Building Cyber Resilience through Polycentric Governance

Masato Kikuchi and Takao Okubo
Institute of Information Security, Yokohama 221-0835, Japan
Email: dgs188101@iisec.ac.jp; okubo@iisec.ac.jp

Abstract—While interconnectivity within cyberspace increases efficiency, it reduces resilience to cyber-attacks. Cyberspace is an artificial environment without borders and free from state control and creating a predominant central authority for the protection of cyberspace is not realistic. This paper proposes an efficient way to build resilience of cyberspace through polycentric governance as an ideal way of absorbing an impact of cyber-attacks. This paper has identified critical factors of polycentric governance and then proposed how these factors should be applied to build resilience of cyberspace.

Index Terms—Polycentric governance, cyberspace, resilience, system thinking

I. Introduction

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. Creating a predominant central authority that has exclusive control of protecting cyberspace is not realistic because cyberspace is an artificial environment without borders and free from state control. Accountability structures need to be reframed, involving all relevant stakeholders.

This paper proposes an efficient way to build resilience of cyberspace through polycentric governance as an ideal way of absorbing an impact of cyber-attacks. First, researches on cyberspace, polycentric governance, resilience and application of polycentric governance to cyberspace are reviewed. Second, the reasons why increasing resilience is important for cyberspace are explained. Third, suitability of polycentric governance for resilience of cyberspace is examined. Fourth, the factors of polycentric governance that are critical for building resilience of cyberspace are identified and then how to apply them is proposed. Fifth, more detailed approach on how polycentric governance made up of these factors contributes to building resilience of cyberspace is explained.

II. Previous Research

This section reviews previous researches on cyberspace, polycentric governance, resilience and application of polycentric governance to cyberspace.

Manuscript received October 12, 2019; revised March 31, 2020.
Corresponding author email: dgs188101@iisec.ac.jp.
doi:10.12720/jcm.15.5.390-397

A. Cyberspace

Choucry [1] defines cyberspace as a venue that allows users to engage in activities conducted over electronic fields whose spatial domains transcend traditional territorial, governmental, social, and economic constraints. According to her, William Gibson is generally regarded as providing the first formal designation for the new arena of interaction we now know as 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 (e.g., actors, entities, and users)
- The information that is stored, transmitted, and transformed in cyberspace (e.g., information makes up interactions)
- The logical building blocks that make up the services and support the platform nature of cyberspace (e.g., ‘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 (e.g., PCs, 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.

Appazov [3] identifies anonymous, asymmetry and global reach as the key challenging features of cyberspace from a legal point of view. Kikuchi and Okubo [4] identifies the following characteristics of cyberspace:

- Anonymous - the identity of an actor in cyberspace is concealed or disguised.
- Asymmetry - an action in cyberspace has an impact disproportionate to their size.
- Borderless - an action in cyberspace is literally borderless and unbounded by such notions as jurisdiction or sovereignly.
- Instantaneity - an action in cyberspace has an impact near-instantaneously around the world.

- Free Entry and Free Exit - anyone can freely enter and leave cyberspace.
- Interactive - interactive actions create knowledge and power.

B. Resilience

The US National Academy of Sciences (NAS) [5] 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) [6] 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 [7] argues 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*. [8] 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 [9] 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.

C. Polycentric Governance

According to Carlisle and Gruby [10], polycentric is a fundamental concept in the work of Vincent and Elinor Ostrom and connotes a complex form of governance with multiple centers of decision making, each of which operates with some degree of autonomy.

According to Feldman [11], polycentric governance has a number of characteristics including ad hoc institutional arrangements that permit bottom-up, multiple-actor governance; cooperative use of physical and virtual knowledge space; and facilitating collaboration within locally accessible institutional frameworks that are flexible enough to adapt to new opportunities and challenges.

