2020年9月3日
博士請求論文発表会

Leveraging Systems Thinking to Complement Cyber Risk Management

Second Year, Doctoral Program　Masato KIKUCHI
博士後期課程　菊地 正人

Index

1 Introduction

1.1 Issues

1.2 View of Conventional Risk Management Approaches

1.3 Nature of Risks in Cyberspace

2 Previous Research

3 Limitations of Conventional Risk Management Approach

4 New Models for Cyber Risk Management

Index

5. Dynamic Cyber Risk Model (DCRM)

5.1 Overview

5.2 Cyber Risk Analysis

5.3 Cyber Risk Treatment

5.4 Consideration

6. Power of Cyberspace Model (POCM)

6.1 Overview

6.2 Cyber Risk Analysis

6.3 Cyber Risk Treatment

6.4 Consideration

7. Conclusion

8. Reference List

1 Introduction

1.1 Issues

Issues

There is a gap between the

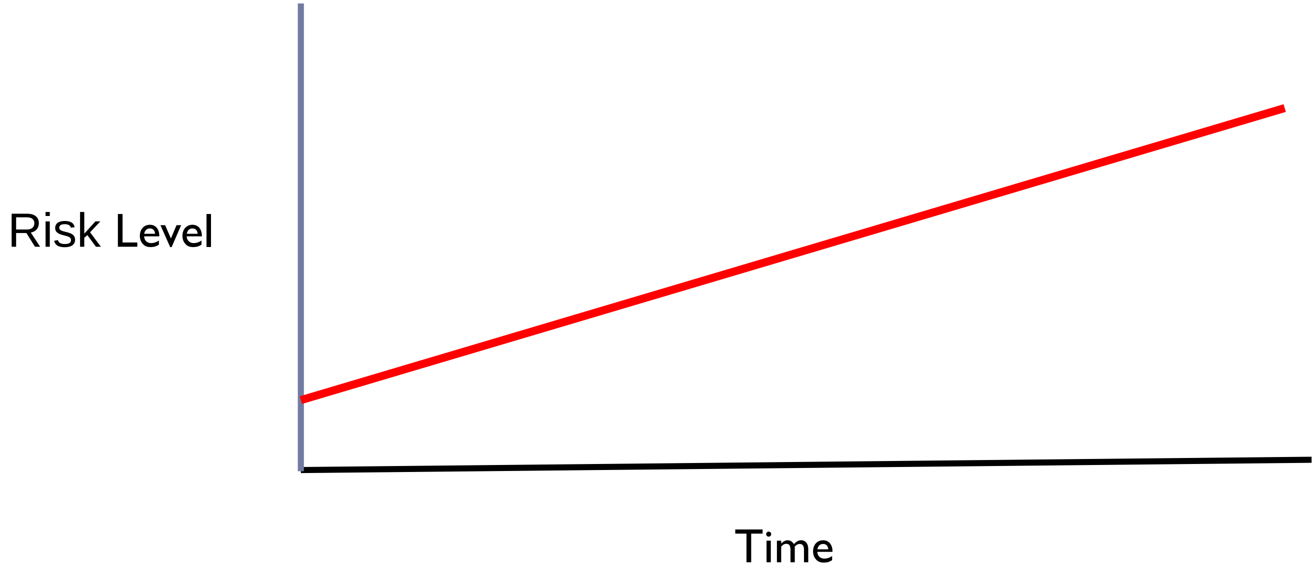
- **Nature of Risks in Cyberspace** and
- **View of Conventional Risk Management Approach** about it.

Conventional risk management approaches have difficulty in analyzing cyber risk and treating it appropriately.

1.2 View of Conventional Risk Management Approaches

Linear Growth Behavior

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. (**Linear Growth Behavior**)



(on the assumption that risk factors grow at a constant rate)

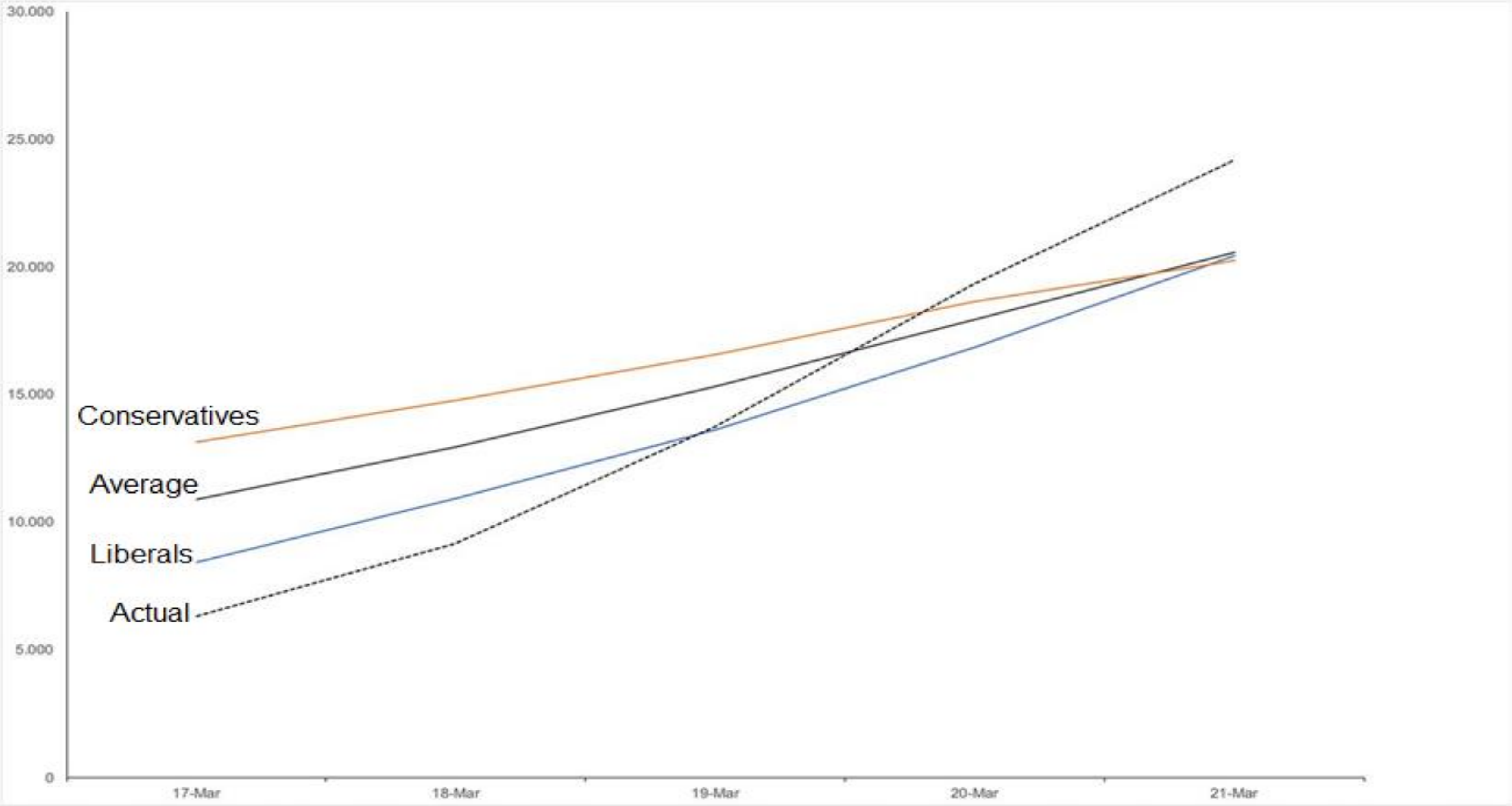
Example of Linear Growth Behavior

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.

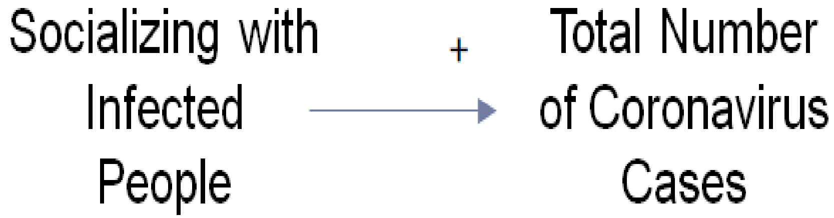
Example of Linear Growth Behavior

American participants were asked to guess the total number of coronavirus cases over specific period.



Example of Linear Growth Behavior

In this case, risk source is socializing with infected people without keeping distance and 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 increase in number of infected people at a proportional rate.



Socializing with Infected People

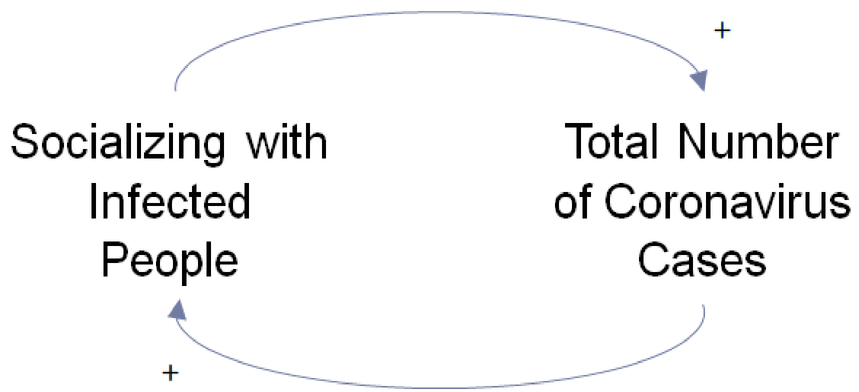
+

Total Number of Coronavirus Cases

This means people perceive that the relationship between risk source and risk level is linear.

Example of Exponential Growth Behavior

In reality, socializing with infected people without keeping distance increases coronavirus in an exponential manner because it grows into large effect on increase in number of infected people by cascading effects of a feedback loop.


+
Socializing with Infected People
Total Number of Coronavirus Cases
+

This means the relationship between risk source and risk level is non-linear.

1.3 Nature of Risks in Cyberspace

Cyberspace and Complex System

Cyberspace is a complex system. Management of risks in cyberspace is itself a complex process.

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 delay

Cyberspace and Complex System

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.

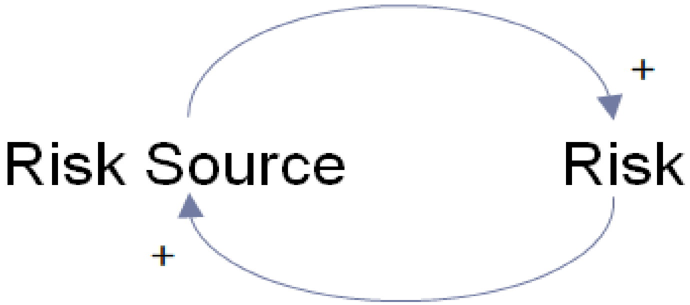
However, exponential growth and oscillation behavior of the risks cannot be treated properly by conventional management approaches because its behavior is caused by the non-linear relationship between risks and their factors and alters the state of equilibrium.

The objective of the research is to propose the new models to treat exponential growth and oscillation behavior of the risks in cyberspace using systems thinking to complement conventional risk management approaches.

Exponential Growth Behavior

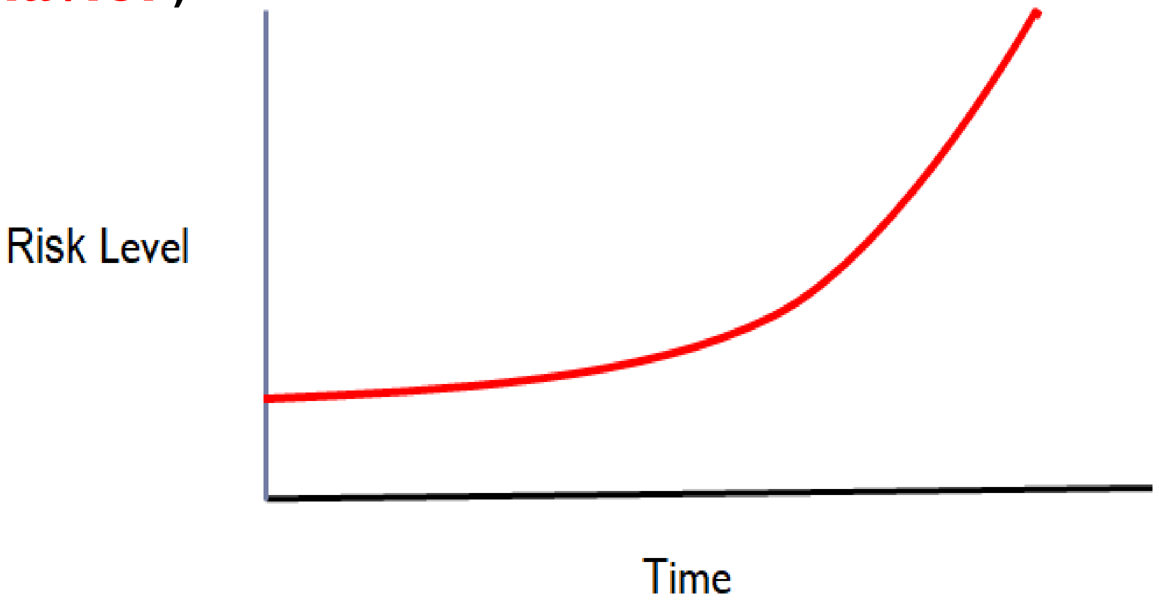
In cyberspace, small risk source can grow into large effect on level of the risks (non-linear relationship) by cascading effects through the global connectivity of the cyberspace.

