Vol.2020-DPS-182 No.3
Vol.2020-CSEC-88 No.3
2020/3/12

Consideration of Extreme Risks in Cyberspace using Systems Thinking

MASATO KIKUCHI[1] TAKAO OKUBO[1]

Abstract: Although the conventional risk management approach successfully analyzes the risks where the factors affecting the risks and their effect upon 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 upon level of the risks by cascading. Without considering real causes of these patterns of change, there are some possibilities that efficient controls may not be implemented. This paper promotes an understanding of the way interrelationships in cyberspace generate exponential growth of risks and proposes a desirable approach that organizations analyze this phenomenon and get useful information to find how it might be influenced.

Keywords: Cyberspace, Cybersecurity, Systems Thinking

1. Introduction

It is a tedious task to identify security risks in cyberspace and treat them because cyberspace is a complex system and the scope is very broad. Appazov [1] identifies anonymous, asymmetry and global reach as the key challenging features of cyberspace. The issues for cyberspace have global effects.

This paper promotes an understanding of the way interrelationships in cyberspace generate exponential growth of risks and proposes a desirable approach that organizations analyze this phenomenon (extreme risk analysis) and get useful information to find how it might be influenced (extreme risk response). First, researches on cyberspace, threats in cyberspace, how extreme events occur are reviewed from the point of view of extreme risk analysis and then researches on resilience are reviewed from the point of view of extreme risk response. Second, resilience for cyberspace is discussed. Third, the model that explains the patterns of threats are developed using a systems thinking approach. Using this model, the tiny initiating events and how they scale up into extreme cybersecurity incidents are identified. Based on those knowledge, suitable mitigations are predicted.

Based on the model developed, the burden in identifying security risks and their mitigations in cyberspace is reduced because it is possible to focus on most likely vulnerabilities and driving forces behind extreme cybersecurity incidents without the need to take into account all elements surrounding the risks.

2. Previous Research

2.1 Introduction

Previous researches on cyberspace and threats for cyberspace are reviewed. Then previous researches on how extreme events occur are also reviewed with an emphasis on complexity science because they will help to explain how extreme events occur. Finally, previous researches on resilience are reviewed because they will help to explain how extreme events are influenced.

2.2 Cyberspace

Clark [2] defines 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. (Physical Layer: E.g. PCs, Servers and Routers)
  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.

According to Clark [2], it is not the computer that creates the phenomenon we call cyberspace. It is the interconnection that makes cyberspace—an interconnection that affects all the layers in cyberspace.

Kramer, Starr and Wentz [3] introduce 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.

2.3 Threats for cyberspace

Meyers et al. [4] construct taxonomies of cyber adversaries and methods of attack, drawing from a survey of the literature in the area of cyber crime.

Hansman et al. [5] focus on the provisioning of a method for the analysis and categorization of both computer and network attacks,

1 Institute of Information Security, Yokohama, Kanagawa 221-0835, Japan

thus providing assistance in combating new attacks, improving computer and network security as well as providing consistency in language when describing attacks. Network attacks focus on attacking a network or the users on the network by manipulating network protocols, ranging from the data-link layer to the application layer. Computer attacks do not focus on manipulation of network protocols. 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. 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.

Richberg [6] proposes a common approach to threat framework that categorizes threat activity and supports missions ranging from strategic decision-making to analysis and cybersecurity measures and users from generalists to technical experts.

Hutchins et al. [7] propose a cyber kill chain model to describe phases of intrusions, mapping adversary kill chain indicators to defender courses of action, identifying patterns that link individual intrusions into broader campaigns, and understanding the iterative nature of intelligence gathering form the basis of intelligence-driven computer network defense (CND).

2.4 How extreme events occur

Perrow [8] observes that disasters are more likely to occur when the tiny initiating events are ‘tightly coupled’, with complex interactions leading to a ‘significant degree of incomprehensibility’.

McKelveya and Andriani [9] drew on ’scale-free theories’ from complexity science that explain how tiny initiating events scale up into extreme positive or negative outcomes. 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.

Olagbemiro [10] observes that positive feedback influences the interactions between the dimensions in a cyber ecosystem by building on previous actions with a resulting effect being that uninhibited positive feedback can lead to exponential rates of growth in output and a cyber ecosystem “exploding” into chaotic behavior.