According to Morrison *et al*. [12], polycentrism is a nonhierarchical set of interactions between public and private actors operating at multiple levels without a predominant central authority and a polycentric system is made up of many autonomous units that are formally independent of one another but which choose to act in ways that take account of others through self-organized processes of cooperation and conflict resolution. Morrison *et al*. [12] summarize characteristics of polycentric governance systems as below:

- Many autonomous units formally independent of one another
- Multiple overlapping scales
- Units choose to act in ways that take account of others (though mutual adjustment)
- Self-organized processes of cooperation and conflict resolution
- System-like behavior

Morrison *et al*. [12] summarize the advantages of polycentric systems as solutions of complex problems as below:

- They are capable of considering multiple environmental, social, or economic conditions.
- Because the potential pathways to solutions of complex problems are ill-defined, they can provide an environment in which different actors can experiment with their preferred strategy of adapting to variability and change of complex problems.
- They permit tailoring of adaptation activities to suit local-regional circumstances and community preferences.
- They allow for specialization and the division of tasks between central, regional, and local levels, thus improving the efficiency of adaptation activities by matching the governance level to the geographic scale of the problem.
- They are flexible in their ability to configure and reconfigure alliances rapidly in order to achieve specific goals, which in turn makes them inherently adaptive.
- They are regarded as being more robust to external stresses and shocks because they can recover more quickly due to their diversity. Their high degree of overlap and redundancy also makes them less vulnerable: if one element fails, others may take over their functions.
- The high levels of uncertainty about the set of solutions, and the lack of definitive answer as to who is responsible for the solution mean that a more monocentric approach is impossible, making polycentricity, in this sense, 'a fact of life.

Morrison *et al*. [12] summarize the disadvantages of polycentric systems as below:

- If different levels of governance opt for conflicting policies, the result can be leakages, meaningless certification, policy incoherence, unnecessary duplication of efforts, counterproductive actions, and/or complete grid-lock.
- Competition between levels and/or responsibilities spilling over from one level into another can lead to suboptimal standards for mitigation and adaptation.
- The costs in time and money of collective action (consultation, reaching agreement, and enforcing such agreements) are high due to the 'complexity of spatial patterning, multiple functional overlays, partial polity formation, and variable system coupling.'

- Collaborative processes and organizations may prioritize goal achievement over democratic procedure, circumventing the 'troublesome' and 'time-consuming' procedures designed to ensure accountability and transparency at lower levels.
- They are believed to suffer from a tendency for inertia and paralysis, especially when efforts to preserve the system's own existence or permanence overtake attempts at implementation.
- They are very vulnerable to internal structural and procedural issues, broader economic factors, and shifts in political sentiment.

Colander and Kupers [13] argue that the success of bottom-up policy depends on the ecostructure within which people operate and the normative codes that they follow. Instead of imposing norms, or even forcing individual actors to self-regulate, it is recommended to develop an ecostructure that encourages self-reliance, and concern about others.

D. Application of Polycentric Governance to Cyberspace

Shackelford [14] argues the atmosphere and cyberspace share similar problems of overuse, difficulties of enforcement, and the associated challenges of collective inaction and free riders although they are distinct extraterritorial arenas. Then he states that an effective system of polycentric governance for cyberspace would use a mixture of laws and norms; market-based incentives; code; self-regulation; public-private partnerships; and bilateral, regional, and multilateral collaboration to enhance cybersecurity.

Eggenschwiler [15] argues that given the polycentric nature of cyberspace governance, one-dimensional, sovereigntist conceptions of accountability that intend to attach ultimate responsibility to a unitary source of authority are misplaced and accountability structures need to be consciously reframed, involving all relevant stakeholders.

Those researches indicate that there are compatibilities between characteristics of cyberspace and polycentric governance.

III. Importance of Resilience for Cyberspace

IRGC [7] categorizes the cyber risks as system risks. System risks are different from conventional risks with linear or well-established cause-and-effect-relationships such as information security risk. System risks are highly interconnected risks with complex causal structures and non-linear cause-effect relationships.

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 cascading 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. Therefore, traditional risk management practices are not sufficient for dealing with the cyber risks. Increasing the overall resilience of cyberspace enhances the capacity to recover quickly and reduce the severity of the impact of cyber-attacks.

IV. Suitability of Polycentric Governance for Cyber Resilience

This section examines suitability of polycentric governance for resilience of cyberspace by comparing dilemmas posed by environmental variability and change with dilemmas derived from the characteristics of cyberspace.