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.



Exponential Growth Behavior

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. (**Exponential Growth Behavior**)

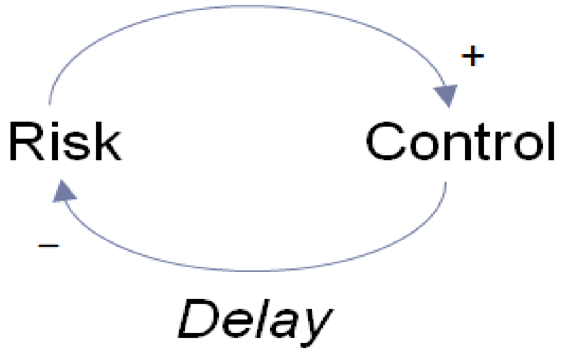


(on the assumption that risk factors grow at a constant rate)

Oscillation Behavior

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.

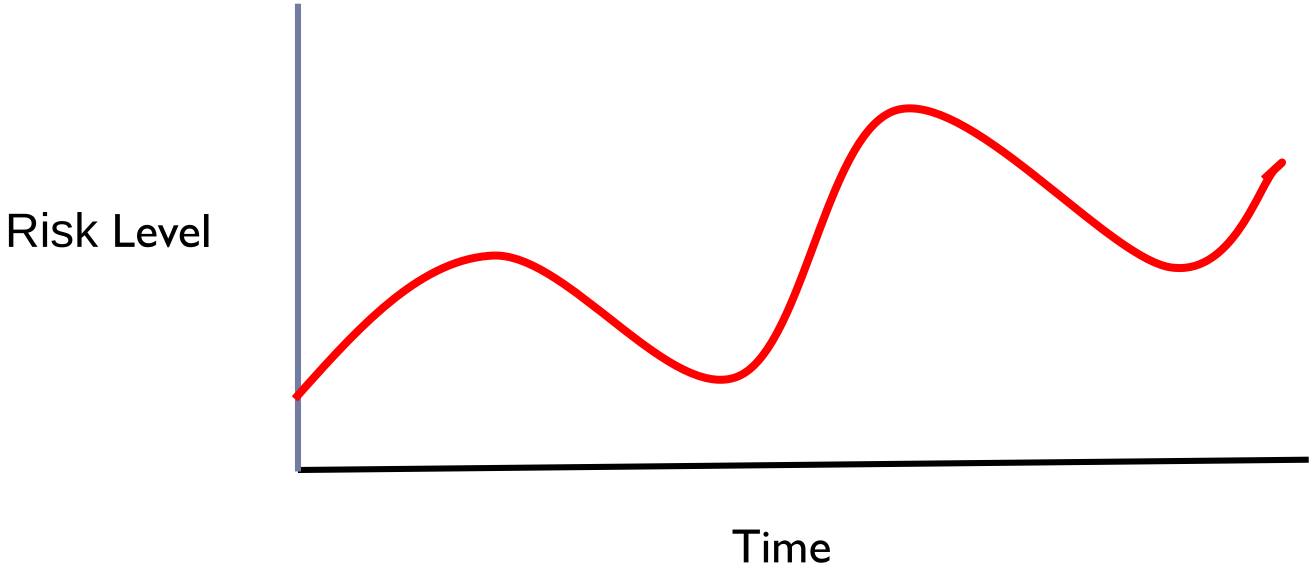
Complexity of the interconnections in the cyberspace may cause the delay of effects of the controls. Risk level exceeding an acceptable level cannot be reduced by implementation of controls with the same scale on the risk level exceeding an acceptable level. It is expressed as a balancing feedback loop with delay between risk and control.



Oscillation Behavior

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.

(**Oscillation Behavior**)



2. Previous Researches

Threats in Cyberspace

Clark [2] defines cyberspace as a hierarchical contingent system composed of people layer, information layer, logical layer and physical layer.

Meyers et al [6] construct taxonomies of cyber adversaries and methods of attack.

Hutchins et al [8] propose a cyber kill chain model to describe phases of intrusions, mapping adversary kill chain indicators to defender courses of action.

Hansman et al [5] propose to use the concept of dimensions that are a way of allowing for a classification of an attack. The dimensions are attack vector, targets of the attack, vulnerabilities, and possibility for an attack to have a payload or effect beyond itself.

Security and Risk Management

Buzan et al [9] defines **securitization** as 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.

Hansen and Nissenbaum [11] argues that the security logic ties referent objects, threats, and securitizing actors together in the cybersecurity sector.

ISO 31000:2018 [12] provides a common approach to managing any type of risk including cyber risk.

ISO/IEC 27005:2018 [13] provides guidelines for information security risk management in an organization.

NIST Cybersecurity Framework [14] helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

Systems Thinking and Cyber Risk

Heylighen [15] argues that complex systems such as the Internet have emergent properties that cannot be reduced to the mere properties of their parts.

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.

With amplification of positive feedback, initially small perturbations reinforce themselves so as to become ever more intense. (Scale-Free Theories)

Systems Thinking and Cyber Risk

Trcek [17] argues that although risk management is a well established in many areas, its direct translation to information systems is not straightforward because of the global connectivity of information systems and almost endless possible ways of interactions, etc.

Branagan et al [19] propose a threat network model based on threat event and threat propagation concepts. The model explores 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.

Limitations and Further Explorations

Limitations	Further Exploration
Propagation dimension and scale-free theories are not practically considered for cyber-attacks analysis.	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. Limitations of Conventional Risk Management Approach

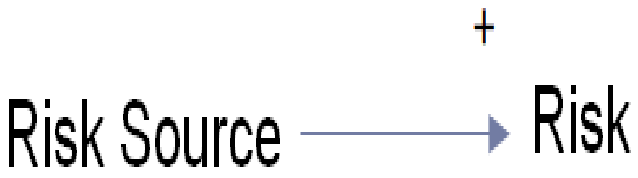
Overview

The limitations of conventional risk management approach are lack of consideration of:

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

Lack of Consideration of Emergent Properties of Risk

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 increase in risk source even as the state of risk changes.

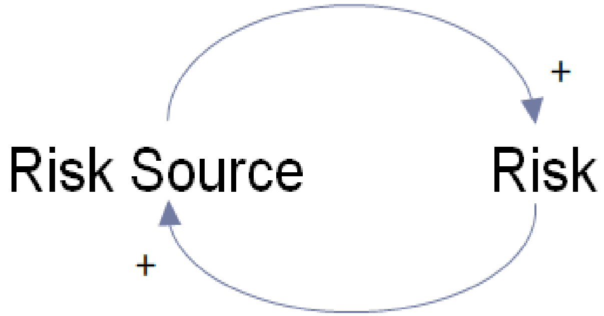


Lack of Consideration of Emergent Properties of Risk

Risk source and risk may not be in a linear relationship but in a feedback loop 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.



Lack of Consideration of Dynamics of Risk

Conventional risk management approaches tend to point to specific events to explain the risk without seeing the structures underlying these events because it sees 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.

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].

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

Requirements

Cyber risk analysis 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**

Cyber risk treatment needs the simulations that:

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

Systems Thinking

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.

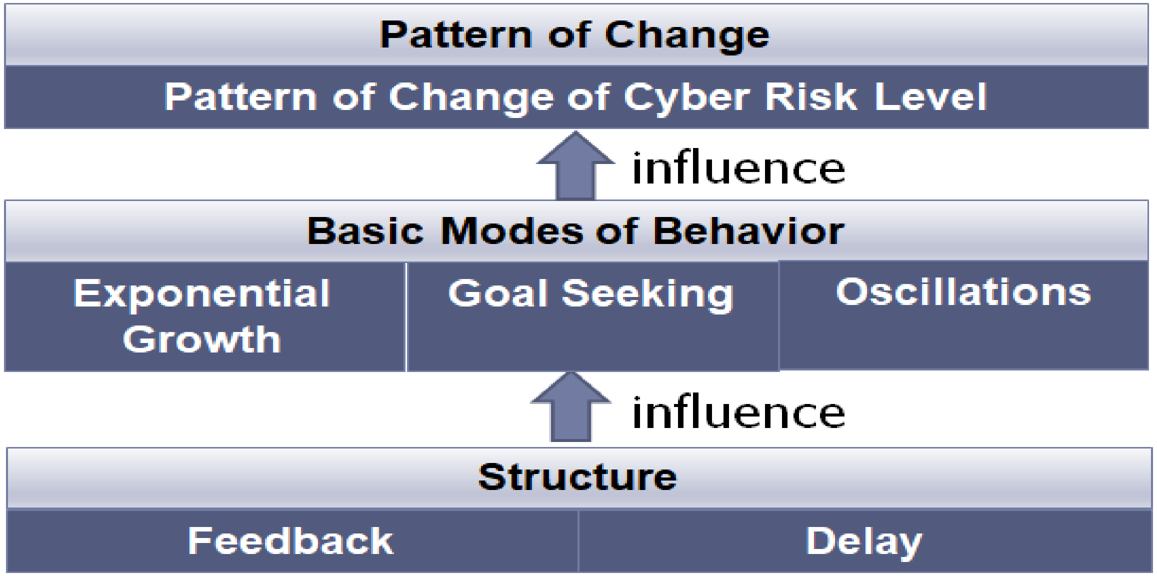
Groš [19] explains that the general features of any complex system are:

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

Systems Thinking

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 below:



Pattern of Change

Pattern of Change of Cyber Risk Level

influence

Basic Modes of Behavior

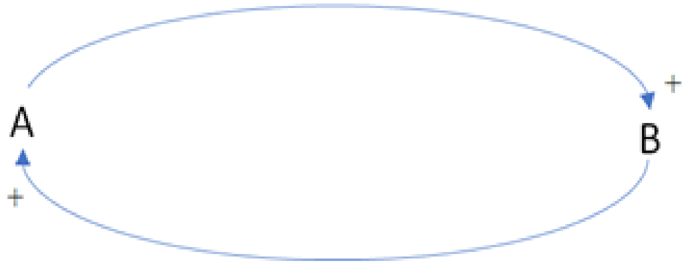
Exponential Growth | Goal Seeking | Oscillations

influence

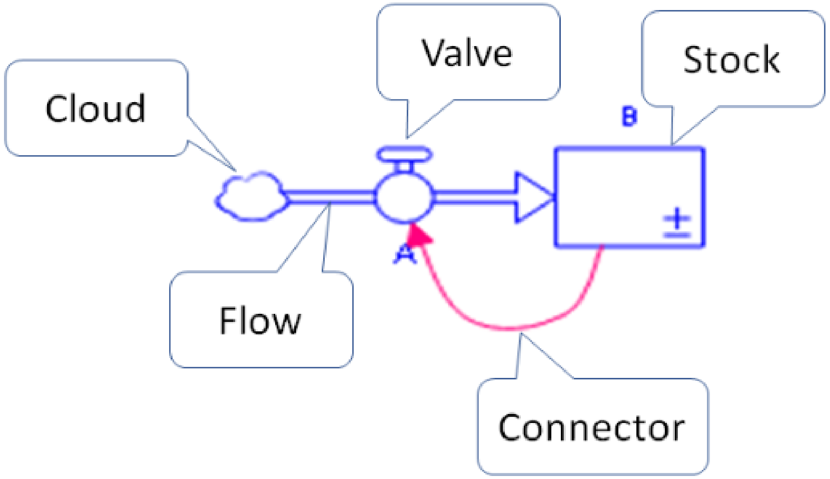
Structure

Feedback | Delay

Systems Thinking and System Dynamics



Feedback Loop Diagram in Systems Thinking



Stock and Flow Diagram in System Dynamics

5 Dynamic Cyber Risk Model (DCRM)

5.1 Overview

Dynamic Cyber Risk Model (DCRM)

At an organization level, a new model called Dynamic Cyber Risk Model (DCRM) is developed to

- 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).