Leveson [11] refers to event-based accident models that explain accidents in terms of multiple events sequenced as a chain over time. He argues that event-based models encourage limited notions of causality—usually linear causality relationships are emphasized—and it is difficult to incorporate non-linear relationships, including feedback.

Cavelty [12] argues that the failures will rapidly escalate beyond control before anyone understands what is happening and is able to intervene if the system is tightly coupled.

2.5 Resilience

The US National Academy of Sciences (NAS) [13] defines disaster resilience as “the ability to plan and prepare for, absorb, recover from, and adapt to adverse events”.

The Organization for Economic Development (OECD) [14] defines resilience as “the ability of individuals, communities and states and their institutions to absorb and recover from shocks, whilst positively adapting and transforming their structures and means for living in the face of long-term changes and uncertainty,”.

IRGC [15] categorize the risks associated with cyberspace as system risks. System risks are highly interconnected risks with complex causal structures and non-linear cause-effect relationships and different from conventional risks with linear or well-established cause-and-effect-relationships. Increasing the overall resilience of an organization can be a way to better deal with the shocks and stresses arising from systemic risks. They also argue that interconnectivity between systems is one of the determining features of our modern world and can increase system efficiency although it can reduce resilience to shocks if it does not include buffer capacity and if the connections between the nodes are too tight.’.

Björck et al. [16] define cyber resilience as “the ability to continuously deliver the intended outcome despite adverse cyber events”, and make use of five aspects; objective, intention, approach, architecture and scope to contrast cyber resilience with cybersecurity. They argue that the business and IT systems need to be viewed as an interconnected network, rather than as a single unit of analysis with an environment to manage resilience.

Engle [17] refers to adaptive capacity that is often described as ‘adaptability’ in resilience studies and means the ability of a system to prepare for stresses and changes in advance or adjust and respond to the effects caused by the stresses.

2.6 Summary

These previous researches identify below:

- Cyberspace is more than computers and digital information. It is the interconnection that makes cyberspace.
- The concept of dimensions that are a way of allowing for a classification of a cyber-attack is used 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.
- Nonlinear outcomes result when a tiny initiating event gets amplified – for example, by reinforcing feedback – to generate an extreme effect extending across multiple levels.
- Disasters are more likely to occur when the tiny initiating events are ‘tightly coupled’, with complex interactions leading to a ‘significant degree of incomprehensibility’.
- Reinforcing feedback influences the interactions between the dimensions in a cyber ecosystem and can lead to exponential rates of growth in output and a cyber ecosystem “exploding” into chaotic behavior.
- Increasing the overall resilience of an organization can be a way to better deal with the shocks and stresses arising from systemic risks such as the risks associated with cyberspace.

There is a lack of propagation dimension and form of

visualization for a classification of a cyber-attack.

This paper proposes below for extreme risk analysis and response:

- Application of resilience to deal with extreme risks in cyberspace with a focus on adaptive capacity
- Addition of propagation dimension to view extreme risks in cyberspace
- Application of systems thinking to propagation dimension where tiny initiating events get amplified by reinforcing feedback to generate an extreme effect on cyberspace
- Visualization of interrelationships among the factors affecting the extreme risks in cyberspace

3. Resilience for Cyberspace

3.1 Concepts

Cyberspace includes a dynamic network of interactions, where feedback loops between various elements and their cascading effects can trigger cyberspace-wide disruptions or changes. Under some conditions, small interactions or disruptions to small elements can generate substantial systemic changes across cyberspace.

Cyberspace needs to have an adaptive capacity that keep it from crossing critical thresholds that can be tipping points before disruptions. This adaptive capacity is created by having buffer capacity and reducing a number of vulnerable relationships or negative reinforcing feedback loops between elements. Resilience refers to the ability of system to create this adaptive capacity as well as the ability of a system to absorb and recover from disruptions.

The adaptive and multi-actor nature of cyberspace makes it inherently difficult to model or analyze via simple linear cause and effect models and traditional risk management practices are not sufficient for dealing with the risks associated with cyberspace. Increasing the overall resilience of cyberspace enhances the capacity to recover quickly and reduce the severity of the impact of cyber-attacks.