Morrison *et al.* [12] argue that environmental variability and change are characterized by cross-scale (spatial and temporal) linkages and feedbacks that generate nonlinear dynamics and uncertainty. They indicate the transformative potential of polycentric governance has been widely advocated in such situations. Examples of dilemmas posed by the Nature of Climate Variability and Change are discussed by Morrison et al. [12] as below:

- Temporal scale - trade-offs exist between protection of what exists now (infrastructure, economies, and values) and long-term adaptation. This temporal dimension leads to moral hazard-short-term actions and interventions that compromise, limit, or trade-off actions in the future (e.g., maladaptation).
- Spatial scale - adaptation actions in one place may have negative impacts elsewhere - either immediately downstream or in more remote places (e.g., teleconnections).
- Transboundary issues - parts of the environment have shared jurisdiction or where natural resources cross boundaries - such as the global atmosphere, oceans, various water bodies, and migratory species (e.g., fish stocks).
- Social-ecological interactions-environmental variability inevitably interacts with complex social dynamics, such as place, identity, and human mobility.
- Nonlinear dynamics-social-ecological systems exhibit nonlinear or threshold responses to changes in climate variability.
- Cross-scale feedbacks-complex interactions at different spatial or temporal scales generate thresholds and alternate stable states.

- Institutional fit - the scale of governance must be capable of responding to the scale of the policy problem.

These dilemmas posed by the Nature of Climate Variability and Change have in common with the dilemmas derived from the characteristics of cyberspace as below:

- Temporal scale - each actor benefits individually in short-term by taking the free rider position and letting others to reduce cyber risks. On the other hand, vulnerabilities untreated by an actor may trigger unexpected large-scale attack to cyberspace in long-term.
- Spatial scale - as instantaneity characteristic of cyberspace, an action in cyberspace has an impact near-instantaneously around the world.
- Transboundary issues - as borderless characteristic of cyberspace, an action in cyberspace is literally borderless and unbounded by such notions as jurisdiction or sovereignly.
- Social-ecological interactions-various activities relying on cyberspace inevitably interacts with complex social dynamics, such as place, identity, and human mobility.
- Nonlinear dynamics - as asymmetry characteristic of cyberspace, an action in cyberspace has an impact disproportionate to their size.
- Cross-scale feedbacks-complex interactions at different spatial or temporal scales in cyberspace generate thresholds and alternate stable states.
- Institutional fit - the scale of governance must be capable of responding to the scale of the problem of cyberspace.

Both dilemmas are very similar and polycentric governance is suitable for the situations facing both dilemmas.

Polycentric governance increases resilience of cyberspace because of its diversity characterized by broader levels of participation and collaboration, and its environmental adaptability.

V. Critical Factors of Polycentric Governance for Cyber Resilience

Through the review of previous related researches and following examination of importance of resilience and polycentric governance for cyberspace, this paper identifies three factors of polycentric governance that are critical for building resilience of cyberspace: ecostructure, collaboration, and accountabilities.

Ecostructure provides the decentralized and bottom-up environment where collaboration takes place. Comparison between centralized and decentralized environments is shown in Fig. 1. Controls (bigger circles) are distributed in the decentralized environment although they are centralized in the centralized environment.

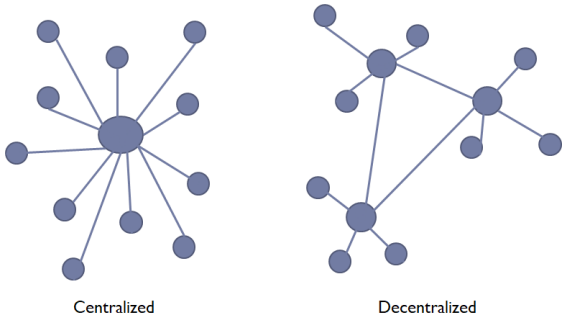

Fig. 1. Comparison between centralized and decentralized environments

Collaboration through public-private multi-stakeholder partnerships plans and prepares for, absorb, recover from, and adapt to cyber-attacks. Accountabilities streamline collective accountability structures and clarify stakeholder-related roles, goals, and expectations that help to ensure their longer-term commitment to collaboration. In this way, three factors implement polycentric governance.

This section proposes how these factors should be applied to build resilience of cyberspace through polycentric governance.

The next section explains more details on how polycentric governance made up of these factors contributes to building resilience of cyberspace.

A. Ecostructure

Meta-policy should be designed to create an ecostructure in which stakeholders can deal with continually evolving cyber risks on their own from the bottom up without relying on a central coordinator and smooth the transition of cyberspace into an ordered state without the use of a central coordinator.

