5.1 Overview

How oscillation behavior of cyber risk level might be influenced is simulated by DCRM Stock and Flow Diagram. In Figure 35 and 36, the second and third simulations show how the patterns of the "Level of Residual Cyber Risk" and "Level of Cyber Risk Treated" are influenced by changing the "Treatment Ratio" as below in the case that "Treatment Delay" is 1 year:

- Run 6: 0.2 (20%)
- Run 7: 0.4 (40%)
- Run 8: 0.6 (60%)
- Run 9: 0.8 (80%)
- Run 10:1.0 (100%)

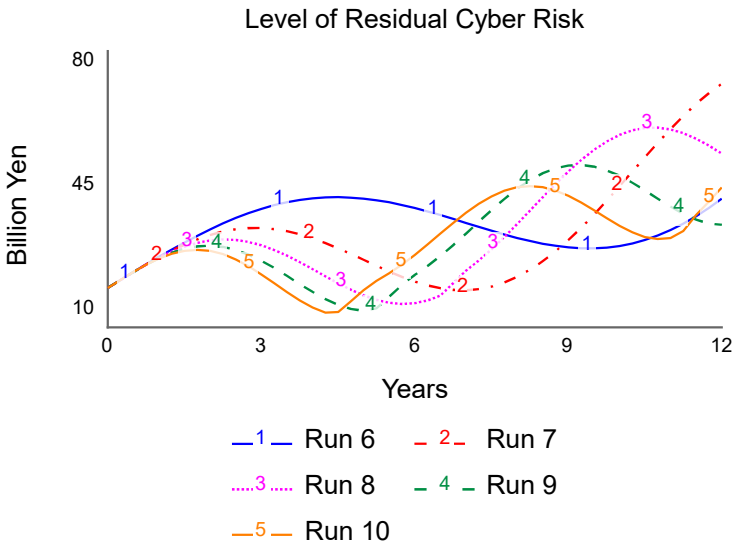

Figure 35. Patterns of Level of Residual Cyber Risk Influenced by Ratio of Implementation of Controls.

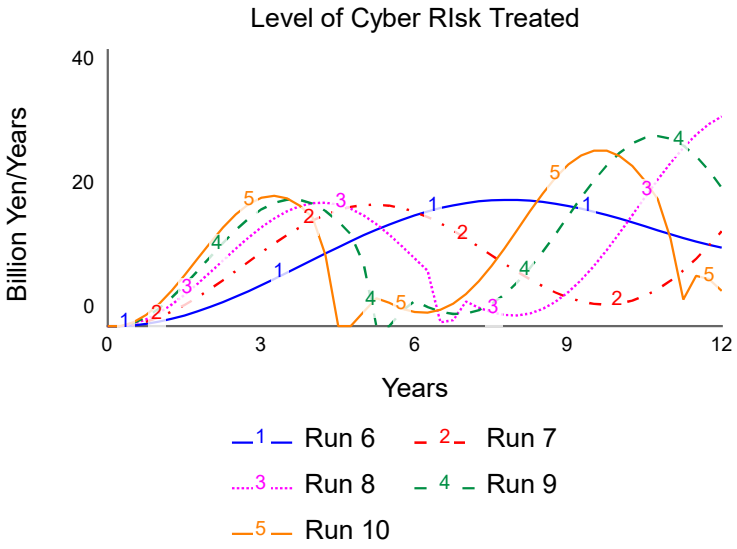

Figure 36. Patterns of Level of Cyber Risk Treated Influenced by Ratio of Implementation of Controls.

5.4.5.2 Impact of Treatment Delay and Ratio

The first simulation visualizes that "Level of Residual Cyber Risk" sometimes unexpectedly rises in the short-term because effects of the controls on the "Level of Residual Cyber Risk" are different in the short-term and the long-term if there is a delay in the implementation of the controls.

The second and third simulations suggest that lowering “Treatment Ratio” (ratio of the implementation of controls) smooth uneven effects of the controls on the “Level of Residual Cyber Risk” over time.

In the second simulation, in the Run 10 where “Treatment Ratio” is 100%, the transition of “Level of Residual Cyber Risk” draws several mountains. On the other hand, in the Run 6 where “Treatment Ratio” is 20%, the mountains that transition of “Level of Residual Cyber Risk” draws are more gentle. In summary, the lowest point of “Level of Residual Cyber Risk” in the Run 6 is higher than the lowest points of “Level of Residual Cyber Risk” in any other Runs while the highest point of “Level of Residual Cyber Risk” in the Run 6 is lower than the highest points of “Level of Residual Cyber Risk” in any other Runs.

5.5 Consideration

5.5.1 Overview

DCRM could analyze how oscillation behavior of cyber risk level occurred (cyber risk analysis) and get useful information to find how that behavior might be influenced (cyber risk treatment).

5.5.2 Cyber Risk Analysis

In cyber risk analysis, the structure was identified using systems thinking for cyber risk and controls at an organization level. The structure included a balancing feedback loop among the factors affecting the cyber risk with a delay and it showed the underlying cause of a fluctuation of cyber risk level. The delay of the implementation of controls contributed to the fluctuation of cyber risk level that was the cause of excessive treatment of cyber risk with excessive controls. DCRM could explore the effect of the delay of the implementation of controls in a balancing feedback loop that create emergent behavior of cyber risk level.

5.5.3 Cyber Risk Treatment

5.5.3.1 Overview

In cyber risk treatment, the structure for cyber risk and controls at an organization level was simulated using system dynamics to determine how oscillation behavior of cyber risk level might be influenced.

5.5.3.2 First Simulation

In the first simulation, without the delay, the implementation of controls produced a constant reduction of the cyber risk level by the action of balancing feedback loop. With the delay, the implementation of controls did not produce a constant reduction of the cyber risk level. The cyber risk level sometimes unexpectedly rose in the short-term because effects of controls on cyber risk level were different in the short-term

and the long-term. As a result, excessive controls were implemented after such a cyber risk level was compared with the cyber risk appetite, and productivities and usability of security controls were undermined.

For example, phishing simulation training is an effective control to prevent PCs from being attacked by phishing emails. However, phishing simulation training may not reduce the risk that employees' action to click the link in the phishing emails to the acceptable level for a while because of their learning curve. According to Spitzner's research [30], it takes 6-12 months to reduce the ratio of clicking from 30-60% to 5-19%. If the ratio of clicking indicates that its risk level in short-term exceeds the acceptable level, more strict phishing simulation training that sends the fake phishing emails looking as good as the legitimate emails to employees may be conducted. It may enforce employees to be too cautious about the incoming emails and ignore or mishandle the legitimate emails.

Using DCRM, the organizations can simulate how the risk level will behave in long term by indicating the delay of effect of the control – phishing simulation training. The simulation allows them to estimate that the risk level will rise temporally because of the delay of effect of the control and the risk level will decline later. They can recognize that conducting more strict phishing simulation training responding to the rise of risk level will not make the situation better but worse because risk level will move up and down sharply in long term.

ISO/IEC 27000:2016 mentions that sometimes it takes time to implement a chosen set of controls and during that time the risk level may be higher than can be tolerated on a long-term basis [31]. The result of the first simulation accorded with this statement. The larger delay of implementation of controls was, the larger the fluctuation of the cyber risk level was. The cyber risk level rose temporally compared to the case where the delay of implementation of controls was smaller. It indicated that even in an environment with the same cyber risk level at a certain time, if the time taken to implement the controls was different, it meant that the cyber risk level was different at any time thereafter. This led to the case that cyber risk level became higher than cyber risk appetite on a long-term basis temporarily. Based on the above grounds, the first simulation, in which the delay of the implementation of controls was changed to different values, and the behavior of the cyber risk level that changed over time was quantitatively evaluated, could be considered to be valid.