3.2 Implementation

Scenarios inform decision-making at multiple levels in cyberspace about how to create adaptive capacity. Development of scenarios identifies the multiple events that disrupt cyberspace and organizations relying on it. These events tend to have complex causal structures and non-linear cause-effect relationships. Diversity of perspectives raised by collaboration of many different stakeholders identifies those events better.

For extreme risk analysis, the scenario-based reviews allow stakeholders to review how specific cyber-attacks perform across a variety of situational conditions and can identify weak points that could trigger a negative reinforcing feedback loop in cyberspace and important thresholds that can be tipping points before disruptions. Because a multitude of interconnections may be involved in negative reinforcing feedback loop, it is difficult to accurately predict the consequence of such disruptions. Scenarios are not necessarily quantitative.

For extreme risk response, the scenarios then, help to identify leverage points where changes to one part of cyberspace can percolate across other connected nodes – inherently using the interconnectivity of cyberspace to generate positive cascading changes to resolve the weak points in cyberspace.

Systems thinking helps to identify the interconnections and feedback loops within cyberspace and how disruptions to one place in cyberspace can have indirect yet significant consequences upon elsewhere.

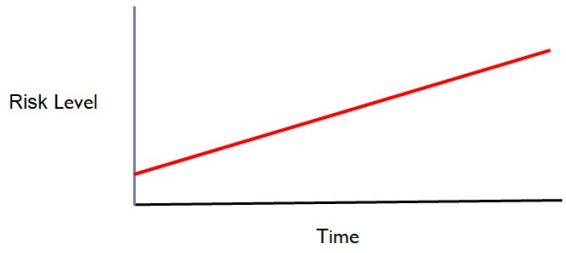
4. Modelling

4.1 Objectives

This paper develops a primitive model to explain the scenario on how extreme cybersecurity incidents occur from a specific threat using a system thinking approach. This model may be used to develop a series of models for particular patterns of cyber-attacks that are selected from the established taxonomies of cyber adversaries and attacks. An example of incident is a targeted attack through emails. The models offer a clue as to how they can be prevented from occurring. These models are called “Power of Cyberspace Model” (POCM). These models are useful for the people who are dealing with specific threats for the cyberspace to find out general ideas on how they should be treated.

4.2 Requirements

Conventional risk management approaches tend to see that the factors affecting the risks and their effect upon level of the risks are close in time and space and their relationship can be drawn with a straight line (linear relationship) because the factors affecting the risks produce a constant proportion (Linear Behavior) as shown in Figure 1. 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.



(on assumption that original factors affecting risks grow at a constant rate)

Figure 1 Linear Behavior of Risk Level.

In reality, the factors affecting the risks and their effect upon level of the risks may not be close in time and space and their relationship may be drawn with curves (non-linear relationship) because the factors affecting the risks may not produce a constant proportion. There are possibilities that the causes emerge years before and small causes generate large scale effects with a transformation on a scale completely different from their own.

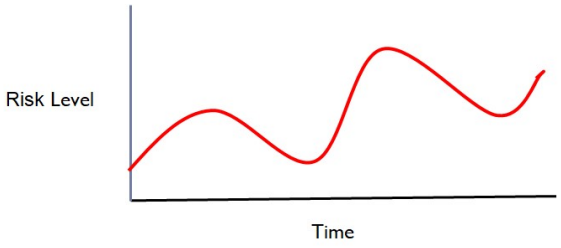
Examples that the factors affecting risks and their effect upon level of the risks in cyberspace are not close in time and space (dynamic complexity) are [18]:

- Same factor has different effect upon level of the risks in

the short-term and the long-term (Oscillation Behavior as shown in Figure 2)

- Small factor can grow into large effect upon level of the risks by cascading effects (Exponential Growth Behavior as shown in Figure 3)

The model needs to be able to describe extreme risks in a rich language with a focus on a non-linear relationship and patterns of change that helps us see the structure underlying extreme risks and find the leverage.



(on the assumption that original factors affecting risks grow at a constant rate)

Figure 2 Oscillation Behavior of Risk Level.

(on the assumption that original factors affecting risks grow at a constant rate)

Figure 3 Exponential Behavior of Risk Level.

4.3 Methodologies

System thinking approach can visualize dynamic relationships among entities and is suitable for modeling how one entity influences other entities' behaviors in the course of cyber-attacks that lead to extreme risks.