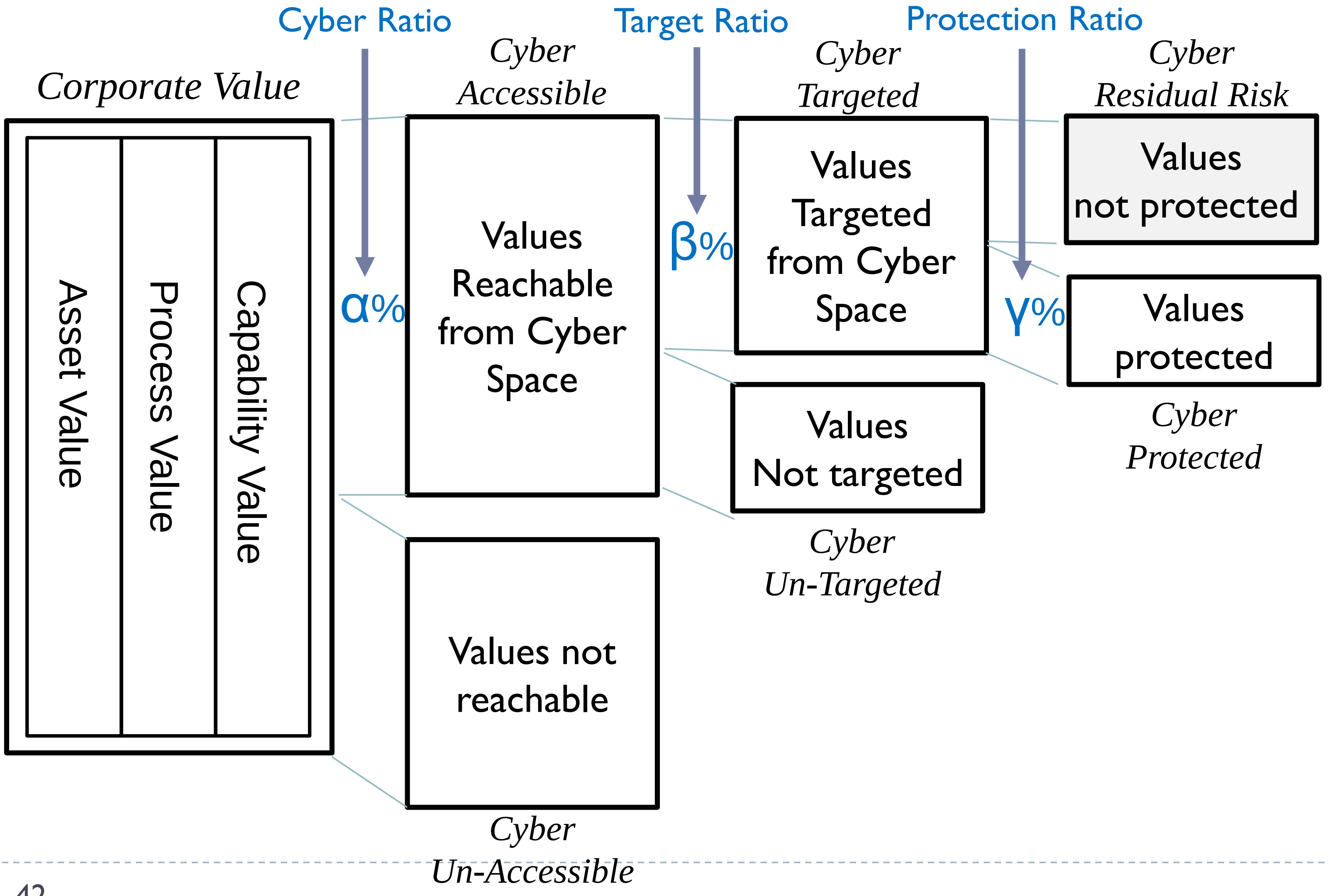
5.2 Cyber Risk Analysis

Overview

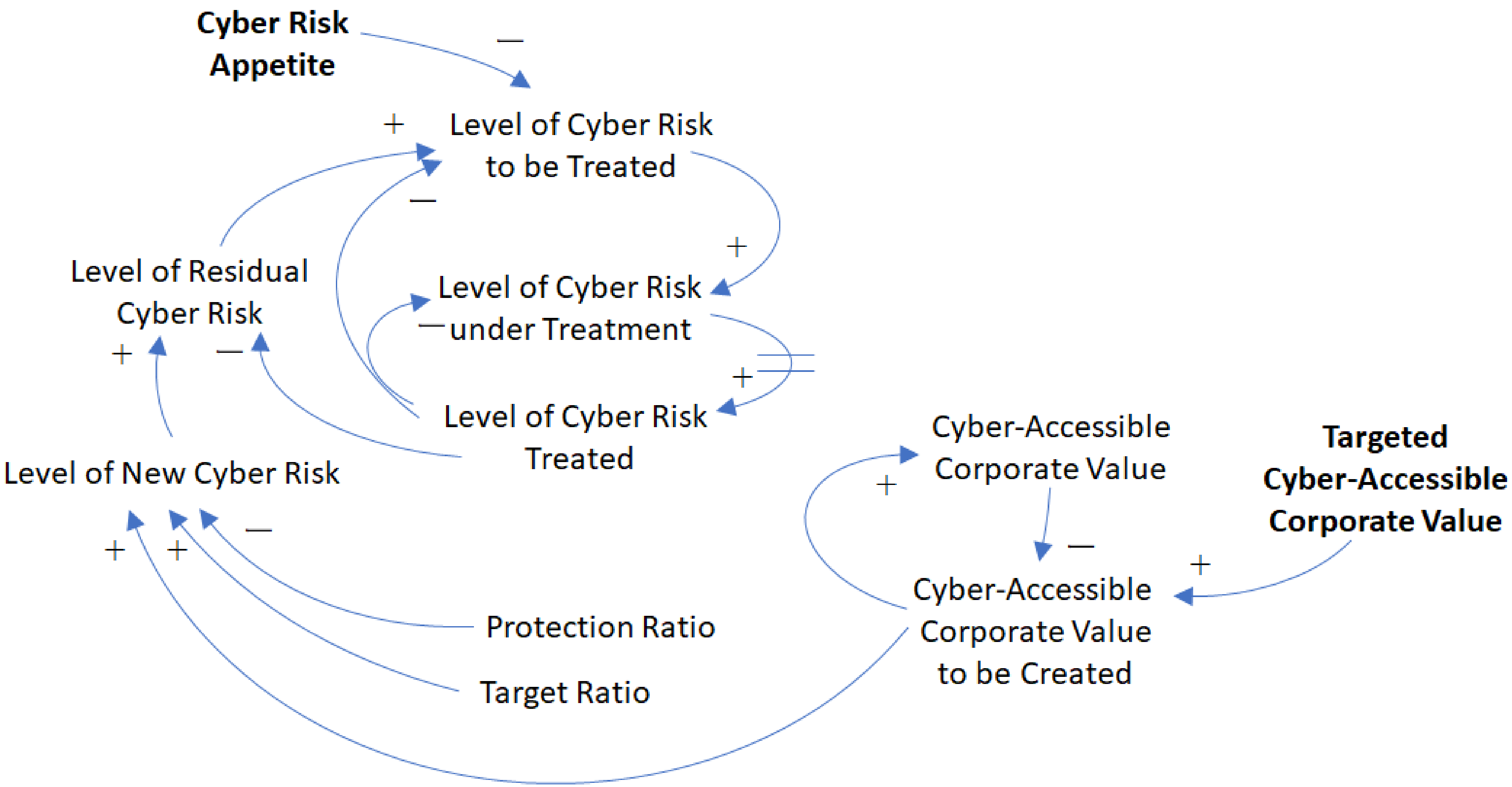
DCRM Feedback Loop Diagram is developed by application of systems thinking to the Corporate Value-Based Cyber Risk Model [23] for cyber risk analysis to identify the real causes of **oscillation** behavior of cyber risk level that leads to the implementation of excessive controls.

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. The main factors affecting cyber risk level and their relationships are identified as components of Corporate Value-Based Cyber Risk Model [23].

Corporate Value-Based Cyber Risk Model [23]



DCRM Feedback Loop Diagram


Cyber Risk Appetite
—
+
Level of Cyber Risk to be Treated
—
+
Level of Residual Cyber Risk
Level of Cyber Risk under Treatment
—
+
—
+
Level of Cyber Risk Treated
Level of New Cyber Risk
+
+
—
Protection Ratio
Target Ratio
Cyber-Accessible Corporate Value
+
—
Targeted Cyber-Accessible Corporate Value
+
Cyber-Accessible Corporate Value to be Created

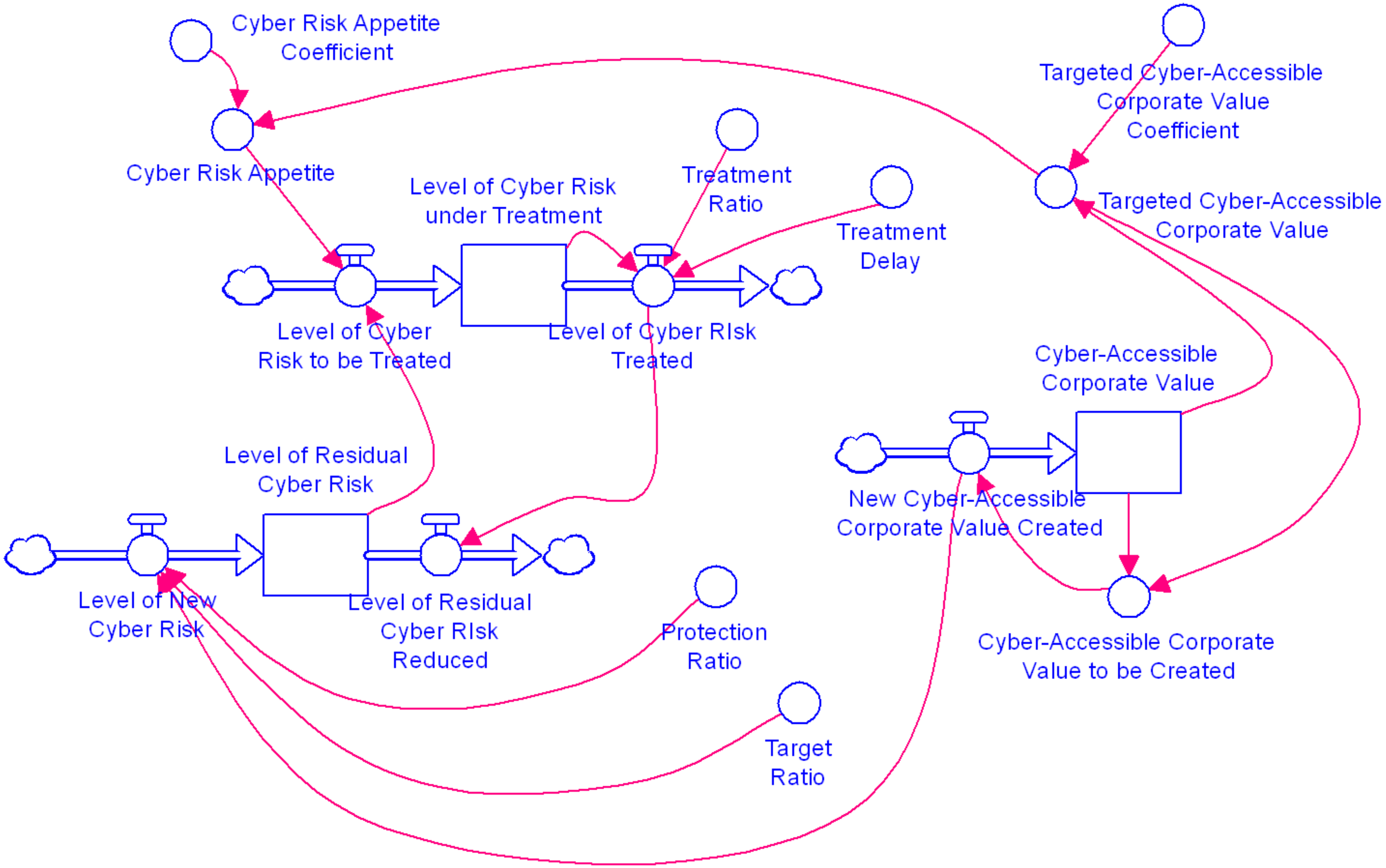
5.4 Cyber Risk Treatment

Overview

DCRM Stock and Flow Diagram is developed by converting DCRM Feedback Loop Diagram using system dynamics for cyber risk treatment.

It is simulated to determine how **oscillation** behavior of cyber risk level that leads to the implementation of excessive controls might be influenced.

