Complex System Governance Theory and Conceptual Links to Cyber Diplomacy

Carmen-Elena CÎRNU[1,2], Alexandru GEORGESCU[1,2]*

[1] Academy of Romanian Scientists – AOSR, 3 Ilfov Street, 050044 Bucharest, Romania

[2] National Institute for Research and Development in Informatics – ICI Bucharest,
8-10 Mareșal Averescu Avenue, Bucharest, 011455, Romania
carmen.cirnu@ici.ro, alexandru.georgescu@ici.ro (**Corresponding author*)

Abstract: Cyber diplomacy is an emerging field of study and practice focusing on transborder coordination between sovereign actors in order to address issues of collective importance related to the digitalization of society, emerging technologies, the threat environment, and other consequences emerging from these developments. This article analyzes cyber diplomacy from the perspective of Complex System Governance theory, which is a framework of thought focusing on the viability of systems-of-systems. Cyber diplomacy can be integrated into such a systemic perspective through its role in communication and coordination among integrated actors. This analysis paves the way for future research into cyber diplomacy, including through modelling and simulation.

Keywords: Cyber diplomacy, Resilience, Complex systems, Governance, Viability.

1. Introduction

Cyber diplomacy is an emerging field of study and practice focusing on transborder coordination between sovereign actors in order to address issues of collective importance related to the digitalization of society, emerging technologies, the threat environment, and other consequences emerging from these developments. Many states have implemented explicit cyber diplomacy initiatives, formalized through consultation groups with companies, positions of Ambassador-at-large for cyber, dedicated departments and centers within Ministries of Foreign Affairs and an active interest in international bodies dedicated to technical issues such as standards or infrastructure. They have also actively tried to develop norms, rules and international law to govern the increasing cyber interaction, dependence, and conflicts between states and between entities operating under different jurisdiction and legal and administrative frameworks. At the same time, there is a growing awareness of cyber diplomacy as an area of theoretical study, which can better explain the evolution of the international system and of the digitalization trend, as well as provide valuable lessons for practical cyber diplomacy efforts.

The present paper expands the theoretical understanding of cyber diplomacy by utilizing an existing framework for analyzing, managing and designing specialty measures for complex systems-of-systems, titled Complex System Governance (CSG). This framework is related to the wider field of Systems-of-Systems Engineering (SoSE) and is utilized, among other applications, for critical infrastructure protection efforts (Pulfer & Bucovețchi, 2016). Drawing on CSG and SoSE theory, it can be noticed that they provide abstractions, concepts and principles (Pulfer & Bucovețchi, 2016) which are useful for systematizing cyber diplomacy in order to expand the state-of-the-art, to make possible modelling and simulation efforts of cyber diplomacy and of systems in which it is used, and to support future theoretical development.

CSG is a particular framework developed in recent years based on SoSE to systematize the challenges facing stakeholders and governance systems, as well as their solutions in a manner applicable to SoS. As a field, it lies at the intersection between system governance, management cybernetics and systems theory (Keating & Katina, 2016). CSG provides, as a framework, "a holistic perspective on the design and operation of a complex system facing a complex system which, in practice, is also beset by ambiguities, uncertainties and political and jurisdictional limits" (Vevera et al., 2019), which can be considered especially relevant for cyber diplomacy. CSG is particularly useful for preventing of "system drift", a phenomenon impacting organically developing complex systems which become affected by various pathologies because of the lack of purposeful design or review. The global ICT infrastructure and ecosystem is a most notably relevant example of organic system evolving in unanticipated directions, without any true overarching intent or design, regardless of attempt by sovereign actors to understand, rationalize and regulate it to a certain degree, which merely adds to the complexity.

https://doi.org/10.24846/v32i2y202312

This paper will prove that the CSG framework is strongly compatible with cyber diplomacy for analytical purposes and, thereby, will provide a better understanding of the high-level governance layer of complex systems-of-systems. This concludes the brief introduction of this article. Section 2 presents the specialty literature for the System-of-Systems Engineering perspective on which the present analysis is based, linking it to cyber diplomacy. Section 3 then presents the Complex System Governance framework to which cyber diplomacy is going to be linked conceptually and which justifies this approach. Following that, in Section 4, the main contributions of this paper can be found, by establishing the conceptual links of cyber diplomacy to CSG theory, including the metasystem functions on which CSG is built. The conclusion summarizes the paper and highlights avenues of further research, based on the results presented in this paper.