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: [19].

- to identify the real causes of issues (extreme risk analysis).
- to know just where to work to address them (extreme risk response).

Systems thinking can describe extreme risks in a rich language with a focus on a vast array of interrelationships and patterns of change that helps us see the structure underlying extreme risks and find the leverage. Structure is concerned with the key interrelationships that influence behavior over time and addresses the underlying causes of behavior at a level at which patterns of behavior can be changed [18]. View of systems thinking about how the extreme risks in cyberspace are influenced is shown in Figure 4.

Feedback loop diagram shows how the change of one element A have an impact on another element B, and then on the original element A as shown in Figure 5. Plus sign indicates that the element A and the element B change in the same direction.

Reinforcing feedback loop amplifies whatever movement occurs, producing more movement in the same direction. Reinforcing feedback loop normally generates exponential growth behavior. Balancing feedback loop is always operating to reduce a gap between what is desired and what exists. Balancing feedback loop with delay normally generates oscillation behavior.

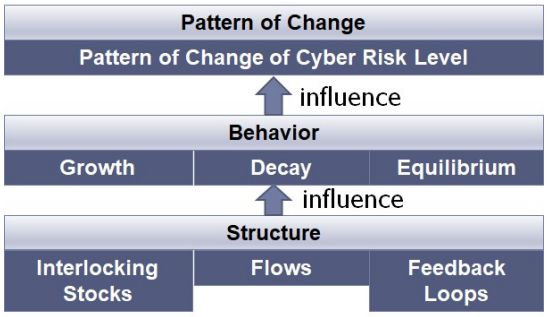


Figure 4 View of Systems Thinking about Cyber Risk.

Figure 5 Feedback Loop.

4.4 Concepts

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

The POCM sees interrelationships and delays among the factors affecting the extreme risks and their effect upon level of the extreme risks over time to gain insight into the leverage. Specifically, the POCM analyzes extreme risks considering:

- How the factors can reinforce through interrelationships such as feedback loop
- How the structure creates a particular pattern of behavior

and respond to extreme risks with useful information that can be used to determine how that pattern might be influenced (leverage).

For example, the POCM 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 interrelationships (extreme risk analysis) to gain insight into the leverage (extreme risk response). It is assumed that interrelationships exist among events that influence each other to generate an extreme event on cyberspace.

4.5 Contributions

Using the POCM, organizations can analyze the way the structure creates extreme incidents on cyberspace (extreme risk analysis) and get useful information to find how that pattern might be influenced (extreme risk response).

The POCM helps management to:

- identify the real causes of an extreme effect on risk level. (extreme risk analysis)
- get useful information to determine where to work to address them (extreme risk response)

This view of the POCM is shown in Figure 6.

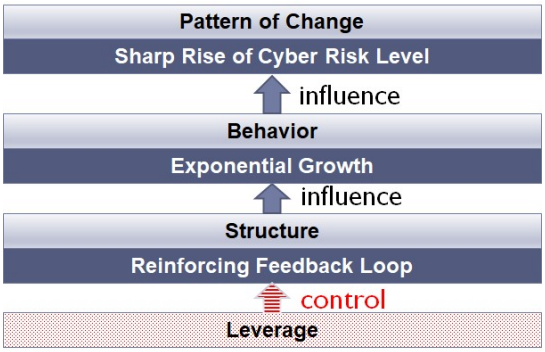


Figure 6 View of the POCM about Cyber Risk.

4.6 Extreme Risk Analysis

In cyberspace, a tiny initiating event may be an execution of malicious program on a single computer connected to cyberspace and then it could generate an extreme effect across cyberspace by reinforcing feedback as shown in Figure 7.

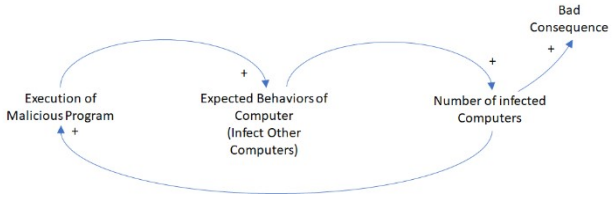


Figure 7 Example on effects of reinforcing feedback on an extreme event.