DCRM Stock and Flow Diagram


Cyber Risk Appetite Coefficient
Cyber Risk Appetite
Level of Cyber Risk under Treatment
Treatment Ratio
Treatment Delay
Targeted Cyber-Accessible Corporate Value Coefficient
Targeted Cyber-Accessible Corporate Value
Level of Cyber Risk to be Treated
Level of Cyber RIsk Treated
Cyber-Accessible Corporate Value
Level of Residual Cyber Risk
New Cyber-Accessible Corporate Value Created
Level of New Cyber Risk
Level of Residual Cyber RIsk Reduced
Protection Ratio
Cyber-Accessible Corporate Value to be Created
Target Ratio

First Simulation

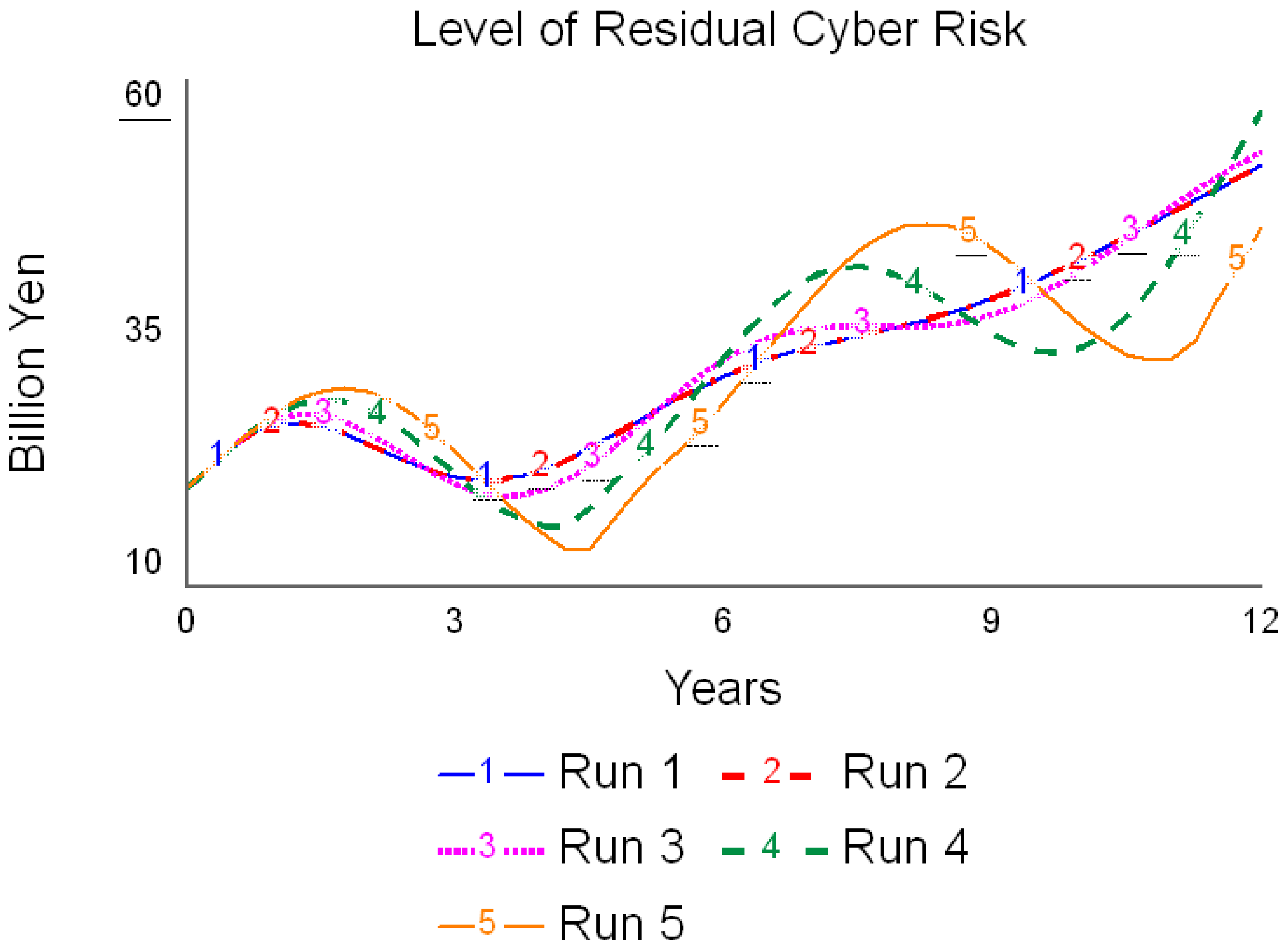
How **oscillation** behavior of cyber risk level occurs is simulated by DCRM Stock and Flow Diagram.

The simulation shows how the patterns of the "Level of Residual Cyber Risk" is influenced by changing the "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)

"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.

First Simulation



Second and Third Simulation

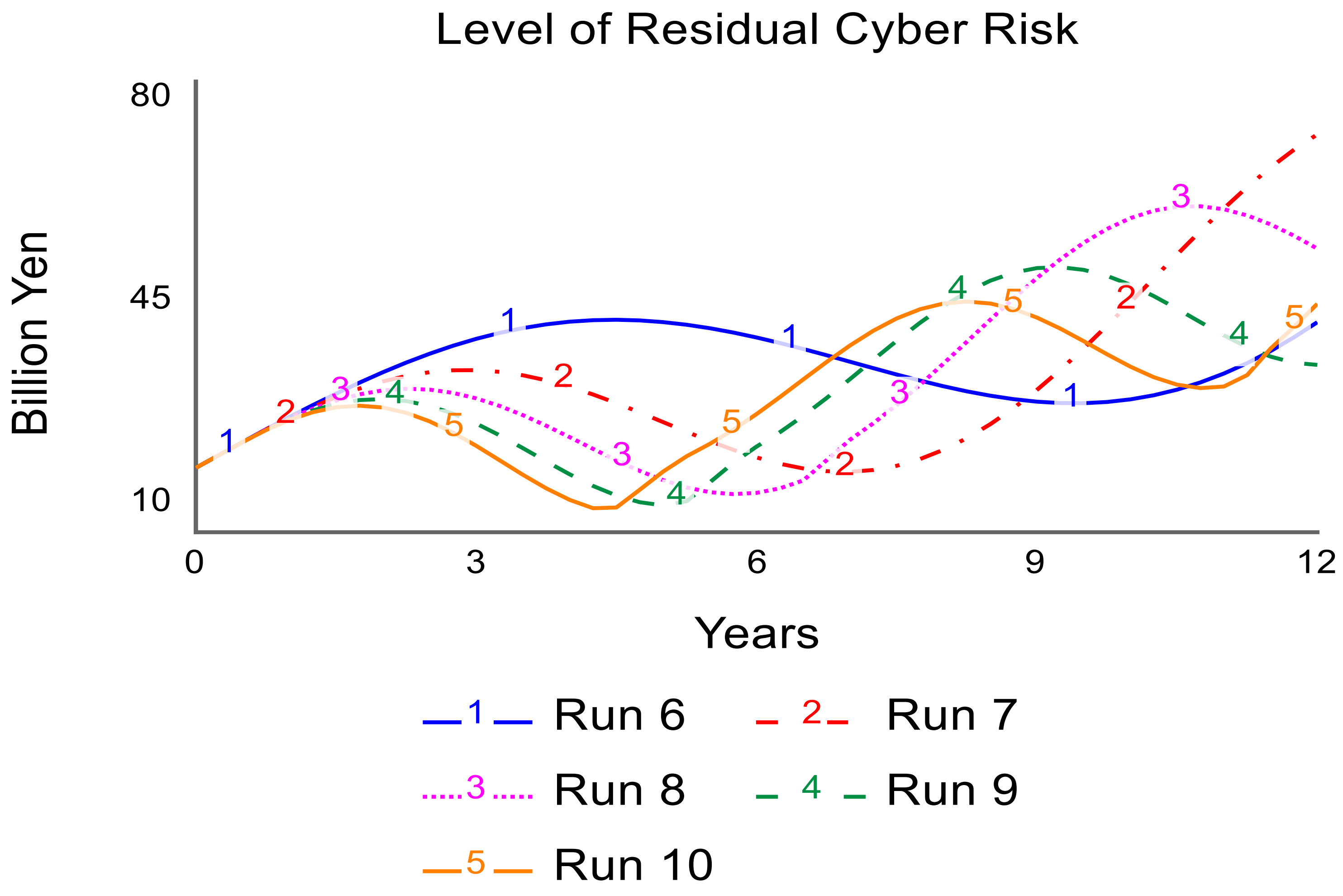
How **oscillation** behavior of cyber risk level might be influenced is simulated by DCRM Stock and Flow Diagram.

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:

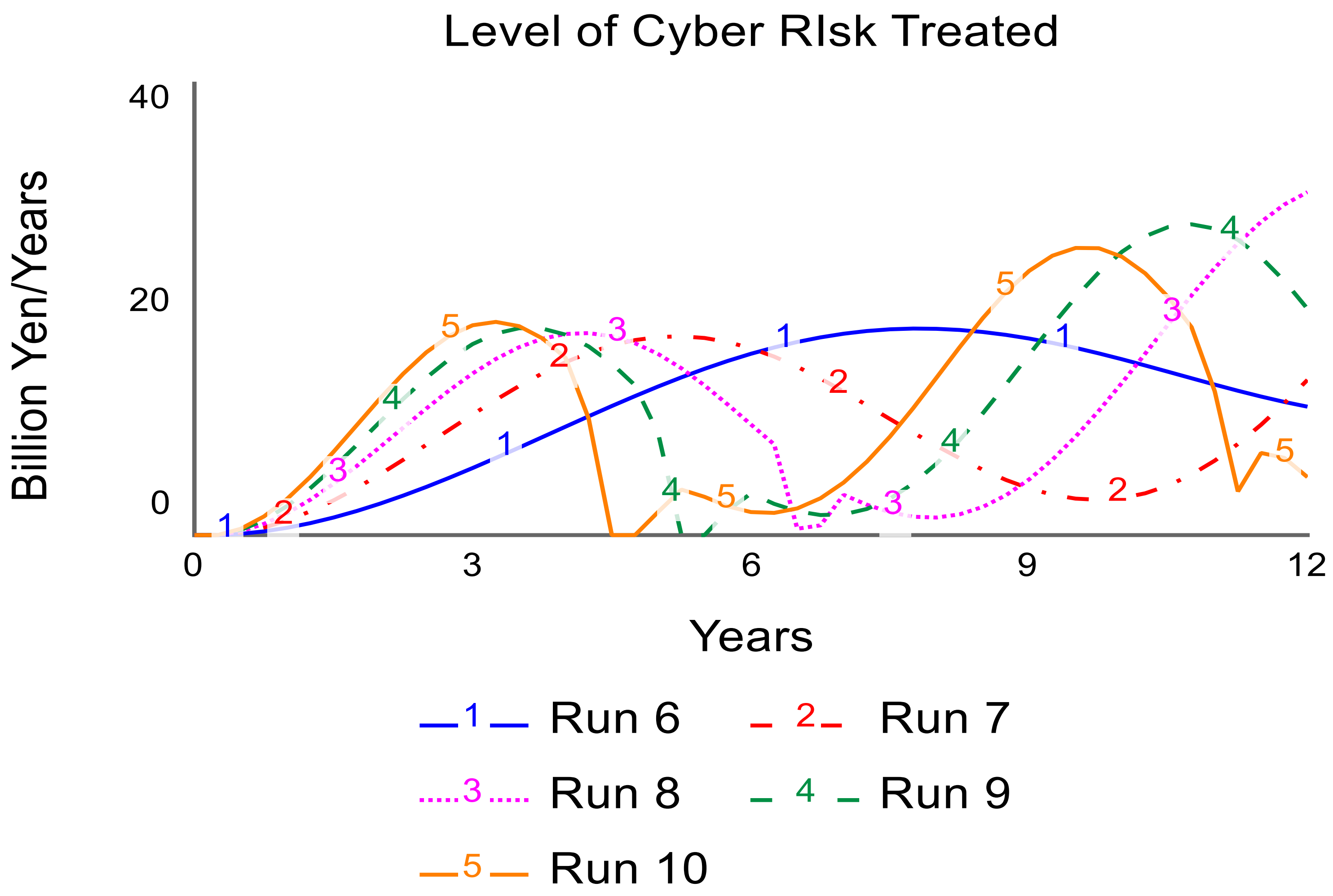
Run 6:	0.2 (20%)
Run 7:	0.4 (40%)
Run 8:	0.6 (60%)
Run 9:	0.8 (80%)
Run 10:	1.0 (100%)

"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.

Second Simulation



Third Simulation



5.5 Consideration

First Simulation

The first simulation of DCRM Stock and Flow Diagram validated the results of cyber risk analysis - the underlying cause of **oscillation** behavior of cyber risk level was a **balancing feedback loop** among the factors affecting the cyber risk with a **delay.**

Using DCRM, the organizations can simulate how the risk level will behave in long term by indicating the delay of effect of the control. 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 implementing more strict control 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.

Second and Third Simulations

The second and third simulations of DCRM Stock and Flow Diagram provided useful information to determine how **oscillation** behavior of cyber risk level might be influenced.