IRGC [7] argues that such management is undertaken from multiple centers of authority, with trust and effective communication between stakeholders and the capacity to develop and use measures of anticipating risks

Carlisle and Gruby [10] provide the following recommendations in the regard of ecostructure:

- Multiple, overlapping decision-making centers with some degree of autonomy
- Choosing to act in ways that take account of others through processes of cooperation, competition, conflict, and conflict resolution

Shackelford [14] provides the following recommendations in the regard of ecostructure:

- Instead of the creation of a centralized artificial organization, local institutions relying to the extent possible on organic self-organization should be created to promote trust and bottom-up governance with active oversight at multiple scales and from diverse stakeholders. These institutions are open to admit the participation of all stakeholders who may be affected by cyber-attacks and allow them to make and modify the rules of cyberspace.

- Regulation at various levels and through various modalities, including laws, norms, markets, code, self-regulation, and multilateral collaboration.

B. Accountabilities

The followings are recommended to ensure accountabilities in polycentric governance for cyberspace.

- Stakeholder's discussions of accountability that are organized around specific, manageable issue areas to identify corresponding responsibilities and streamline collective accountability structures
- Creation of independent oversight mechanisms and review authorities, and clear standards that provide useful instruments in the regard of resilience of cyberspace
- Mission statements, mandates and clarity about stakeholder-related roles, goals, and expectations that help to ensure their longer-term commitment and guidance

Eggenschwiler [15] argues that accountability structures are contested by the specific elements of cyberspace governance and these elements are the heterogeneity of stakeholders, the profusion of issue areas, as well as the malleability of institutional arrangements. His explanation of these challenges and recommendations from the point of view of polycentric governance are as follows.

Heterogeneity of stakeholders refers to a condition of accountability obfuscation caused by a great number of actors engaged in concurring regulatory ventures. First his recommendation includes the enlistment of stakeholders essential to the resolution of specific governance problems as a first step with regard to streamlining collective accountability structures and identifying corresponding responsibilities. Second his recommendation includes independent, constitutionally inspired oversight mechanisms, such as ombudsmen or multistakeholder-versed third-party supervisory and review authorities, and clear standards that provide useful instruments in the regard of accountability enforcement.

Profusion of issue area spans across technical, socio-political. and economic spheres. In the context of cyberspace governance, the excess and coming together of technical and non-technical issue areas can severely complicate accountability structures. His recommendation includes discussions of accountability that are organized around specific, manageable issue areas, and include stakeholders from different backgrounds, which are capable of flagging areas of intersection and convergence.

Malleability of institutional arrangements refers to a condition of accountability structures suffered from the dispersion of topics across different organizational settings. His recommendation includes well-defined mission statements and mandates that help to create longer-term commitment and guidance, and reduce the risk of ad-hocism and agenda shifting brought about by changing stakeholder configurations.

C. Collaboration

Platform for public-private multi-stakeholder partnerships should be designed to plan and prepare for, absorb, recover from, and adapt to cyber-attacks.

IRGC [7] argues that addressing the risks driven by a web of complex interaction effects between various actors may require collaboration between public and private actors to overcome common obstacles because a disruption in one area can have percolation effects that disrupt others. Because cyberspace is borderless and an action in cyberspace has an impact near-instantaneously around the world, collaboration between public and private actors is important to overcome cascading effects of cyber-attacks.

IRGC [7] also argues that multi-stakeholder partnerships will inherently require some elements of value-chain analysis to transparently assess the role of each participant in the creation and use of a product or service. This could serve to provide incentives to those actors who contribute to reducing risks by adding diversity, modularity or other components of resilience, in such a way that the supply chain can be more adaptive and able to re-organise if needed. Cyberspace accelerates extension of value-chain across multiple organizations around the world and multi-stakeholder partnerships help to build resilience of such an extended value-chain through their collaborative analysis.

According to IRGC [7], diversity of perspectives raised by the many different actors in a decision-making group address uncertainty better.

Feldman [11] provides the following recommendations in the regard of collaboration:

- Platform for public-private partnerships and better incorporation of social science expertise to build public trust and confidence
- Public participation infrastructure needs: 1) support for stakeholder dialogue, 2) sound design for public engagement processes, 3) support for a wide range of participatory tools
- Small virtual communities making use of social networking. Social scientific research shows that the maximum number of people with whom individuals maintain social relationships is approximately 150
- Repositories to collect, disseminate, and translate information on risks to lay audiences

VI. Scenario-Based Approaches for Cyber Resilience

Polycentric governance mentioned in the previous section contributes to building resilience of cyberspace. Resilience of cyberspace requires adaptive capacity. 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 and influence pattern

of change of cyber risks. Diversity of perspectives raised by collaboration of many different stakeholders, that is a critical factor of polycentric governance, identifies those events better.