The large fluctuations in the cyber risk level that occurred when it took time to implement controls could be said to be due to the repetition of the cycle of the following elements:

1. As the "Cyber-Accessible Corporate Value" increased, the "Level of Residual Cyber Risk" increased. Then, by comparing the increased "Level of Residual Cyber Risk" with the "Cyber Risk Appetite", it was decided to implement controls to reduce the gap.
2. There was a time lag between the decision to implement controls and the actual reduction of the "Level of Residual Cyber Risk". Therefore, the "Level of Residual Cyber Risk" continued to increase.

3. As a result of comparing the temporarily increased “Level of Residual Cyber Risk” with the “Cyber Risk Appetite” and implementing excessive controls to reduce the gaps, this time, the “Level of Residual Cyber Risk” suddenly decreased with a delay.
4. The implementation of controls was suppressed by comparing to “Cyber Risk Appetite”.

5.5.3.3 Second and Third Simulation

In the second and third simulations, lowering the ratio of the implementation of controls smoothed uneven effects of the controls on the level of cyber risk over time. These results validated that the simulation provided useful information to determine how oscillation behavior of cyber risk level might be influenced. In this case, the simulations suggested the organizations might accept the cyber risk level exceeding cyber risk appetite for a certain period of time and avoid to implement additional controls.

For example, using DCRM, the organizations can simulate how the risk level will behave in long term if they do not conduct more strict phishing simulation training responding to the rise of risk level in short term by indicating lower ratio of the implementation of the controls. The simulation allows them to estimate that the risk level will not move up and down very much and be stable in long term and recognize that they do not need to conduct more strict phishing simulation training by accepting the ratio of clicking beyond their acceptable level at least for 6-12 months. In this way, the organizations can prevent unnecessary productivity loss caused by mishandling the legitimate emails.

ISO/IEC 27000:2016 mentions that risk criteria should cover tolerability of risks on a short-term basis while controls are being implemented [31]. The result of the second and third simulations accorded with this statement.

Decreasing the treatment ratio, which was the ratio at which controls reduced the cyber risk level, did not mean that controls were implemented until the risk level was simply reduced to the risk acceptance criteria. It meant that controls were implemented until the risk level exceeding the risk acceptance criteria was reduced to the level that was acceptable to some extent. Based on the above grounds, the second and third simulations, in which the treatment ratio was changed to different values, and the behavior of the cyber risk level that changes over time was evaluated quantitatively, could be considered to be appropriate.

If the treatment ratio was lowered, the cyber risk level was more gradually reduced compared to the case where the treatment ratio was high. However, from the point of view of the effect of reducing the cyber risk level over a long-time axis, the deviation that appeared at a specific time when the treatment ratio was high was softened and became more equal if the treatment ratio was lowered, so fluctuations in the cyber risk level could be softened.

5.5.4 Limitations

In order to highlight the impact of the time taken to implement the controls on the cyber risk level, sensitivity to the ever-changing business environment is relieved to some extent in the simulation.

The simulation assumes that the time taken to implement the controls collectively for cyber risk level is same to clarify the impact of the time taken to implement the controls. In real business environment, there are various type of controls to treat each cyber risk and the time taken to implement these controls may vary, If the time taken to implement the controls varies, its impact on the patterns of the cyber risk level may be smaller.

There are a wide range of factors that affect the business environment in addition to the corporate value and risk appetite and they are not taken into account in the simulation.

6 Power of Cyberspace Model (POCM)

6.1 Background

Although the conventional risk management approaches successfully analyze the risks where the factors affecting the risks and their effect on level of the risks have a linear relationship, it has a difficulty in analyzing the risks where a small factor can grow into large effect on level of the risks by cascading in the scenario of a cyber-attack. Without considering real causes of these patterns of change, there are some possibilities that efficient controls may not be implemented. To solve this issue, Power of Cyberspace Model (POCM) is created by application of systems thinking.

6.2 Concept

6.2.1 Power of Communication

It is important to consider how one entity influences other entities' behaviors through communication in order to understand how cyber-attack occurs. Such an influence is called a "Power of Communication" in this paper. There is an event that initiates communication by an originator called an "initiating event" and another event caused by the initiating event called a "consequential event", that occurs on opponents of the communication. System thinking can visualize dynamic relationships among these events occurring on entities and is suitable for modeling how one entity influences other entities' behaviors through communication.

This paper assumes that there are four types of basic influence reflecting the evolution of communication means toward cyberspace era from ancient times. Four types of influence include influence of person on person through conversation, influence of program on computer, influence of device on device over Internet, and influence of person on person through emails. Influence of person on person through emails is also customized as a case of phishing emails and influence of program on computer is also customized as a case of malicious program. This paper considers that these models are useful for the people who are dealing with threats for cyberspace to understand the primitive drivers of these threats.

Various communication means have been created in many circumstances. Human being created the languages that are communication means among people. Human being also created other communication means: programming languages between human being and software, machine languages between software and computer, and network protocols among devices connected to the network. All those communication means influence the behaviors of communication's opponent entities and this is "Power of Communication".

Communication using languages (initiating event) influences listener's behaviors (consequential event) as intended by a speaker as shown in Figure 37.

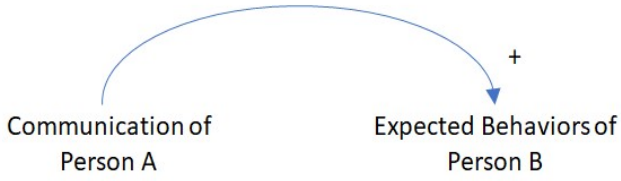

Figure 37. Influence of person on person through conversation.

Machine languages translated from computer programs developed using programming languages (initiating event) influence computer's behaviors (consequential event) as intended by a programmer as shown in Figure 38.

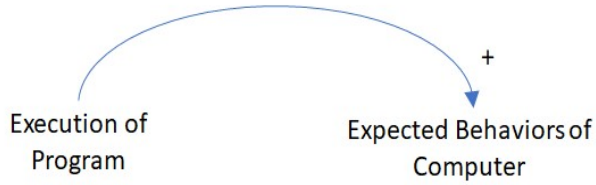

Figure 38. Influence of program on computer.

Communication initiated by TCP/IP protocols (initiating event) influence behaviors of any destination devices connected to Internet (consequential event) as intended by a source device as shown in Figure 39.

Figure 39. Influence of device on device over Internet.

Languages on Email and Twitter that are conveyed by the combination of TCP/IP and other protocols (initiating event) influence a lot of recipients' behaviors (consequential event) as intended by a sender as shown in Figure 40.

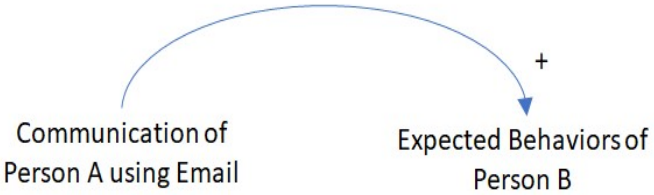

Figure 40. Influence of person on person through emails

Because expectations of the communication originator vary, the outcomes of behaviors of the communication opponents influenced by the originator are not necessarily benefits for specific entities.