This issue of event-based models that cannot incorporate non-liner relationships is resolved by the model as shown in Figure 7. Reinforcing feedback shows non-linear outcomes of increasing number of infected computers because the infected computers infect more computers connected to cyberspace. Reinforcing feedback normally generates an exponential growth behavior.

One of the typical triggers of this reinforcing feedback could be communication conducted by an adversary using a phishing email as shown in Figure 8. It does not have any feedback so that it may generate a linear behavior.

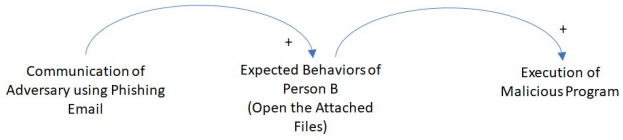


Figure 8 Example on a trigger of reinforcing feedback.

Executions of malicious program on a single computer as tiny initiating events are tightly coupled with interaction of various agents on cyberspace because cyberspace facilitates various communication means by removing the barrier of time and physical space. Interaction with adversaries is achieved through communication conducted by phishing emails. Interaction with other computers is achieved through network protocols and leads to extreme cybersecurity incidents

4.7 Extreme Risk Response

Visualization of interrelationships in the structure provides useful information to find the leverage. The following leverages are imagined from the POCM.

An increase of users' awareness about suspicious emails by communication reduces their mishandling of suspicious emails. As a result, it reduces number of malicious programs executed as shown in Figure 9.

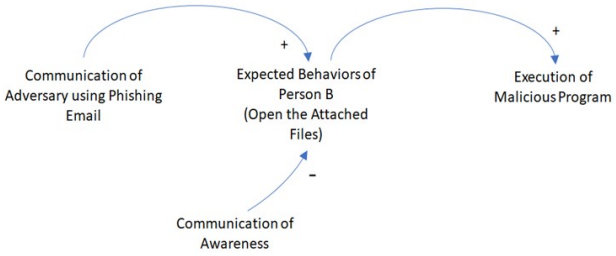


Figure 9 Leverage in the Example of POCM (Attack Vector).

Mail filtering program reduces number of phishing emails that users receive and then number of malicious programs executed by their bad behaviors as shown in Figure 10.

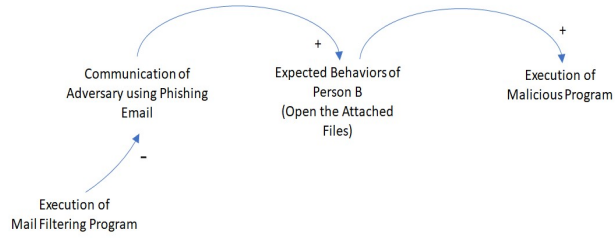


Figure 10 Leverage in the Example of POCM (Attack Vector).

Anti-virus program identifies malicious programs and reduces number of malicious programs executed by users' bad behaviors as shown in Figure 11.

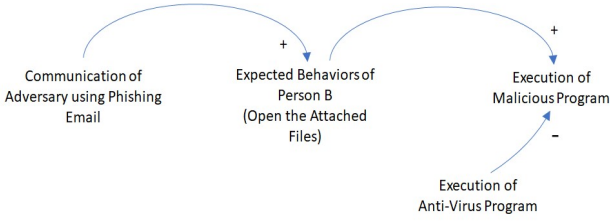


Figure 11 Leverage in the Example of POCM (Attack Vector).

Anti-virus program also prevents the small events from scaling up into extreme incidents by reducing number of infected computers if it also propagates through all computers connected to cyberspace. It weakens the reinforcing feedback loop as shown in Figure 12.

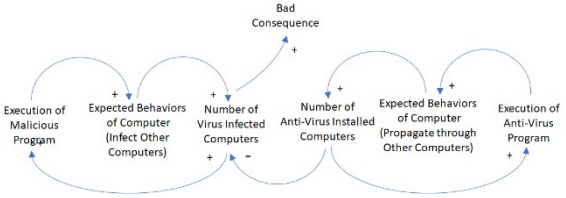


Figure 12 Leverage in the Example of POCM (Propagation).