A. Methodologies for Scenario-Based Review

Systems thinking approach can visualize dynamic relationships among entities and is suitable for modeling how one entity influences other entities in the scenarios.

Systems thinking can describe scenarios in a rich language with a focus on a vast array of interrelationships and patterns of change of cyber risks. It helps to facilitate effective communication among public and private multiple stakeholders and them to see the structure underlying the 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 [16]. View of systems thinking about how the cyber risks are influenced is shown in Fig. 2.

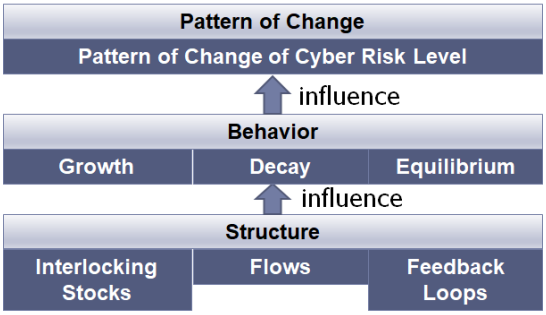

Fig. 2. View of systems thinking about cyber risk

The feedback loops that are core elements of the structure 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 Fig. 3. Plus sign indicates that the element A and the element B change in the same direction.

Fig. 3. Feedback loop

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.

System Dynamics [17] is based on systems thinking and an approach to understanding the non-linear behavior of complex systems over time.

B. Scenario-Based Review at a Cyber-Attcak Level

The scenario-based reviews at a cyber-attack level using systems thinking approach allow multiple stakeholders to review how specific cyber-attacks perform across a variety of situational conditions. Based on the scenarios identified in the reviews, the stakeholders who may be affected by cyber-attacks can identify weak points that could trigger a negative reinforcing feedback loop in cyberspace and important thresholds that can be tipping points before disruptions. According to the output of these reviews, these stakeholders may propose the new rules of cyberspace and discuss accountability around these specific scenarios.

Because a multitude of interconnections may be involved in negative reinforcing feedback loop, it may be difficult to accurately predict the consequence of such disruptions. Scenarios are not necessarily quantitative.

For example, there is a scenario that a malicious program may be executed on a single computer connected to cyberspace and then it could generate an extreme effect across cyberspace by reinforcing feedback as shown in Fig. 4.

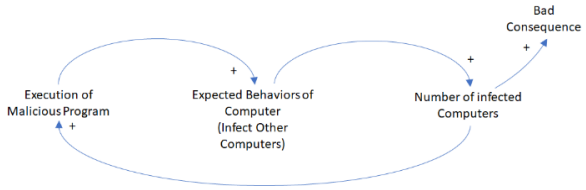

Fig. 4. Example of a scenario

The scenario 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.

For example, anti-virus program may prevent 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 5.

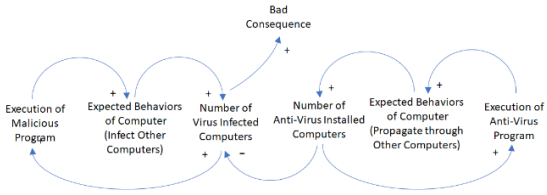

Fig. 5. Example of a leverage

Systems thinking approach 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.

C. Scenario-Based Review at an Individual Organization Level

The scenario-based review at an individual organization level using system dynamics approach allows the organization to analyze the organization's cyber risk across a variety of situational conditions with holistic understanding of their business that relies on cyberspace. It helps to determine organization`s

appropriate appetite for cyber risk considering that the factors affecting the cyber risks and their effect upon level of the risks may not be close in time and space.

For example, there is a scenario that there is a delay until the cyber risk is reduced by controls because of the time taken to implement them and it could influence the level of cyber risk over time. System dynamics helps to simulate how the level of cyber risk is influenced with different time scales and how it can be controlled by adjusting organization`s appetite for cyber risk [18].

VII. Conclusions

This paper demonstrated how polycentric governance could be applied to build resilience of cyberspace as an ideal way of absorbing an impact of cyber-attacks.