For example, phishing email (initiating event) influences a mail recipients' behaviors that give harm to them (consequential event) as intended by a sender as shown in Figure 41.

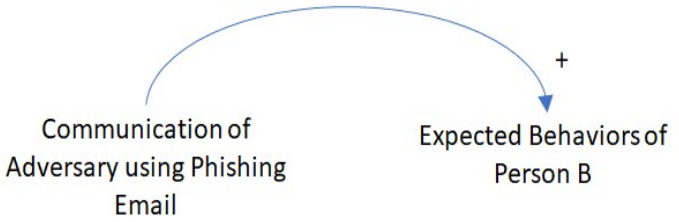

Figure 41. Influence of person on person through phishing emails

Malicious program (initiating event) triggers computer's mal-behaviors that give harm to the computer (consequential event) as intended by the program as shown in Figure 42.

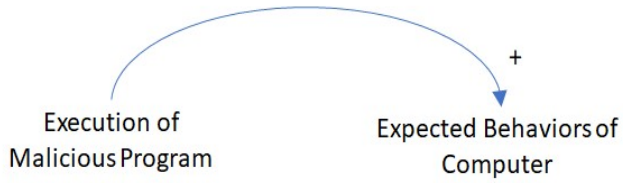

Figure 42. Influence of malicious program on computer

6.2.2 Power of Cyberspace

Cyberspace is regarded as a framework that facilitates various communication means by removing the barrier of time and physical space and builds a virtual world. In ancient times, human being could communicate with other parties only when they are face-to-face. This means there was a barrier of physical space. Telephone removed this barrier for communication among people although only voice can be used as a communication medium. Cyberspace allows the use of various communication medium such as voice, video, and writing among people in real time and the use of various communication medium among any devices connected to Internet. The comparison among these communication means is shown in Table 4.

Table 4. Comparison among Communication Means

Communication	Entities	Medium	Restrictions
Conversation	Human	Voices	Space
Telephone	Human	Voices	
Email	Human	Writing	Time
Internet	Devices	Network Protocol	
Cyberspace	Human, Devices	Voices, Videos, Writing, Network Protocol	

"Power of Communication" tends to be a cause of events on cyberspace. The consequences of these events include positive ones like productivities improvement and negative ones like cybersecurity incidents. Such influence of the entity on other entities in cyberspace is called "Power of Cyberspace" in this paper. "Power of Cyberspace" is built on "Power of Communication" in the context of Cyberspace and produces great benefits as well as great drawbacks depending on how they are used. Although Kramer et al. [6] define the similar concept called "cyberpower", it clearly distinguishes between content and connectivity and regards content as an individual static object. "Power of Cyberspace" is built on "Power of Communication" where content and connectivity are regarded as properties of communication and not distinguished as individual objects.

A model is developed to explain the scenario on how extreme cybersecurity incidents occur from a specific threat: cyber-attack as an example of the initiating event that may have extreme negative effect on cyberspace with the help of "Power of Cyberspace". The model offers a clue as to how their impact can be reduced. The model is called "Power of Cyberspace Model (POCM)". The model is useful for the people who are dealing with specific threats for cyberspace to find out general ideas on how they should be treated. There are also other scenarios for different threats and the models for these scenarios may be developed by the people who are dealing with these threats for cyberspace by adapting the concept of "Power of Cyberspace".

6.2.3 POCM

POCM uses graphs of patterns of cyber-attacks to understand how interrelationships among events in cyberspace generate exponential growth of cyber risks (dimension of propagation) in addition to the dimension of attack vector.

For example, it helps the organizations to see how a small event such as an execution of malicious program on a single computer connected to cyberspace generates an extreme effect across cyberspace through the interrelationships (structure) and to gain insight into the leverage. It is assumed that the interrelationships exist among events that influence each other in coupling between entities in cyberspace to generate an extreme event on cyberspace.

Using POCM, organizations can analyze how exponential growth behavior of cyber risk level occurs (cyber risk analysis) and get useful information to find how that behavior might be influenced (cyber risk treatment).

This view of POCM is shown in Figure 43.

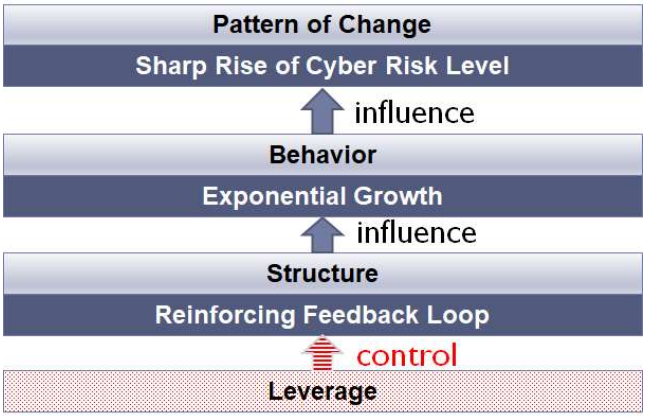

Figure 43. View of POCM about Cyber Risk.

Exponential growth behavior of cyber risk level is created by the structure that includes reinforcing feedback loop among events in cyberspace and results in a sharp rise in cyber risk level. Treatment of a sharp rise in cyber risk level requires addressing the structure underlying exponential growth behavior of cyber risk level.

6.3 Cyber Risk Analysis

6.3.1 Overview

POCM Feedback Loop Diagram is developed by application of systems thinking for cyber risk analysis to identify the real causes of an extreme effect of cyber-attack on cyber risk level.

Development of POCM Feedback Loop Diagram requires the identification of the factors and their relationships in the context of analysis of exponential growth behavior of cyber risk level.

6.3.2 Development of POCM Feedback Loop Diagram

6.3.2.1 Identification of Factors Related to Cyber-Attacks and Their Relationships

There are two main elements of cyber-attacks:

- Attack Vector
- Attack Propagation

The attack vector is the method by which an attack reaches its target [8]. Attack propagation encodes the propagation of the effect of the attack through the events and is the real cause to create exponential growth behavior of cyber risk level. Given the likelihood that an attack reaches its target analyzed in the structure for attack vector,

and the effect of its propagation between events analyzed in the structure for attack propagation, its extreme effect across cyberspace is estimated.

6.3.2.2 Identification of Factors Related to Attack Propagation and Their Relationships

The following factors are identified to analyze attack propagation:

- Execution of Malicious Program
- Expected Behaviors of Computer
- Number of Infected Computers
- Bad Consequence

A small event such as an "Execution of Malicious Program" on a single computer connected to cyberspace (first round of an initiating event) can generate "Bad Consequence" that has an extreme effect across cyberspace by reinforcing feedback loop.

Reinforcing feedback loop shows non-linear outcomes of increasing "Number of Infected Computers" (consequential event) because the "Execution of Malicious Program" on the computer (initiating event) triggers "Expected Behaviors of Computer" that infect more computers connected to cyberspace through propagation.

These factors and their relationships are drawn in POCM Feedback Loop Diagram for Attack Propagation as shown in Figure 44.