2. The System-of-Systems Engineering Perspective

Fundamentally, the approach of this paper is based on System-of-Systems Engineering (SoSE), of which Complex System Governance is a late addition. The approach rests on the issue of escalating complexity in interlocking systems. Gharajedaghi (1999) explained the issue by dividing systemic realities into four cases: organized simplicity, chaotic simplicity, organized complexity and chaotic complexity. SoSE approaches the latter two, by embodying, per Katina et al. (2016), "the planification, analysis, organization and integration process of a mix of preexisting systems and new systems in a system-of-system capability that is more than the sum of its constituent parts." SoSE proposes, according to Boardman and Sauser (2006) to "achieve interoperability, amongst the legacy systems and possibly additions of new systems to the SoS". As a multidisciplinary domain, it has been used for everything, from energy and industrial systems, to weapon systems, transport systems, financial constructs (carbon trading), and myriad others (Katina et al., 2016).

Baugh (2015) also convincingly argues that one driver of the complexity which SoSE can and does handle is that stemming from cross-border operation and governance of complex systems, given that national borders are natural jurisdictions separating different organizations, authorities, standards, philosophies, and acquisition processes in place, not to mention a long-term source of differentiation in how these systems are built-up.

From this perspective, it can be stated that SoSE perspective is tailor made as a lens for analysis of cyber diplomacy as process, practice, and field. Cyber diplomacy, according to Georgescu et al. (2020), is a process using traditional diplomatic means, agents, and institutions, alongside new ones, to tackle transborder cooperation/conflict on issues relating to the digitalization of societies divided by these borders and increasingly unified in cyberspace. Table 1 presents a series of issues tackled by cyber diplomacy, but in a non-exhaustive manner.

Cyber diplomacy emerges as a valuable domain of analysis and practice through the compatibility of its previously stated subject domain with the characteristics of systems-of-systems defined by specialty literature, including Maier (1996) and DeLaurentis (2006).

Maier (1996) and DeLaurentis (2006) presented several characteristics of Systems-of-Systems, as follows:

- Operational independence – Systems can operate independently or autonomously, but can still be a part of a larger SoS featuring interdependencies and exchanges, including through the transmission of changes in one system (positive or negative) to another, potentially setting up feedback loops (vicious our virtuous);

- Managerial independence – Systems can be created, run, managed, acquired, liquidated independently from one another. This obviously describes the fragmentary state of cyber infrastructure across nations, but also the varying competent authorities;

- Evolutionary development – The SoS evolves, by adding new capabilities, systems, components, and competencies based on necessity, experience, interest. Obviously, the pursuit of greater efficiency, productivity, capability, and security in the cyber realm is an instance of evolutionary development;

- Emergent behaviors – The SoS features properties, behaviors and emerging capabilities that are not necessarily found in the individual systems and could not have been anticipated from their analysis in a void. The emerging problems addressed by cyber diplomacy, from ransomware to cryptocurrency regulation and ethical AI,

Table 1. Cyber diplomacy domain

The Cyber Diplomacy Domain of Action	
Crime	Cybercrime in its myriad forms, cyberterrorism, law enforcement cooperation, intelligence exchanges
Harmonization of value-based regimes of governance	Digital authoritarianism, censorship, fair access to reliable data, protection of minors, and other vulnerable groups
Intellectual property	Protection of cross-border intellectual property rights
Privacy protection	Data sovereignty, privacy, protection of minors
Strategic autonomy	Data sovereignty, digital autonomy, strategic autonomy, technological autonomy (including in the European sense)
Standards	Standards for information technology and communication such as 5G
Warfare (conventional, hybrid, asymmetric)	Cyber warfare, the applicability of the Laws of Warfare, cyber restraint, protection of civilians and civilian infrastructures, intelligence exchanges
Emerging technologies	AI ethics, AI bias, Blockchain, threats from deepfakes, non-cyber technological systems undergoing digitalization (smart grids)
Productivity growth through investment	Cross-border investment, value chains, supply chain security
Emerging issues	Any other issues which become current as a result of digitalization (ex.: cryptocurrency and smart contract regulation)

as well as data sovereignty and strategic autonomy indicate that cyber diplomacy is a tool for a cyber SoS governance;