The researches on cyberspace, polycentric governance, resilience and application of polycentric governance to cyberspace were reviewed. The importance of resilience for cyberspace was demonstrated by highlighting the characteristics of the cyber risks. And then, suitability of polycentric governance for resilience of cyberspace was verified by finding common between dilemmas posed by environmental variability and change and the dilemmas derived from the characteristics of cyberspace. The critical factors of polycentric governance for building resilience of cyberspace were identified and how to apply them was explained. In addition to that, by focusing on adaptive capacity, more detailed approach on how polycentric governance made up of these factors contributes to building resilience of cyberspace was explained

Although polycentric governance has already proved to be suitable for environmental variability and change, the attempts to apply polycentric governance to build resilience of cyberspace are relatively new. It is not easy to test how polycentric governance really works in actual cyberspace world. Further study of application of polycentric governance to the entities that have many characteristics in common with cyberspace is required in the future research.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Masato Kikuchi conducted research and wrote the paper. Takao Okubo supervised research and reviewed the paper. All authors had approved the final version.

Acknowledgment

Masato Kikuchi thanks IISEC.

References

[1] N. Choucry, *Cyberpolitics and International Relations*, MIT, 2012.

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

[3] A. Appazov, "Legal aspects of cybersecurity," University of Copenhagen, 2014.

[4] M. Kikuchi and T. Okubo, *Cyber Governance Complex in Firms*, ICCCV 2019, 2019.

[5] A National Academy of Sciences (NAS). Disaster Resilience: A National Imperative. The National Academies Press, 2012.

[6] OECD. Guidelines for Resilience Systems Analysis, OECD Publishing, 2014.

[7] International Risk Governance Center (IRGC). Guidelines for the Governance of Systemic Risks, 2018.

[8] F. Björck, M. Henkel, J. Stirna, and J. Zdravkovic, "Cyber resilience – fundamentals for a definition," *Springer. Advances in Intelligent Systems and Computing*, vol. 353. 2015.

[9] N. Engle, "Adaptive capacity and its assessment," *Global Environmental Change*, vol. 21, no. 2, pp. 647-656, 2011.

[10] K. Carlisle and R. Gruby, "Polycentric systems of governance: A theoretical model for the commons," *Policy Studies Journal*, 2017.

[11] D. Feldman, "Polycentric governance," in *Handbook of Science and Technology Convergence*, 2016.

[12] T. Morrison, N. Adger, K. Brown, M. Lemos, D. Huitema, and T. Hughes, "Mitigation and adaptation in polycentric systems: sources of power in the pursuit of collective goals," *Wiley Interdisciplinary Reviews: Climate Change*, vol. 8, no. 5, 2017.

[13] D. Colander and R. Kupers, *Complexity and the Art of Public Policy: Solving Society's Problems from the Bottom Up*, Princeton University Press, 2014.

[14] S. Shackelford, "On climate change and Cyber Attacks: Leveraging polycentric governance to mitigatee global collective action problems," *SSRN*, 2015.

[15] J. Eggenschwiler, "Accountability challenges confronting cyberspace governance," *Journal on Internet Regulations – Internet Policy Review*, vol. 6, no. 3, 2017.

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

[17] J. Forrester, *Industrial Dynamics*, MIT Press, 1961.

[18] M. Kikuchi and T. Okubo, "Issues and remedies for excessive security controls explored by relationships between the time taken to implement security controls and the fluctuation of cyber risk level," *Information Processing Society of Japan (IPSJ) Journal*, vol. 60, no. 12, pp. 2184–2195, 2019.

Masato Kikuchi is a PhD student of Institute of Information Security, Japan. He received the MS degree in Computation from University of Manchester in 1994. From 1994 to 2007, he worked for various Japanese and British companies in London as an IT consultant. In 2007, he joined Oracle Global Information Security. He is a co-editor of ISO/IEC 27005. He is a member of JSSM and IPSJ.

He is a fellow of the British Computer Society. His current interests are cyber resilience and system thinking.

Takao Okubo is a professor of Institute of Information Security, Japan. He received the MS degree in Engineering from Tokyo Institute of Technology in 1991. From 1991 to 2013 he worked as a researcher in Software Engineering and Software Security with Fujitsu laboratories. He received the PhD degree in informatics from the Institute of Information Security in 2009. In 2013 he moved to the Institute of Information Security as an associate professor. He is a member of IEICE, IPSJ, ACM and IEEE CS. His current interests are secure development and threat analysis.