Through the visualization on how a small event generates an extreme effect across cyberspace by reinforcing feedback loop, the organizations get useful information to find the high leverage that is a change which — with a minimum of effort — would lead to significant improvement, to prevent extreme risk from materializing.

The organizations may use POCM to apply the structure of the one of the selected patterns of a cyber-attack to visualize a reinforcing feedback loop underlying the expected cyber-attack and select the most efficient controls to moderate it. Mapping between particular pattens of a cyber-attack and specific controls is out of the scope of POCM.

5. Conclusion

The model developed in this paper successfully showed driving forces behind extreme cybersecurity incidents (extreme risk analysis). The driving forces included interrelationships among entities connected to cyberspace and the way in which tiny initiating events such as an execution of malicious program on a single computer scale up into extreme cybersecurity incidents by an effect of reinforcing feedback. The model also made this phenomenon clearly understandable for the people who are dealing with threats for the cyberspace using system thinking approach that visualized dynamic relationships among entities.

The model could provide useful information to find how extreme cybersecurity incidents might be controlled (extreme risk response). For example, anti-virus program can prevent the initiating events such as an execution of malicious program on a single computer from occurring. At the same time, it can also prevent the initiating events from scaling up into extreme incidents by weakening reinforcing feedback if it can use the interconnectivity of cyberspace to generate cascading changes to resolve the amplification of the events.

6. Future Work

There are a lot of vulnerabilities in cyberspace and various methods of attacking cyberspace. Because the primitive model developed in this paper considered only limited number of vulnerabilities and methods of attacking cyberspace, in the future research, a series of models for particular patterns of cyber-attacks that are selected from the established taxonomies of cyber adversaries and attacks will be developed based on this model.

These models will be simulated with actual cyber-attack cases and then how the consequences of these cases will be controlled by the mitigations predicted from them will be verified.

Reference

[1] Appazov, A. Legal Aspects of Cybersecurity, University Copenhage, 2014.
[2] Clark, D. Characterizing Cyberspace: Past, Present and Future, MIT CSAIL, 2010.
[3] Kramer, F. Starr, S. and Wentz, L. Cyberpower and National Security, National Defense University Press, 2009.
[4] Meyers, C A. Powers, S S. Faissol, D M. Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches. Lawrence Livermore National Lab, 2009.
[5] Hansman, S. Hunt, R. A taxonomy of network and computer attacks, Elsevier, Computer and Security, 2005, vol. 24, 1, 31–43p.
[6] Richberg, J. A Common Cyber Threat Framework, National Intelligence Manager for Cyber National Security Partnerships, 2018.
[7] Hutchins, E. Cloppert, M. Rohan, A. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains, Lockheed Martin Corporation, 2018.
[8] Perrow, C. Normal Accidents, Living with High Risk Technologies, New York: Basic Books, 1999, 68–73p.
[9] McKelveya, B. and Andriani, P. Avoiding extreme risk before it occurs: A complexity science approach to incubation. Macmillan Publishers, Risk Management, 2010, vol. 12, 1, 54–82p.
[10] Olagbemiro, A. Cyberspace as a Complex Adaptive System and the Policy and Operational Implications for Cyber Warfare, Defense Technical Information Center, 2014.
[11] Leveson, N. A New Accident Model for Engineering Safer Systems, Safery Science, 2004, vol. 42, 4, 237–270p.
[12] Cavelty, M. A Systemic cyber/in/security – From risk to uncertainty management in the digital realm, Swiss Re Risk Dialogue Magazine, 2011.
[13] A National Academy of Sciences (NAS). Disaster Resilience: A National Imperative, The National Academies Press, 2012.
[14] OECD. Guidelines for resilience systems analysis, OECD Publishing, 2014.
[15] International Risk Governance Center (IRGC). Guidelines for the Governance of Systemic Risks, 2018.
[16] Björck, F. Henkel, M. Stirna, J. Zdravkovic, J. Cyber Resilience – Fundamentals for a Definition, Springer, Advances in Intelligent Systems and Computing, 2015, vol. 353.
[17] Engle, N. Adaptive capacity and its assessment, Global Environmental Change, 2011, vol. 21, 2, 647-656p.
[18] Senge, P. The Fifth Discipline, Crown Business, 1990.
[19] McNamara, C. Field Guide to Consulting and Organizational Development, Paperback, 2006.