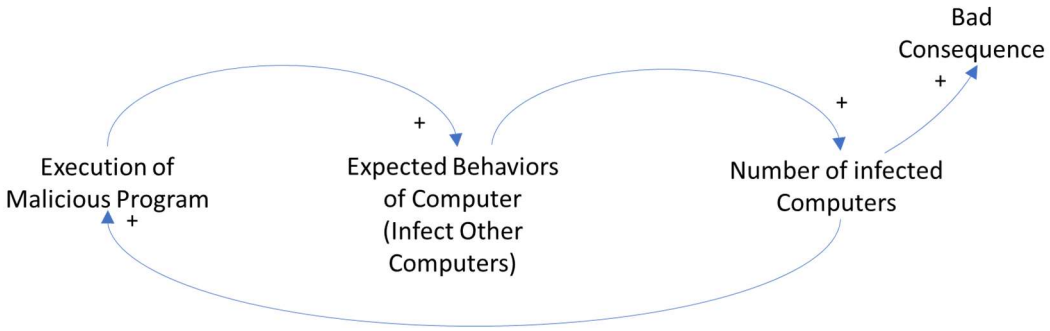

Figure 44. POCM Feedback Loop Diagram for Attack Propagation.

Although the diagram intuitively visualizes how reinforcing feedback loop creates an extreme effect, it does not clarify how to quantify the extreme effect. The diagram is refined to quantify the extreme effect generated by initiating events by application of the concept of the threat network model developed by Branagan et al. [20] described in Subsection 2.3.2.5.

The following factors are identified to refine the diagram:

- Number of Infected Entities
- Number of Reproduced Malware Infection per Specific Period
- Reproduction Number per Specific Period

- Number of Packet Received per Specific Period
- Likelihood that an Entity is Infected with Malware per Packet Received

The threat network model developed by Branagan et al. [20] is based on two key concepts: a threat event and threat propagation. POCM Feedback Loop Diagram for Attack Propagation is based only on a chain of events. The concept of propagation defined by Branagan et al. [20] is added to the diagram to define how propagation increases the number of infected entities in cyberspace.

"Number of Infected Entities" (initiating event) indicates number of entities infected in cyberspace. "Number of Reproduced Malware Infection per Specific Period" (consequential event) indicates number of malware infection reproduced by the "Number of Infected Entities". It is calculated as the product of "Number of Infected Entities" and "Reproduction Number per Specific Period". There is a feedback loop between the initiating event and the consequential event. This means that "Number of Reproduced Malware Infection per Specific Period" triggered by "Number of Infected Entities" is added back to "Number of Infected Entities".

"Reproduction Number per Specific Period" indicates expected number of infection directly reproduced by one infected entity per specific period. It is calculated as the product of "Number of Packets Received per Specific Period" and "Likelihood that the Entity is Infected with Malware per Packet Received". "Number of Packets Received per Specific Period" indicates number of packets received by each entity per specific period. "Likelihood that the Entity is Infected with Malware per Packet Received" indicates the likelihood that each entity is infected with Malware per packet received.

These factors and their relationships are redrawn in POCM Feedback Loop Diagram for Attack Propagation as shown in Figure 45.

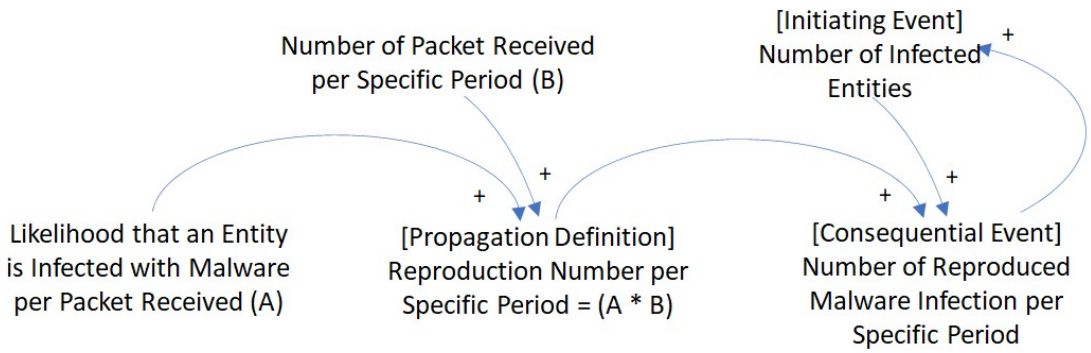

Figure 45. Refined POCM Feedback Loop Diagram for Attack Propagation.

The threat network model developed by Branagan et al. [20] explores propagation of infection in linear cause effect chains. Leveson [32] argues that event-based models that explain accidents in terms of multiple events sequenced as a chain over time encourage limited notions of causality such as linear causality relationships and it is difficult to incorporate non-linear relationships, including feedback. The refined

POCM Feedback Loop Diagram for Attack Propagation explores propagation of infection in the feedback loops that create emergent behavior of cyber risk level.

6.3.2.3 Completion of Development of POCM Feedback Loop Diagram for Attack Propagation

The complete POCM Feedback Loop Diagram is developed as shown in Figure 45. It incorporates all factors and their relationships in the context of analysis of exponential growth behavior of cyber risk level.

6.3.2.4 Example of POCM Feedback Loop Diagram for Attack Vector

Attack vector is the cause of the first round of initiating event in the attack propagation. There are various types of attack vectors and researches on them are well established, particularly by Hansman et al.[8]. The development of PCOM Feedback Structure for each attack vector is out of the scope of this paper because the objective of this paper is to complement the established fields of risk management.

One example of the attack vectors is communication conducted by an adversary using an email. The POCM Feedback Loop Diagram for this attack vector is shown in Figure 46. This attack vector influences likelihood that the first round of initiating event occurs in attack propagation.

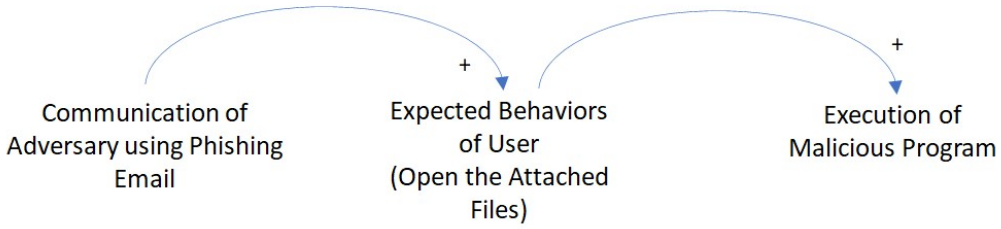

Figure 46. Example of POCM Feedback Loop Diagram for Attack Vector.

6.4 Cyber Risk Treatment

6.4.1 Overview

POCM Stock and Flow Diagram for Attack Propagation is developed by application of system dynamics for cyber risk treatment to get useful information to determine where to work to address the causes of an extreme effect of cyber-attack on cyber risk level. POCM Stock and Flow Diagram for Attack Propagation is simulated to determine how exponential growth behavior of cyber risk level might be influenced. The example of POCM Feedback Loop Diagram for Attack Vector provides useful information to reduce likelihood that the first round of initiating event occur in attack propagation.

Development of POCM Stock and Flow Diagram for Attack Propagation requires the conversion of POCM Feedback Loop Diagram for Attack Propagation.

6.4.2 Conversion of POCM Feedback Loop Diagram for Attack Propagation into POCM Stock and Flow Diagram for Attack Propagation

6.4.2.1 Overview

During the conversion of the POCM Feedback Loop Diagram for Attack Propagation into the POCM Stock and Flow Diagram for Attack Propagation by application of system dynamics, the factors shown in POCM Feedback Loop Diagram for Attack Propagation are assigned to the stocks, flows and converters used in system dynamics while their relationships are kept.