- lowering the **ratio of the implementation of controls** smoothed uneven effects of the controls on the level of cyber risk over time.

Using DCRM, the organizations can simulate how the risk level will behave in long term if they do not implement more strict controls 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 implement controls.

6 Power of Cyberspace Model (POCM)

6.1 Overview

Power of Cyberspace Model (POCM)

At an individual cyber-attack level, a new model called Power of Cyberspace Model (POCM) is developed to

- 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).

6.2 Cyber Risk Analysis

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.

Overview

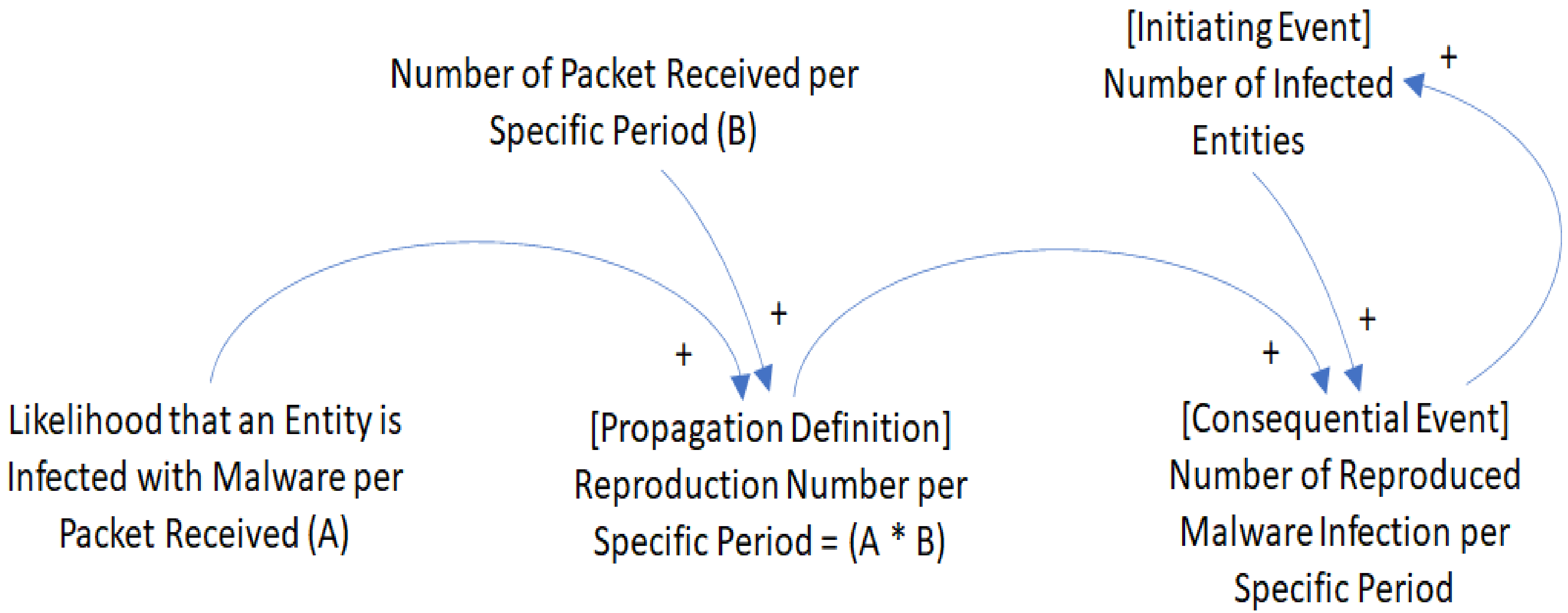
There are two main elements of cyber-attacks:

- **Attack vector**
- **Attack propagation**

The **attack vector** is the method by which an attack reaches its target [5].

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.

POCM Feedback Loop Diagram for Attack Propagation



Number of Packet Received per Specific Period (B)

[Initiating Event] Number of Infected Entities

Likelihood that an Entity is Infected with Malware per Packet Received (A)

[Propagation Definition] Reproduction Number per Specific Period = (A * B)

[Consequential Event] Number of Reproduced Malware Infection per Specific Period

6.3 Cyber Risk Treatment

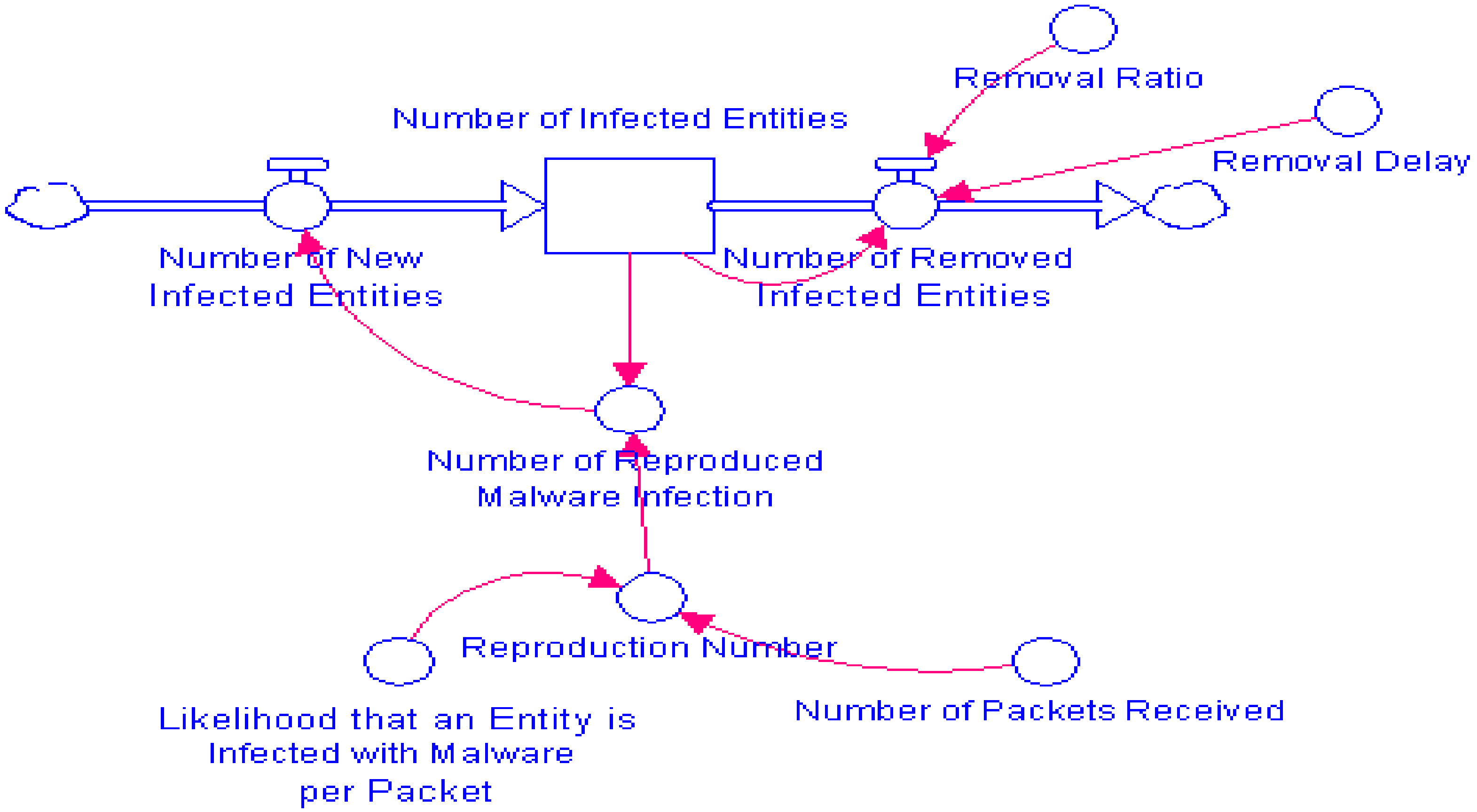
Overview

POCM Stock and Flow Diagram for Attack Propagation is developed by converting POCM Feedback Loop Diagram for Attack Propagation using system dynamics for cyber risk treatment.

It is simulated to determine how **exponential growth** behavior of cyber risk level might be influenced.

POCM Stock and Flow Diagram for Attack Propagation

.



First Simulation

How **exponential growth** behavior of cyber risk level occurs is simulated by POCM Stock and Flow Diagram.

The simulation on the outbreak of **Mirai** in 2016 is conducted by referring to the analysis of Antonakakis et al [29].

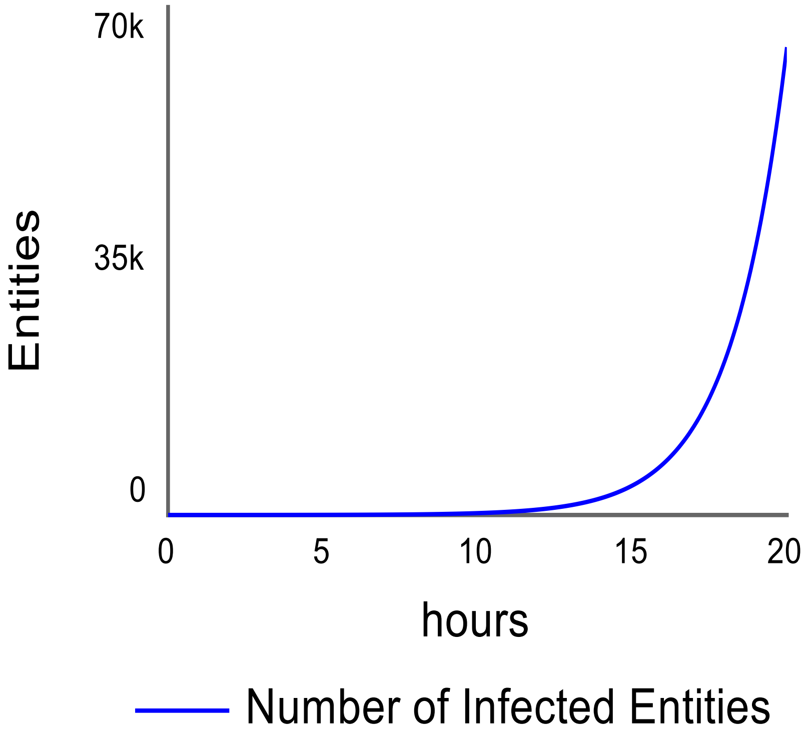
The simulation is conducted in a way that the number of infected IoT devices reaches 64,500 within 20 hours.

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 [30].

[a] NICTER Analysis Report 2019 of National Institute of Information and Communications Technology (NICT)

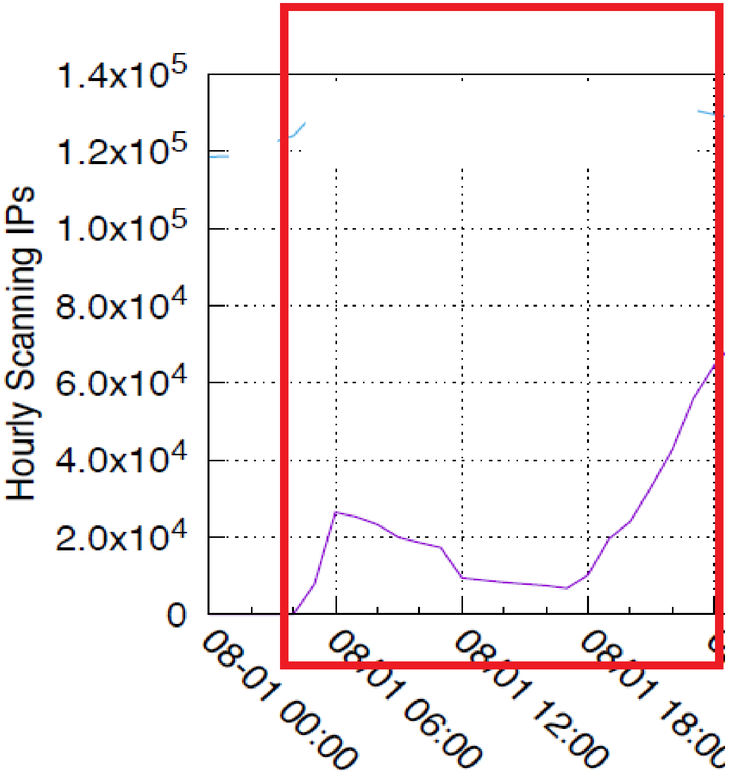
First Simulation

Pattern of Number of LoT Devices Infected by **Mirai** for Initial 20 Hours in Simulation of POCM.



First Simulation

Pattern of Number of LoT Devices Infected by **Mirai** for Initial 20 Hours in Analysis of Antonakakis et al [29].



First Simulation

It is recognized that **propagation** effects are shown in continuous steep slope leading to the target value.