- Geographical distribution – Systems are not necessarily located in loose proximity to each other, in the same jurisdiction or are not necessarily made up of discrete locatable assets, and can include distributed systems/infrastructure in networks;

- System heterogeneity – The components are different, operate according to different logics and necessities, subject to differing constraints. A wider view of the definition of infrastructure as encompassing also organizations, competent authorities, and legislative/administrative frameworks adds to this heterogeneity and is a specific source of necessity for cyber diplomacy;

- Systems are networked – The SoS components are organized within networks which also establish the rules and norms of interactions, whether by design or in an emergent pattern. The chaotic evolution of the digital realm is a prime example;

- Interdisciplinary study – SoSE is a discipline-of-disciplines, requiring knowledge for different fields. Georgescu et al. (2020) establish this as being the case for cyber diplomacy, requiring not only classically trained diplomats, but also subject matter experts, and a cross-fertilization of fields, with diplomats absorbing technical knowledge and experts becoming "diplomatized".

3. Complex System Governance

Keating et al. (2015) define CSG as "a paradigm starting from a theoretical conceptual foundation of a system which defines nine interrelated functions which must function together through various mechanisms. These mechanisms invoke metasystem governance to provide the communication, control, coordination, and, integration necessary for system viability." Keating et al. (2014) provide an alternate definition as "the design, execution and evolution of metasystem functions necessary for communication, control, coordination, and integration of complex systems". According to Katina & Calida (2017), this metasystem approach distinguishes CSG from SoSE, since the metasystem is a conscious abstraction developed by CSG practitioners to understand the system and to design measures to iteratively improve its operation.

In exploring the realm of governance in complex systems, it is crucial to examine various techniques and approaches that have shown potential for improvement. Auditing in machine learning, as discussed by Kearns et al. (2018) and Wilson et al. (2021), offers valuable insights into ensuring transparency and accountability in algorithmic decision-making. Collaborative decision-making, as explored by Filip et al. (2017) and Filip (2020), harnesses collective intelligence and stakeholder participation for more inclusive governance outcomes. The socio-technical aspects within information systems, as addressed

by Tarafdar et al. (2007) and Tarafdar et al. (2020), highlight the intricate interplay between social and technical dimensions, emphasizing the need for a holistic approach to governance. Social contracts in privacy, as exemplified by Martin (2016), establish mutual obligations and responsibilities between data subjects and collectors, contributing to ethical data governance. Cultural aspects in improving machine learning fairness, as investigated by Awwad et al. (2020), shed light on addressing biases and disparities in algorithmic decision-making. Considering the issue of data sovereignty, initially explored by Peterson et al. (2011) and reviewed by Hummel et al. (2021), becomes crucial in governing data-intensive complex systems. Furthermore, industry standards like IEEE 802.11 and IEEE 802.3 provide a solid foundation for establishing technical norms and interoperability in domains such as 5G. By incorporating these diverse techniques and considering their conceptual links to cyber diplomacy, this study aims to contribute to a comprehensive understanding of complex system governance, fostering effective and sustainable governance practices in an increasingly interconnected and digital world.

In the opinion of the authors, it also provides an ideal use case for cyber diplomacy analysis and also for cyber diplomacy as a CSG-compliant mechanism of ensuring system viability for cross-border digitalized systems (which is on track to be all of them, from energy and finance to administration and industry and more).

CSG relies on the concept of complex systems in a wider sense. Complexity is a qualitative measure while complicatedness is a quantitative one. With the application of sufficient effort, one can hope to completely map and understand a complicated system, but not a complex one, since linear growth in the number of system components and functions creates an exponential growth in the possible interactions, leading to characteristics such as emergent behaviors (Eusgeld et al., 2011). Figure 1, compiled by the authors from the specialty literature, emphasizes multiples aspects of this complexity.