6.4.2.2 Stocks

The following factor is quantities of entities that have incoming and/or outgoing flows. Therefore, it is assigned to a stock:

- Number of Infected Entities

6.4.2.3 Flows

The following new factors are identified as incoming or outgoing flows for the stock "Number of Infected Entities":

- Number of New Infected Entities
- Number of Removed Infected Entities

6.4.2.4 Converters

The following factors are not stocks nor flows but constants or calculations based on other factors. Therefore, they are assigned to converters:

- Number of Reproduced Malware Infection
- Reproduction Number
- Likelihood that an Entity is Infected with Malware per Packet
- Number of Packets Received

The following new factors are assigned to converters to determine where to work to address the causes of an extreme effect of cyber-attack on cyber risk level:

- Removal Ratio
- Removal Delay

"Removal Ratio" indicates the ratio at which infected entities are removed. "Removal Delay" indicates the time taken to remove infected entities in hour.

6.4.2.5 Completion of Conversion into POCM Stock and Flow Diagram for Attack Propagation

The complete POCM Stock and Flow Diagram for Attack Propagation is developed by conversion of POCM Feedback Loop Diagram for Attack Propagation as shown in Figure 47. It incorporates all factors converted and their relationships in the context of treatment of exponential growth behavior of cyber risk level.

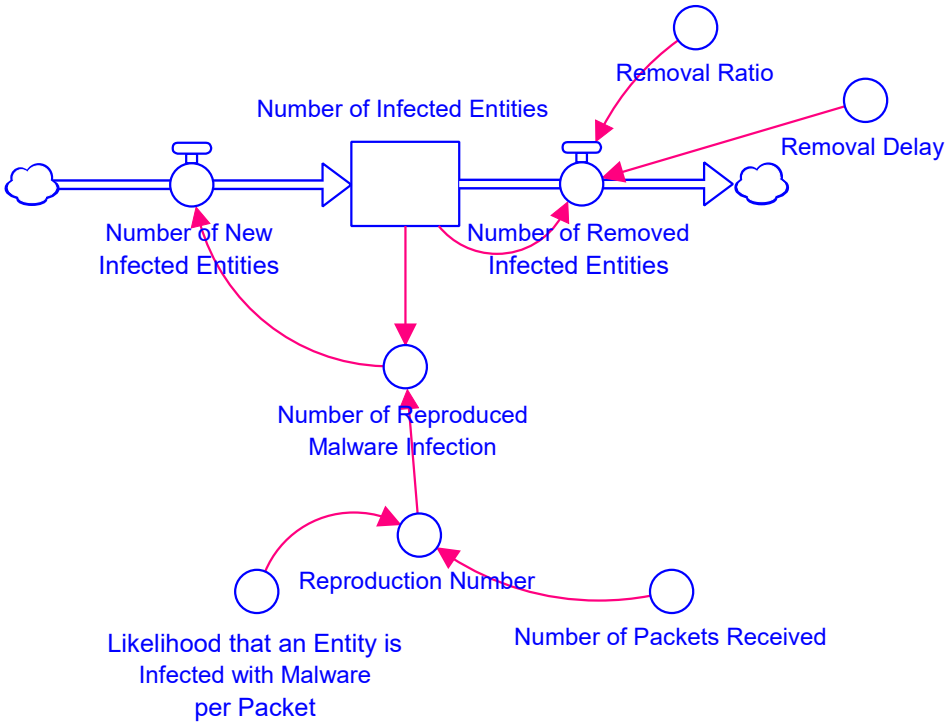

Figure 47. POCM Stock and Flow Diagram for Attack Propagation.

6.4.3 First Simulation

In order to justify that attack propagation simulated by POCM reasonably accords with reality, the simulation on the outbreak of Mirai in 2016 is conducted by referring to the analysis of Antonakakis et al. [33]. The simulation explores how Mirai infects entities in cyberspace (IoT devices in in this case) in its first 20 hours and provides useful information that can be used to determine how the infections might be controlled.

The simulation is conducted in a way that the "Number of Infected Entities (IoT devices)" reaches 64,500 within 20 hours according to the analysis of Antonakakis et al. [33]. "Number of Packets Received" by each device per hour is set to 55 according to the analysis of NICTER report about packets monitored in 2016. [34].

The Figure 48 shows the result of the simulation.

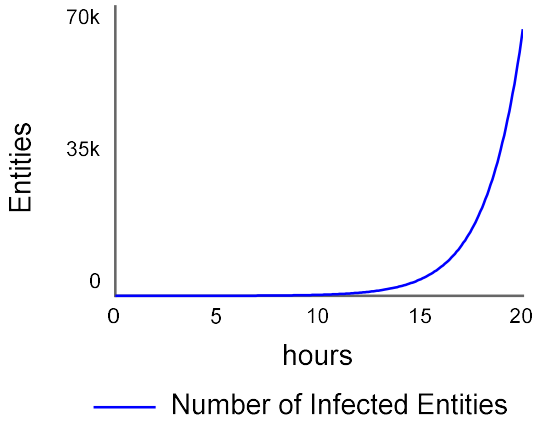

Figure 48. Pattern of Number of IoT Devices Infected by Mirai in Simulation of POCM.

The “Likelihood that an Entity (IoT device) is Infected with Malware (Mirai) per Packet” is worked out to 1. 0114 % from the simulation. “Reproduction Number” per hour is the product of the “Likelihood that an Entity (IoT device) is Infected with Malware (Mirai) per Packet” and the “Number of Packets Received” by each IoT device per hour. The result of the calculation is 0.556.

The Figure 49 shows the pattern of number of IoT devices infected by Mirai in analysis of Antonakakis et al.[33].

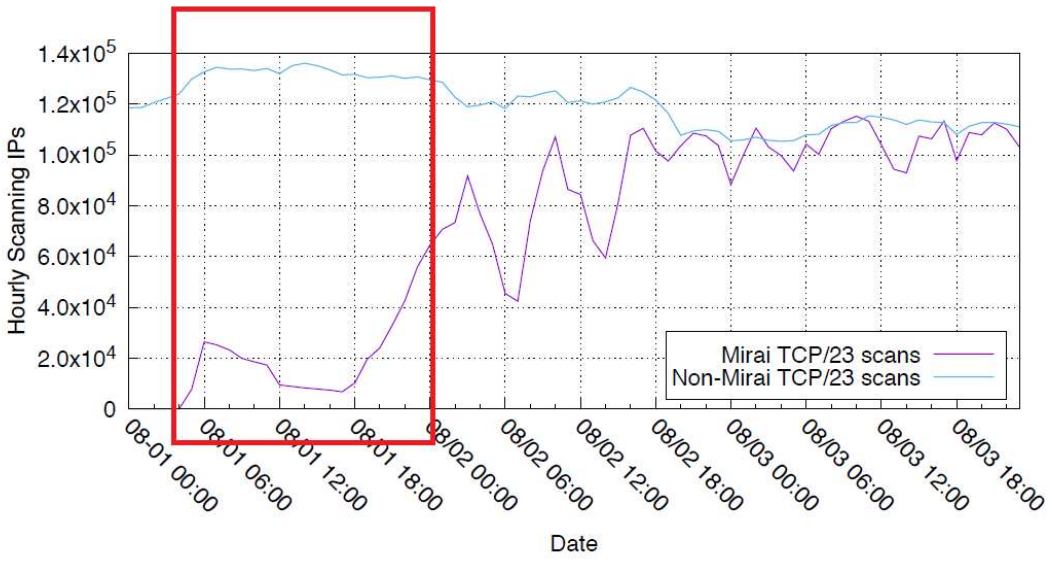

Figure 49. Pattern of Number of IoT Devices Infected by Mirai in Analysis of Antonakakis et al. [29].