Both of the result of the simulation of POCM and the analysis of Antonakakis show:

- The continuous steep slope leading to the target value (64,500) starts around 11 hours.
- The number of infected device is 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. is very similar.

Second Simulation

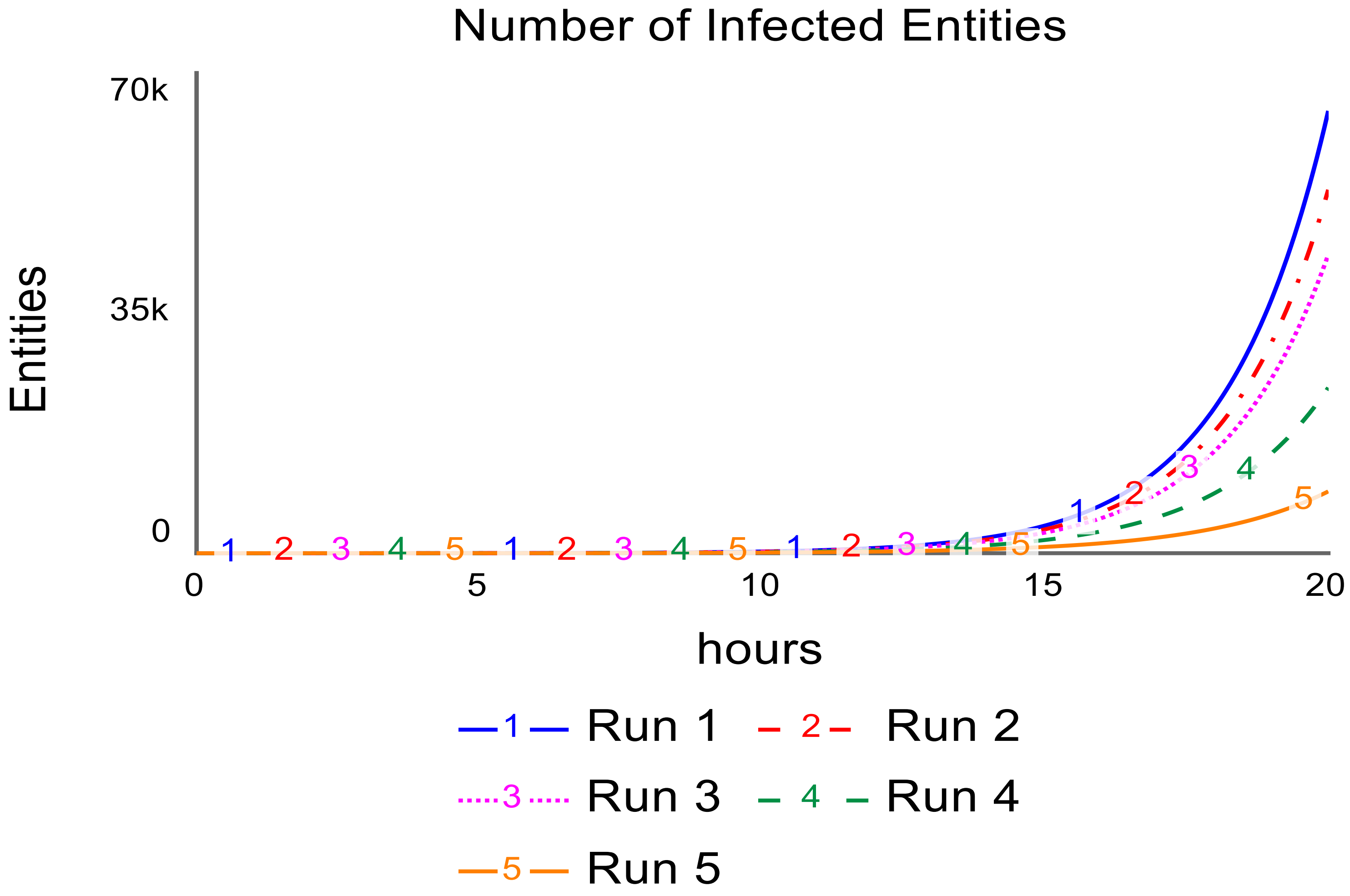
How **exponential growth** behavior of cyber risk level might be influenced is simulated by POCM Stock and Flow Diagram.

The second 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:

- 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%)

"Removal Ratio" indicates the ratio at which infected devices are removed.

Second Simulation



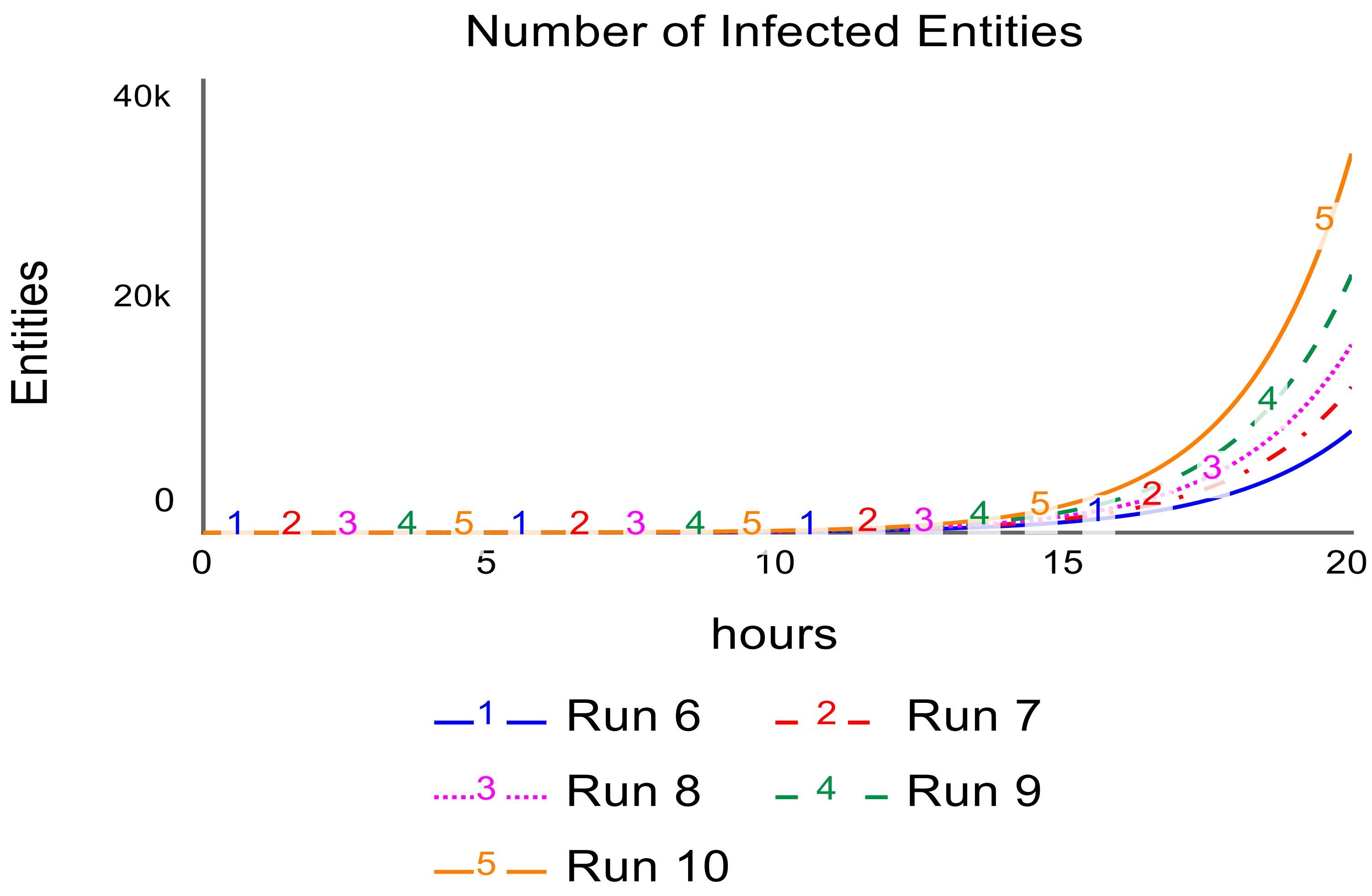
Third Simulation

The third 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 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)

"Removal Delay" indicates the time taken to remove infected devices in hour.

Third Simulation



6.4 Consideration

Cyber Risk Treatment (First Simulation)

The first simulation of POCM Stock and Flow Diagram validated the results of cyber risk analysis - the underlying cause of **exponential growth** behavior of cyber risk level was a **reinforcing feedback loop** among events in cyberspace.

- **Exponential growth** behavior of cyber risk level was caused by **attack propagation** that is formed by a **reinforcing feedback loop** among events in cyberspace.
- The simulation on the **attack propagation** of Mirai in 2016 reasonably accorded with reality that described in the analysis of Antonakakis et al. [29].

Cyber Risk Treatment (Second and Third Simulations)

The second and third simulations of POCM Stock and Flow Diagram provided useful information to determine how **exponential growth** behavior of cyber risk level might be influenced.

- Even if 10% of infected devices were removed, it had a significant positive effect on mitigation of **attack propagation** (86% reduction of infected devices).
- Delay to remove the infected devices offset 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 devices increased nearly by 4 times.

7 Conclusion

Overview

The new models 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 Approach** 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.

Future Research

The new models 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.

8. Reference List

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.

Reference List

[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.

Reference List

[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.

Reference List

[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.

Reference List

[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

Reference List

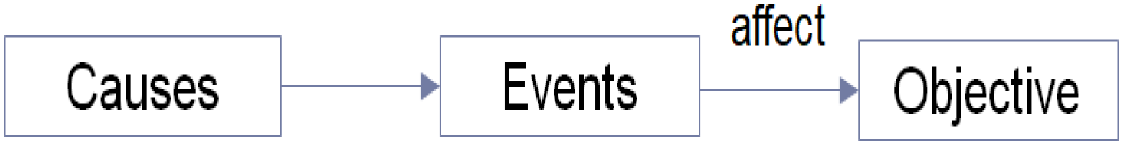
[34] National Institute of Information and Communications Technology (NICT). 2020. NICTER Observation Report 2019.

Appendix

1.2.1 View of Conventional Risk Management Approaches

View of Conventional Risk Management Approaches

In ISO 31000:2018 [1] is a representative risk management standard and defines risk as 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.

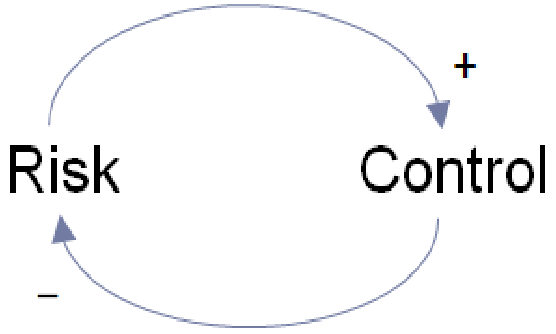


Conventional risk management approaches tend to see that the factors affecting the risk and their effect on the risk level are close in time and space and their relationship is linear because they tend to ignore feedback processes and associated delays.

Goal Seeking Behavior

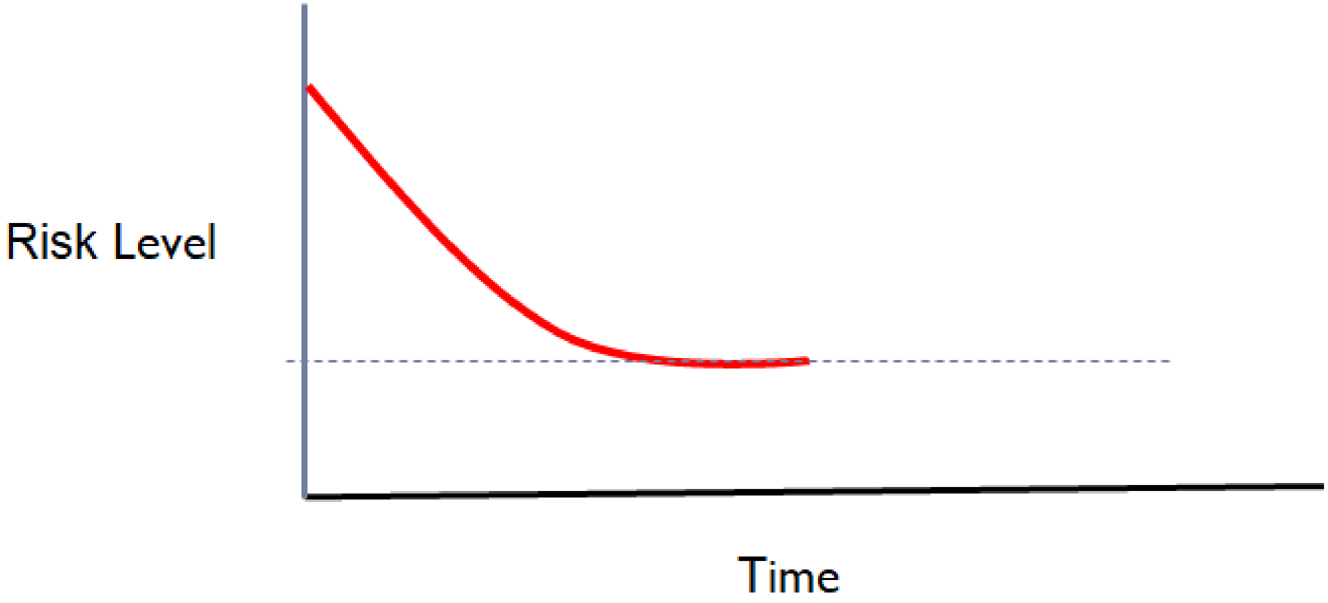
Conventional risk management approaches assume that the control instantly produces a proportional effect on the risk level (linear relationship) because of the lack of the consciousness of delay.