The line of Mirai TCP/23 scans indicates number of the IoT devices infected by Mirai over time and the square shows the time axis in the same range as the Figure 48. It is recognized that propagation effects are shown in continuous steep slope leading to the target value.

In the simulation of POCM shown in Figure 48, the continuous steep slope leading to the target value (64,500) starts around 11 hours. The "Number of Infected Entities (IoT devices)" is in the range of around +-1000 of 5000 at 11 hours. In the analysis of Antonakakis et al. [29] shown in Figure 49, the continuous steep slope leading to the target value (64,500) also starts around 11 hours. The number of infected device is also in the range of around +-1000 of 5000 at 11 hours. This indicates that angle of the continuous steep slope leading to the target value from 11 hours to 20 hours in the simulation of POCM and the analysis of Antonakakis et al. [33] is very similar and the POCM simulates the attack propagation that reasonably accords with reality.

6.4.4 Second and Third Simulations

6.4.4.1 Overview

There is a way to influence the behavior of attack propagation in the simulation. It is assumed that removing the devices infected by Mirai from cyberspace will influence the behavior. It is simulated by changing the "Removal Ratio" as below:

- Run 1: 0.00 (0%)
- Run 2: 0.01 (1%)
- Run 3: 0.02 (2%)
- Run 4: 0.05 (5%)
- Run 5: 0.10 (10%)

In Figure 50, the simulation shows how the behavior of attack propagation expressed by the pattern of "Number of Infected Entities (IoT devices)" is influenced by changing the "Removal Ratio" as below:

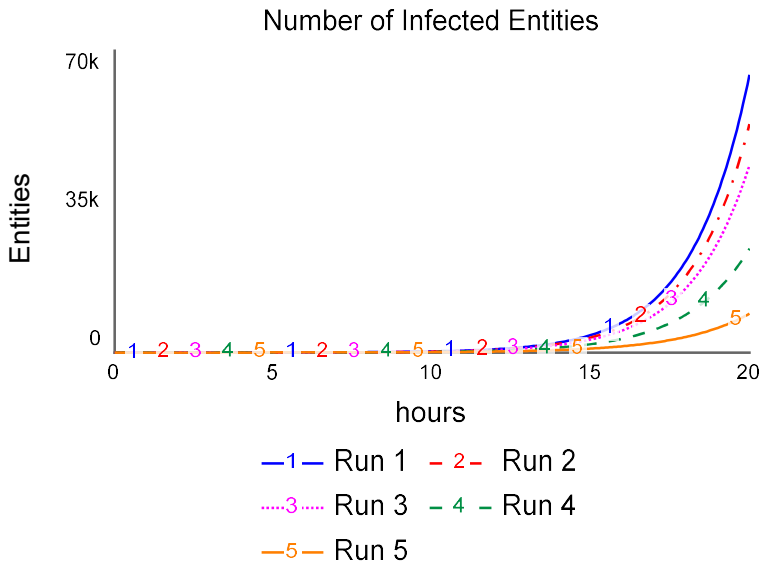

Figure 50. Pattern of Number of IoT Devices Infected by Mirai Influenced by Removal Ratio.

There may be a delay in removal of the devices infected by Mirai from cyberspace. It is simulated by changing the "Removal Delay" in the case that "Removal Ratio" is 10% as below:

- Run 6: 0.0 (0 hour)
- Run 7: 0.5 (0.5 hour)
- Run 8: 1.0 (1 hour)
- Run 9: 2.0 (2 hours)
- Run 10:5.0 (5 hours)

In Figure 51, the simulation show how the behavior of attack propagation expressed by the pattern of "Number of Infected Entities (IoT devices)" is influenced by changing the "Removal Delay" as below:

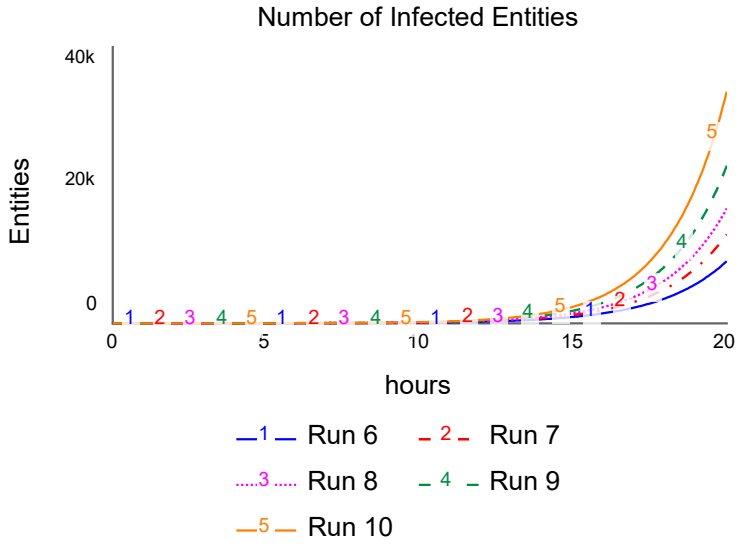

Figure 51. Pattern of Number of IoT Devices Infected by Mirai Influenced by Removal Delay.

6.4.4.2 Impact of Removal Ratio and Delay

The first simulation visualizes non-linear behaviors of attack propagation expressed by the pattern of "Number of Infected Entities (IoT devices)" that is the element of cyber risk level.

The second simulation suggests that even if 10% of infected devices are removed, it has a significant positive effect on mitigation of attack propagation. "Number of Infected Entities (IoT devices)" at 20 hours is reduced from 64,500 to 9,000 (86% reduction).

However, the third simulation suggests that the delay to remove the infected devices offsets a lot of the positive effect on mitigation of attack propagation. For example, if it takes 5 hours to remove the 10% of infected devices, "Number of Infected Entities (IoT devices)" at 20 hours is increased nearly by 4 times from 9,000 to 33,600 .

6.4.5 Treatment in the Example of POCM Feedback Loop Diagram for Attack Vector

Visualization of interrelationships in the example of POCM Feedback Loop Diagram for Attack Vector described in subsection 6.3.2.4 provides useful information to reduce likelihood that the first round of initiating event occur in attack propagation. The following controls are imagined to reduce likelihood that the first round of initiating event occur in attack propagation.

An increase of users' awareness about suspicious emails by communication reduces their mishandling of suspicious emails as shown in Figure 52. As a result, it reduces the likelihood that the first round of initiating event occurs in attack propagation.

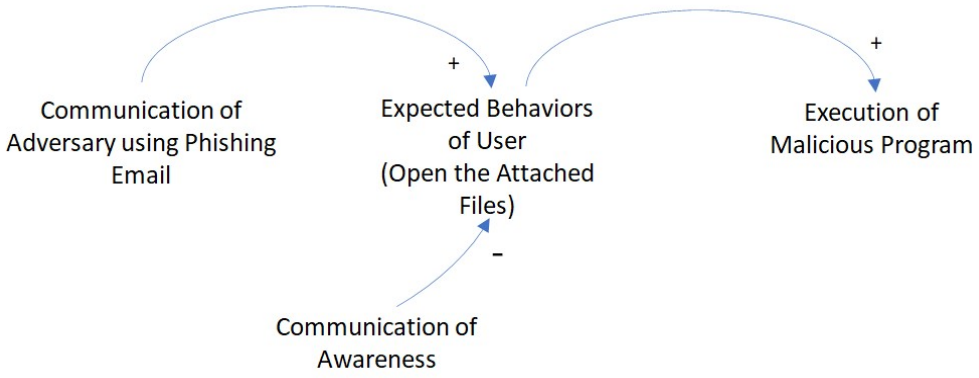

Figure 52. Control in the POCM Feedback Loop Diagram for Attack Vector 1.