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 .



Goal Seeking Behavior

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.



Goal seeking behavior seeks equilibrium (acceptable risk level).

1.2.3 Summary

Issues (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 behaviors 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

Objectives

The objective of the research is to propose the new models to complement conventional risk management approaches as stated in ISO 31000 (Risk Management Standard) [1] and ISO/IEC 27005 (Information Security Risk Management Standard) [4] to fill the gap between the **nature of cyber risk** and **view of conventional risk management approach** 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.

4.2 Methodologies

System Thinking

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.

System Thinking

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.

System Thinking

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 include:

- exponential growth, created by reinforcing feedback;.
- goal seeking, created by balancing feedback; and
- oscillation, created by balancing feedback with delay

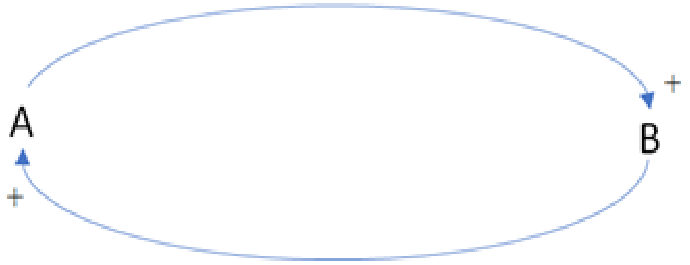
System Thinking

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.

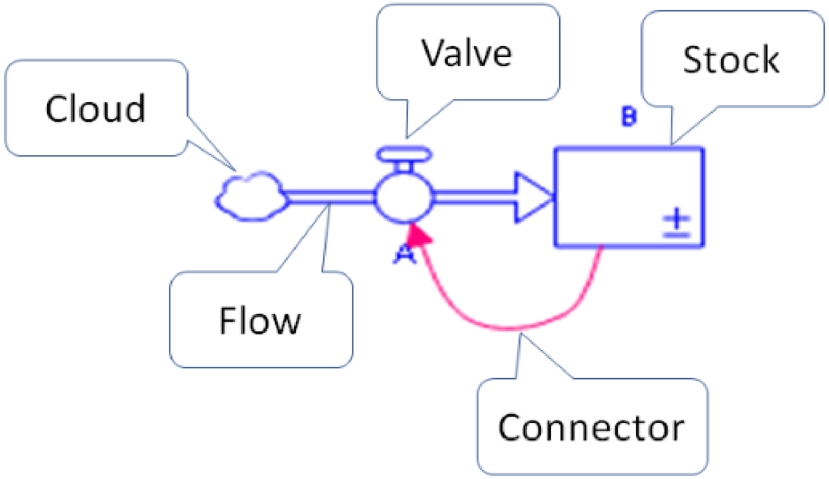
Goal seeking arises from balancing feedback. Every negative loop includes a process to compare the desired and actual conditions and take corrective action. Large gaps between desired and actual states tend to generate large responses while small gaps tend to generate small responses.

Oscillation arises from balancing feedback with delay. The state of the system constantly overshoots its equilibrium state, reserves, then undershorts, and so on. The delay causes 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.

Systems Thinking and System Dynamics



Feedback Loop Diagram in Systems Thinking



Stock and Flow Diagram in System Dynamics

5 Dynamic Cyber Risk Model (DCRM)

5.1 Overview

Dynamic Cyber Risk Model (DCRM)

At an organization level, a new model called Dynamic Cyber Risk Model (DCRM) is developed to

- 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).

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.

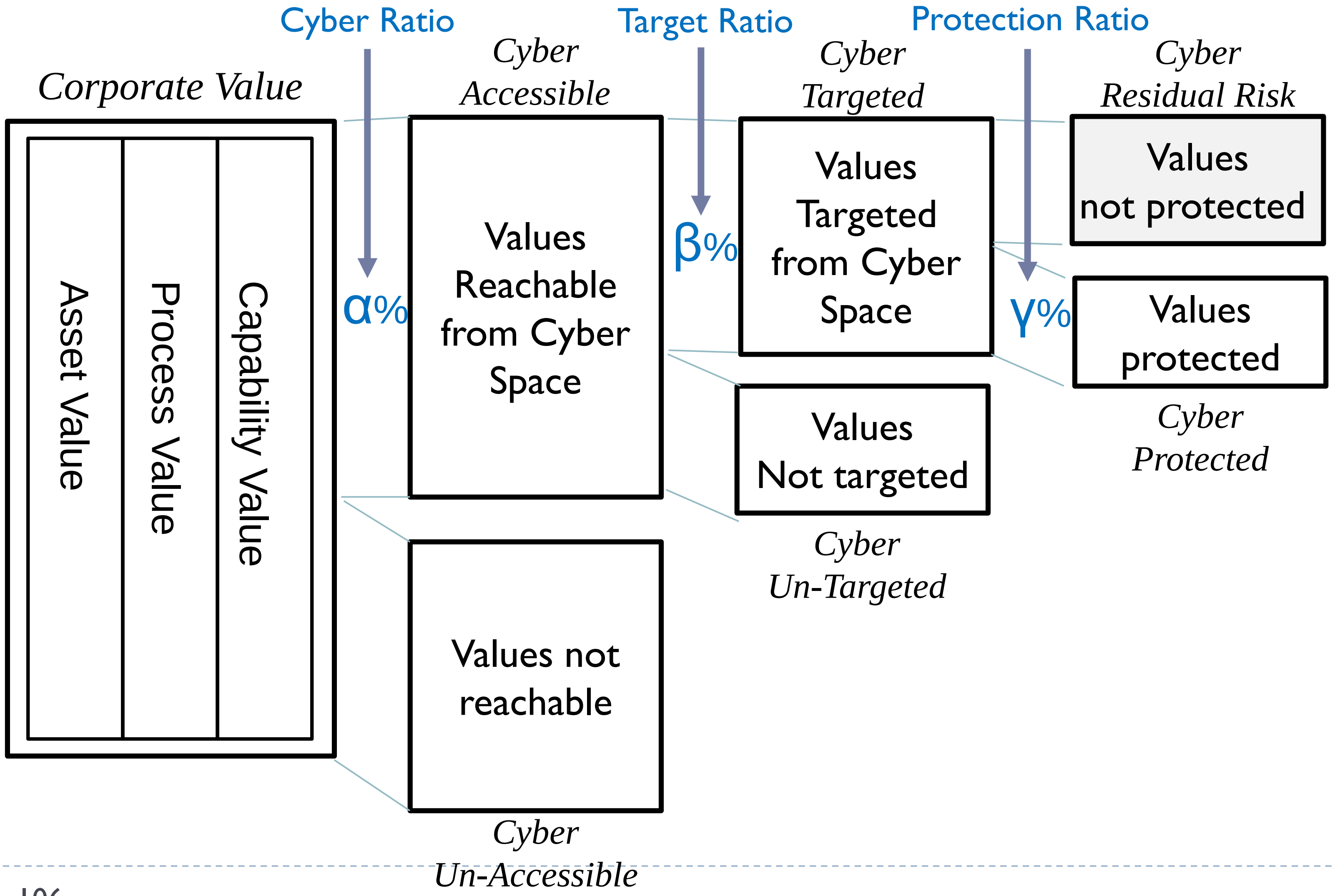
5.2 Cyber Risk Analysis

Overview

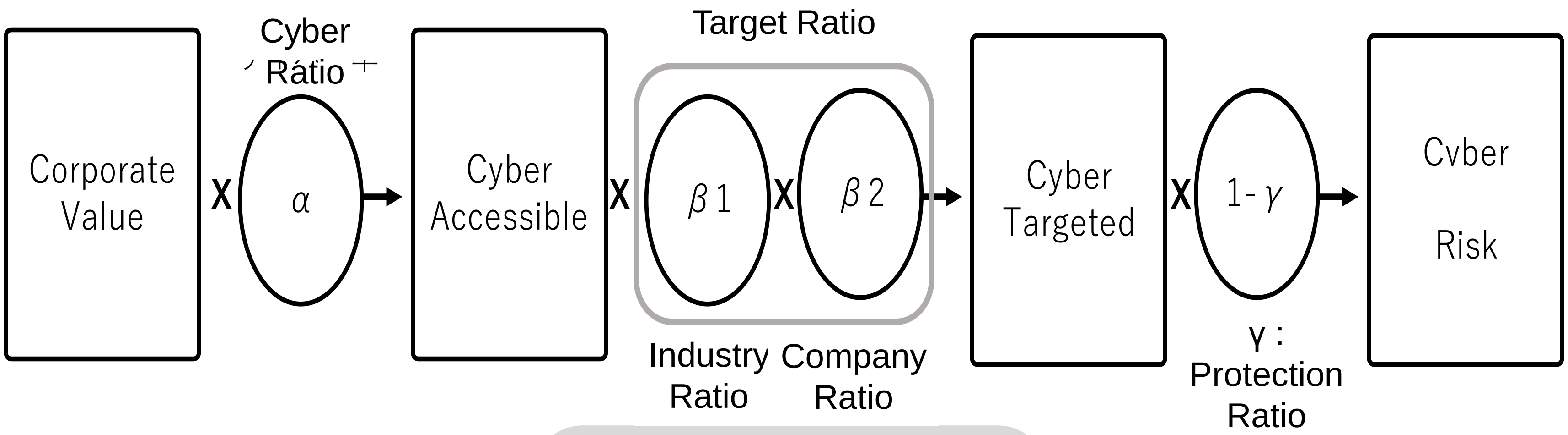
DCRM Feedback Loop Diagram is developed by application of systems thinking to the Corporate Value-Based Cyber Risk Model [23] for cyber risk analysis to identify the real causes of **oscillation** behavior of cyber risk level that leads to the implementation of excessive controls.

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. The main factors affecting cyber risk level and their relationships are identified as components of Corporate Value-Based Cyber Risk Model [23].

Corporate Value-Based Cyber Risk Model [23]



Corporate Value-Based Cyber Risk Model



Cyber Ratio

α

%

Depend on corporate IT strategy and implementation

Target Ratio

β

%

Depend on cyber attack tendency, sector characteristics, and corporate character

Protection Ratio

γ

%

Depend on selected counter-measures and effective managements

[5] Ohki et al, K. 2018.A proposal of cyber security risk modeling based on corporate values for business executives. Japan Society of Security Management. Vol.32, No.1

Corporate Value-Based Cyber Risk Model

Corporate Value =

Asset Value + Process Value + Capability Value

- Asset value
  - Past Value accumulated in the assets
  - Shown in Balance Sheet
- Process Value
  - Current Value creation through business processes
  - Shown in P/L statement
- Capability Value
  - Source of future competitiveness
  - Utilize Resource based view

[5] Ohki et al, K. 2018.A proposal of cyber security risk modeling based on corporate values for business executives. Japan Society of Security Management.Vol.32, No.1

Corporate Value-Based Cyber Risk Model

Cyber-accessible corporate value is calculated by multiplying **corporate value** by cyber ratio.

- Cyber ratio is the ration of corporate assets, processes and capabilities that are accessible from cyberspace.

Cyber-targeted corporate value is calculated by multiplying **cyber-accessible corporate value** by target ratio.

- Target ratio is the likelihood that cyber attacks occur.

Cyber risk is calculated by multiplying **cyber-targeted corporate value** by (1 - protection ratio).