Mail filtering program reduces number of phishing emails that users receive as shown in Figure 53. As a result, it reduces the likelihood that the first round of initiating event occurs in attack propagation.

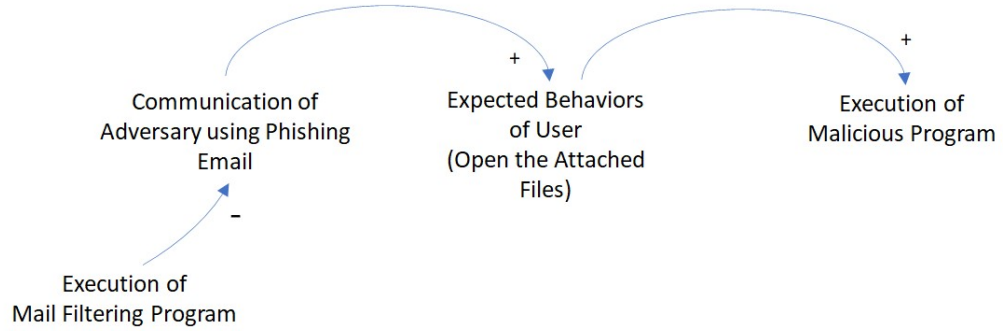

Figure 53. Control in the POCM Feedback Loop Diagram for Attack Vector 2.

Anti-virus program identifies and treats malicious programs as shown in Figure 54. As a result, it reduces the likelihood that the first round of initiating event occurs in attack propagation.

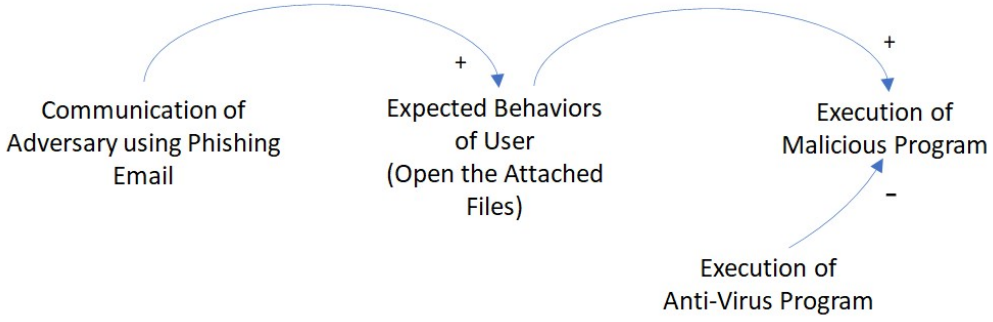

Figure 54. Control in the POCM Feedback Loop Diagram for Attack Vector 3.

6.5 Consideration

6.5.1 Overview

POCM could analyze how exponential growth behavior of cyber risk level occurred (cyber risk analysis) and get useful information to find how that behavior might be influenced (cyber risk treatment).

6.5.2 Cyber Risk Analysis

In cyber risk analysis, two structures were identified using systems thinking for main elements of cyber-attacks that create exponential growth behavior of cyber risk level: attack vector and attack propagation. The structure for attack propagation included reinforcing feedback loop among events in cyberspace that showed the underlying cause of a sharp rise in cyber risk level. The reinforcing feedback loop amplified the effect of cyber-attack on cyberspace and was a driving force of attack propagation. The structure for attack vector visualized the cause of the first round of initiating event in the attack propagation.

Traditionally, attack propagation was explored in linear cause effect chains such as the threat network model developed by Branagan et al. [20]. It was argued that linear cause effect chains encouraged limited notions of causality by such as Leveson [32]. POCM could explored attack propagation in the feedback loops that create emergent behavior of cyber risk level.

6.5.3 Cyber Risk Treatment

In cyber risk treatment, the structure for attack propagation was simulated using system dynamics to determine how exponential growth behavior of cyber risk level might be influenced.

The simulation on the outbreak of Mirai in 2016 reasonably accorded with reality that described in the analysis of Antonakakis et al. [33]. It was validated that the simulation visualized exponential growth behavior of cyber risk level caused by non-linear outcomes of increasing number of infected devices through attack propagation. Then simulation was conducted to forecast change of the number of infected devices by changing ratio at which infected devices were removed. It was found that even if 10% of infected devices were removed, it had a significant positive effect on mitigation of attack propagation (86% reduction of infected devices). Furthermore, another simulation was conducted to forecast change of the number of infected devices by changing the time taken to remove infected devices. It was found that the delay to remove the infected devices offset a lot of the positive effect on mitigation of attack propagation. These results validated that the simulation provided useful information to determine how exponential growth behavior of cyber risk level might be influenced. In this case, the simulation suggested that removal of certain numbers of infected devices from cyberspace without a long delay would have a significant positive effect on mitigation of exponential growth behavior of cyber risk level.

Visualization of interrelationships in the example of the structure underlying attack vector provided useful information to reduce likelihood that the first round of initiating event occurred in attack propagation.

6.5.4 Limitations

In order to highlight the impact of attack propagation on the cyber risk level, sensitivity to the ever-changing cyberspace environment is relieved to some extent in the simulation.

Only the key factors constituting feedback loops that generate attack propagation are identified and taken into account in the simulation. The simulation assumes that cyberspace is the network environment where devices have instant accesses each other. There are more factors that affect attack propagation in real cyberspace environment. In the network environment where these devices do not have instant accesses each other, it slows down attack propagation.

7 Conclusion

7.1 Results

7.1.1 Overview

The models developed in this paper could analyze and treat non-linear behaviors of cyber risk level to fill the gap between the nature of risks in cyberspace and view of conventional risk management approaches about it.

DCRM could analyze and treat oscillation behaviors of cyber risk level. POCM could analyze and treat exponential growth behaviors of cyber risk level. These models filled the gap between the nature of risks in cyberspace and view of conventional risk management approaches about it by addressing the limitations of conventional risk management approaches.

7.1.2 DCRM

DCRM provided useful information on how pattern of the oscillation behaviors of cyber risk level occurred through cyber risk analysis. The cyber risk analysis met the requirements described in subsection 4.1.2 as below:

- The structure underlying oscillation behavior of cyber risk level was identified for cyber risk and controls at an organization level.
- Dynamic interrelationships among the factors affecting the cyber risk were identified in the structure.

The cyber risk analysis addressed the limitations of conventional risk management approaches by exploring:

- How the cyber risks and controls were balanced through feedback loops.
- How the feedback loops among the factors affecting the cyber risk created emergent oscillation behavior of cyber risk level that could not be observed in its constituent parts.
- How the dynamic interrelationships among the factors affecting the cyber risk occurred through graphical causal presentation.

DCRM provided useful information that could be used to determine how pattern of the oscillation behaviors of cyber risk level might be influenced through cyber risk treatment. The cyber risk treatment met the requirements described in subsection 4.1.3 as below:

- The simulation explored how the feedback loop among the factors affecting the cyber risk influenced oscillation behavior of cyber risk level over time.
- The simulation predicted oscillation behavior of cyber risk level and provided an opportunity to experiment with risk treatment decisions that control the behaviors.

The cyber risk treatment addressed the limitations of conventional risk management approaches by exploring oscillation behavior of cyber risk level through the dynamic simulations.

For the setting of environment in which the organization managed cyber risk in the simulation, the values that faithfully represented reality were carefully chosen. The behavior of the cyber risk level and controls suggested by the simulation in this environment accorded with the statement in ISO/IEC 27000:2016. Based on the above grounds, DCRM was considered to be justified.

7.1.3 POCM

POCM provided useful information on how pattern of the exponential growth behaviors of cyber risk level occurred through cyber risk analysis. The cyber risk analysis met the requirements described in subsection 4.1.2 as below:

- The structures underlying exponential growth behavior of cyber risk level were identified for attack propagation.
- Dynamic interrelationships among initiating events and consequential events that amplified the effect of cyber-attack on cyberspace were identified in the structure.

The cyber risk analysis addressed the limitations of conventional risk management approaches by exploring:

- How the initiating events and consequential events in cyberspace could reinforce each other through feedback loops.
- How the feedback loops for attack propagation created emergent exponential growth behavior of cyber risk level that could not be observed in its constituent parts.
- How the dynamic interrelationships among initiating events and consequential events that amplified the effect of cyber-attack on cyberspace occurred through graphical causal presentation.

POCM provided useful information that could be used to determine how pattern of the exponential growth behaviors of cyber risk level might be influenced through cyber risk treatment. The cyber risk treatment met the requirements described in subsection 4.1.3 as below:

- The simulation explored how the feedback loop between initiating events and consequential events in cyberspace influenced exponential growth behavior of cyber risk level over time.
- The simulation predicted exponential growth behavior of cyber risk level and provided an opportunity to experiment with risk treatment decisions that control the behaviors.

The cyber risk treatment addressed the limitations of conventional risk management approaches by exploring exponential growth behavior of cyber risk level through the dynamic simulations.

For the setting of environment in which actual cyber-attack occurred in the simulation, the values monitored in the actual cyberspace were carefully chosen. The simulation drawn the non-linear outcomes of increasing number of infected devices through attack propagation that caused the exponential growth behavior of cyber risk and they reasonably accorded with reality monitored. Based on the above grounds, POCM was considered to be justified.

7.2 Future Research

The models developed in this paper considered the simple simulated environment that highlighted non-linear behavior of the cyber risk level without excessive reaction to excess factors. Future research will consider more factors affecting the cyber risk level.

For example, the additional factors related to business environment and cyberspace environment will be identified and then incorporated into these models for simulation. In this way, the organization will be able to simulate behavior of cyber risk level in wider range of scenarios and then find more detailed treatment. By simulating how behavior of cyber risk level will change depending on allocation of specific controls, it will be possible to predict most effective combination of controls for the specific risk scenarios.

8 Reference List

[1] ISO 31000:2018 Risk Management – Guidelines.

[2] Lammers, J. Crusius, J. and Gast, A. 2020. Correcting misperceptions of exponential coronavirus growth increases support for social distancing. Proceedings of the National Academy of Sciences of the United States of America. vol. 117, 28, pp. 16264-16266.

[3] Sterman, J. 2000. Business Dynamics: Systems Thinking and Modeling for a Complex World. Irwin McGraw-Hill.

[4] ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management.

[5] Clark, D. 2010. Characterizing Cyberspace: Past, Present and Future. MIT CSAIL.

[6] Kramer, F. Starr, S. and Wentz, L. 2009. Cyberpower and National Security. National Defense University Press.

[7] Appazov, A. 2014. Legal Aspects of Cybersecurity. University of Copenhagen.

[8] Hansman, S. and Hunt, R. 2005. A taxonomy of network and computer attacks. Elsevier. Computer and Security, vol. 24, 1, pp. 31–43

[9] Meyers, C. Powers, S. and Faissol, D. 2009. Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches. Lawrence Livermore National Lab.

[10] Richberg, J. 2018. A Common Cyber Threat Framework. National Intelligence Manager for Cyber National Security Partnerships.

[11] Hutchins, E. Cloppert, M. and Rohan, A. 2018. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Lockheed Martin Corporation.

[12] Buzan, B. Waver, O. and Wilde, J. 1998. Security A New Framework for Analysis. Lynne Rienner Publishers.

[13] Anderson, R. and Hearn, A. 1996. An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: ‘‘The Day After … in Cyberspace II’’. RAND.

[14] Hansen, L. and Nissenbaum, H. 2009. Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly. 53, pp. 1155-1175

[15] National Institute of Standards and Technology. 2014. Framework for Improving Critical Infrastructure Cybersecurity Version 1.0.

[16] Heylighen, F. 2008. Complexity and self-organization, in Encyclopedia of Library and Information Sciences. Taylor & Francis.

[17] McKelveya, B. and Andriani, P. 2010. Avoiding extreme risk before it occurs: A complexity science approach to incubation. Macmillan Publishers. Risk Management, vol. 12, 1, pp. 54–82

[18] Trček, D. 2008. Using System Dynamics for Managing Risks in Information Systems. WSEAS Trans. Information Science & Applications. vol.5, 2, pp. 175–180

[19]Groš, S. 2011. Complex systems and risk management. MIPRO.

[20]Branagan, M., Dawson, R. and Longley, D. 2006. SECURITY RISK ANALYSIS FOR COMPLEX SYSTEMS. ISSA.

[21]Saunders, J.H. 2002. A Dynamic Risk Model for Information Technology Security in a Critical Infrastructure Environment.10th United Engineering Foundation Conference.

[22]Meadows, D. 2008. Thinking in Systems. Chelsea Green Publishing.

[23]McNamara, C. 2006. Field Guide to Consulting and Organizational Development. Paperback.

[24]Senge, P. 1990. The Fifth Discipline. Crown Business.

[25]Forrester, J. 1961. Industrial Dynamics. MIT Press.

[26]Ohki, E. Tamura, J. Shimizu, K. Sugiura, M. Kikuchi, M. Nasu, H. Tsunekawa, N. and Fuji, K. 2018. A proposal of cyber security risk modeling based on corporate values for business executives. Japan Society of Security Management. vol. 32, 1, pp. 16-32

[27]Wikipedia. Unicorn Companies. Accessed https://ja.wikipedia.org/wiki/ユニコーン企業_(ファイナンス) on 2020-06-13.

[28]Japan Users Association of Information System (JUAS). 2017. 23rd Corporate IT Trend Survey 2017.

[29]Information-Technology Promotion Agency Japan（IPA）. 2015. Information Security Event Damage Situation Survey Report 2014.

[30]Spitzner, L. 2014. Measuring Change in Human Behavior. RSA Conference 2014.

[31]ISO/IEC 27000:2016 Information technology – Security techniques – Information security management systems – Overview and vocabulary

[32]Leveson, N. 2004. A New Accident Model for Engineering Safer Systems. Safery Science, vol. 42, 4, pp. 237–270

[33]Antonakakis, M. April, T. Bailey, M. Bernhard, M. Bursztein, E. Cochran, J. Durumeric, Z. Halderman, A. Invernizzi, L. Kallitsis, M. Kumar, D. Lever, C. Ma, Z. Mason, J. Menscher, D. Seaman, C. Sullivan, N. Thomas, K. and Zhou, Y. 2017. Understanding the Mirai Botnet. Proceedings of the 26th USENIX Security Symposium. pp. 1093-1110

[34]National Institute of Information and Communications Technology (NICT). 2020. NICTER Observation Report 2019.