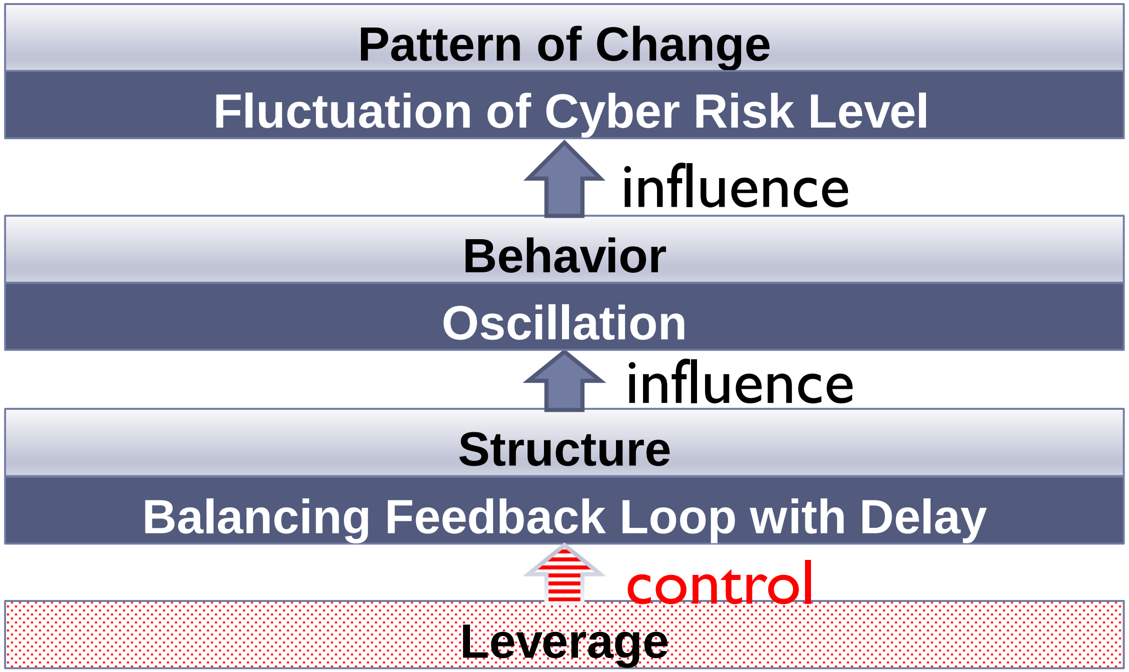
- Protection ratio is the likelihood that the implementation of controls prevents cyber-attacks from occurring.

[5] Ohki et al, K. 2018. A proposal of cyber security risk modeling based on corporate values for business executives. Japan Society of Security Management. Vol.32, No.1

5.2 Concept

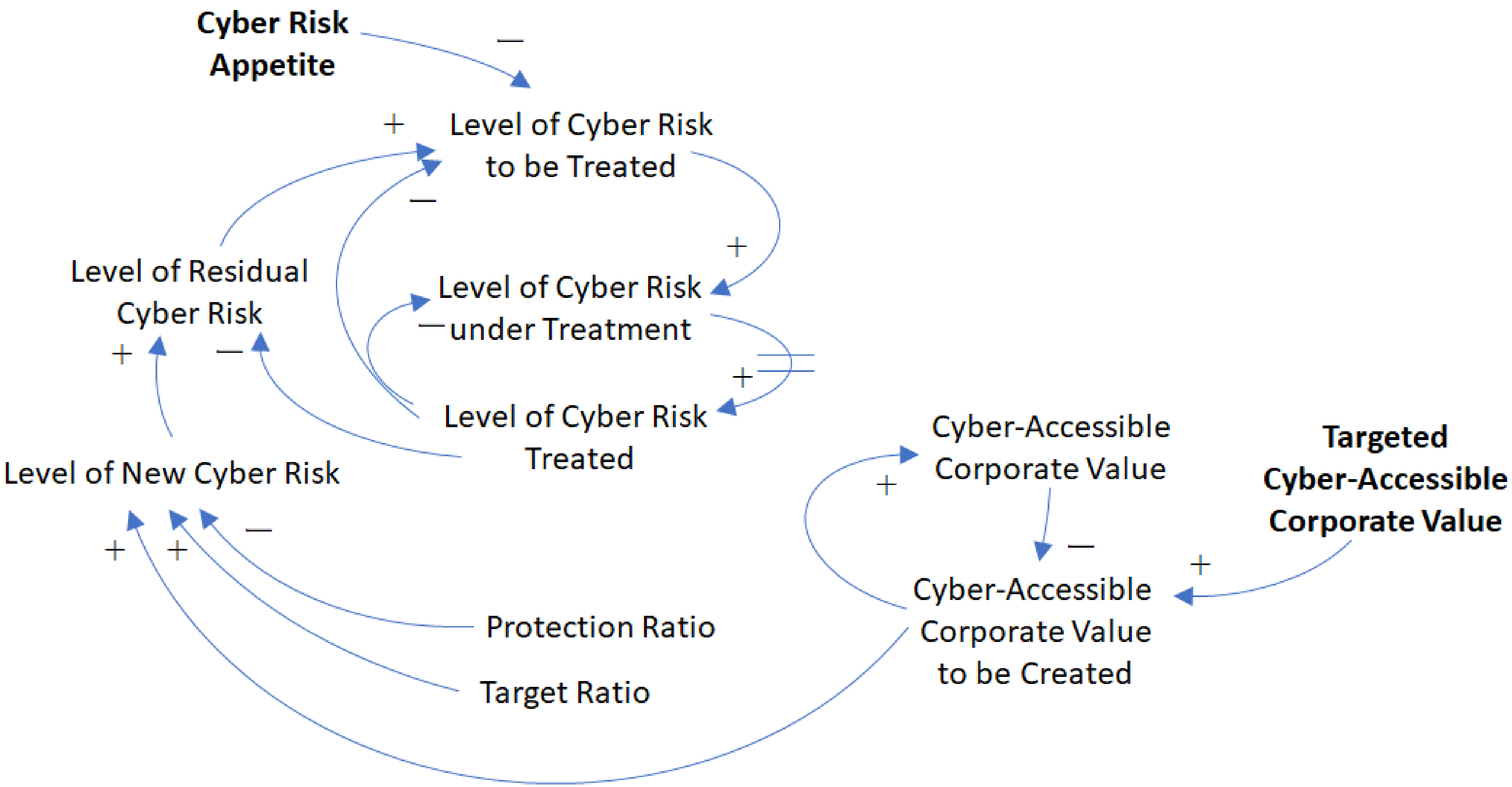
Cyber Risk Analysis

DCRM Feedback Loop Diagram identified that the underlying cause of **oscillation** behavior of cyber risk level was a **balancing feedback loop** among the factors affecting the cyber risk with a **delay.**



5.3 Cyber Risk Analysis

DCRM Feedback Loop Diagram



Cyber Risk Appetite

Level of Cyber Risk to be Treated

Level of Cyber Risk under Treatment

Level of Cyber Risk Treated

Level of Residual Cyber Risk

Level of New Cyber Risk

Protection Ratio

Target Ratio

Cyber-Accessible Corporate Value

Cyber-Accessible Corporate Value to be Created

Targeted Cyber-Accessible Corporate Value

Scenario

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

- Because of **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

Assumptions of Simulation

For the setting of environment in which the organization manages cyber risk, the values that faithfully represent reality are carefully chosen as shown below:

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 (100%) in 1st Simulation
Treatment Delay	1.0 (1 Year Delay) in 2nd & 3rd Simulation
Level of Residual Cyber Risk	2 Billion Yen
Level of Cyber Risk under Treatment	0 Yen

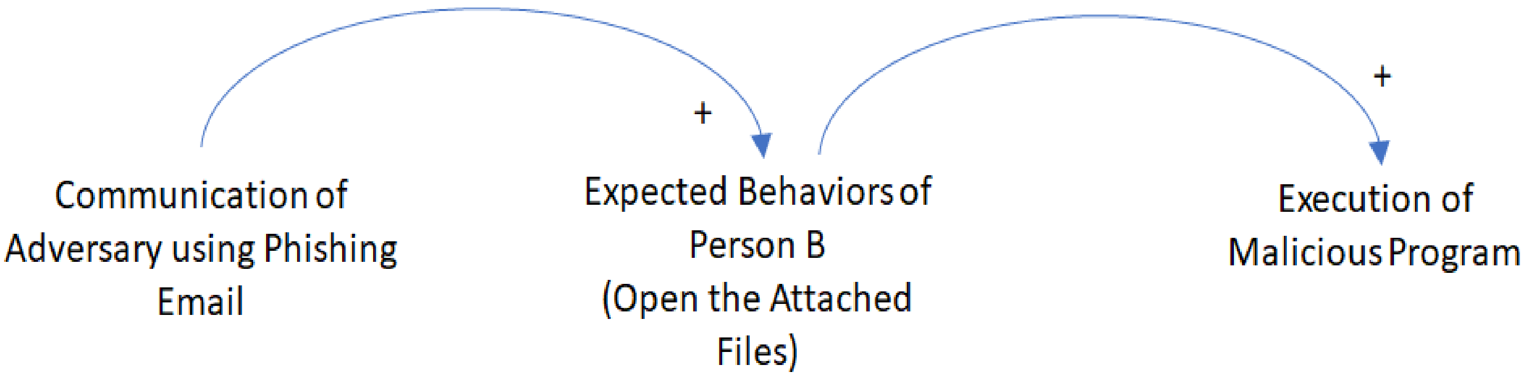
_6.2 Cyber Risk Analysis

POCM Feedback Loop Diagram for Attack Propagation

- An **initiating event** occurs when a certain number of entities are infected in cyberspace.
- A **consequential event** occurs when malware infection is reproduced by the entities infected with malware by the **initiating event** per specific period.
- **Propagation definition** indicates expected number of infection directly reproduced by one infected entity per specific period. It depends on **number of packets received per specific period** and **likelihood that the entity is infected with malware per packet.**

Example of POCM Feedback Loop Diagram for Attack Vector

The example diagram is developed for the communication conducted by an adversary using an email. This attack vector influences likelihood that the first round of initiating event occurs in attack propagation.

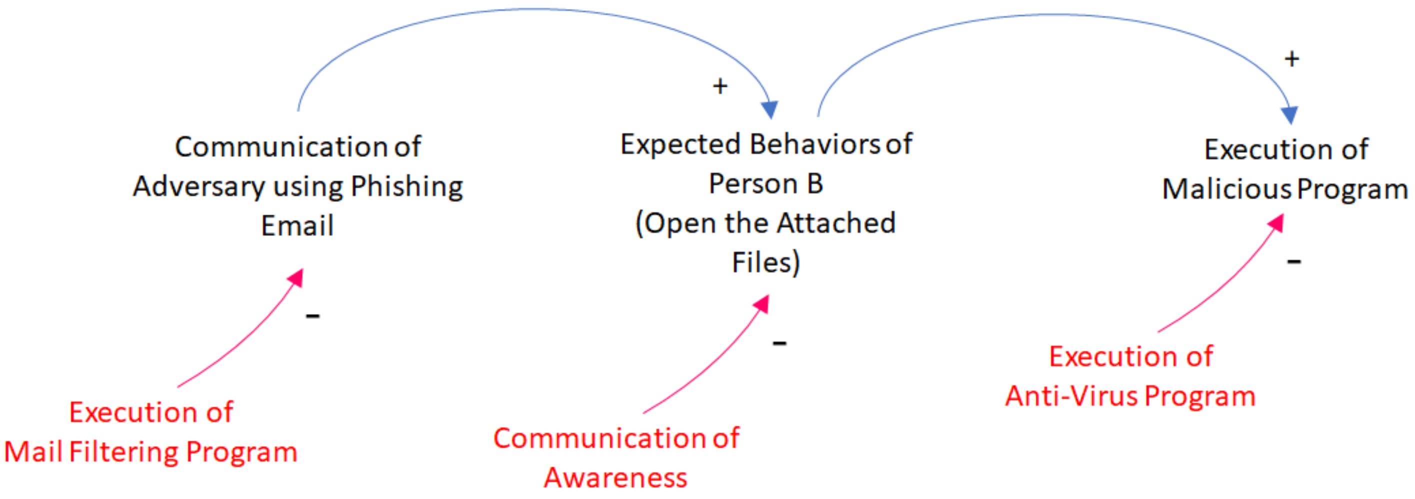

+
+
Communication of Adversary using Phishing Email
Expected Behaviors of Person B (Open the Attached Files)
Execution of Malicious Program

_6.3 Cyber Risk Treatment

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

Mail filtering program reduces number of phishing emails that users receive. An increase of users' awareness about suspicious emails by communication reduces their mishandling of suspicious emails. Anti-virus program identifies malicious programs.

They reduce the likelihood that the first round of initiating event occurs in attack propagation.


Communication of Adversary using Phishing Email
+
Expected Behaviors of Person B (Open the Attached Files)
+
Execution of Malicious Program
-
Execution of Mail Filtering Program
-
Communication of Awareness
-
Execution of Anti-Virus Program

_6.4 Consideration

Cyber Risk Treatment

Visualization of interrelationships in the example of the structure identified using systems thinking for attack vector provided useful information to reduce likelihood that the first round of initiating event occurred in attack propagation.