There are two fundamental goals for CSG (Keating & Katina, 2016). The first is system viability, which is simply its continued existence. Normally, systems designers and governors aim for resilience, which is the ability of a system to minimize the risk of disruptive events appearing

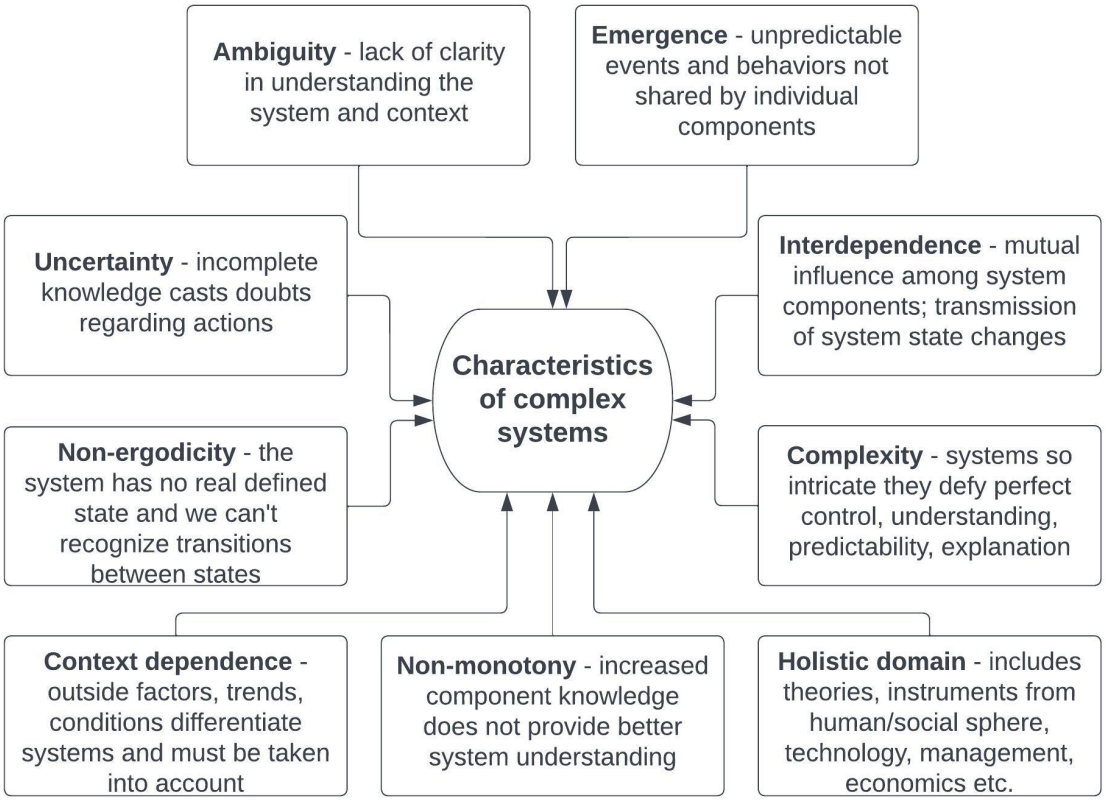

Figure 1. Complex systems and their characteristics (Gheorghe et al., 2018; Keating et al., 2014; Sousa-Poza et al., 2008)

and, should they occur, the minimization of damages and the rapid resumption of a minimum acceptable level of functioning, while taking measures to improve performance (Georgescu et al., 2019; Gheorghe et al., 2018). System viability is the minimum level of continued existence and potential recovery for a complex system. As it has been noted, cyber diplomacy is preoccupied with a variety of governance problems made more difficult by the necessity of cross-border cooperation, with system destruction being a possible worst-case scenario if warnings related to cyber warfare, Internet balkanization, existential AI risk, the destruction of civilian infrastructures with mass damages and casualties and other scenarios advanced in the public realm are taken into account, as justifying state engagement in cyber diplomacy (Georgescu, 2022).

The second goal is the prevention of "system drift". It appears when systems are not subject to a rigorous design and therefore become prey to undesirable and unanticipated consequences. System evolution is chaotic, uncontrolled, self-organizing under myriad pressures stemming from new technologies, techniques, functions, interactions, assets, new security and economic imperatives, new management etc. (Vevera et al., 2022). Since there is no underlying design in the organic growth of the cyber realm, it is predisposed to system drift of numerous types which are relevant from a cyber diplomacy perspective (Georgescu et al., 2020):

- The appearance and adoption of emerging technologies, sometimes in competing forms and in an uncontrolled way;
- The contradictions appearing from the tensions between economic efficiency and security (e.g.: the minimization of security investment as a cost, the rapid uptake of new technology);
- The appearance of criminal, terroristic, or adversarial state actors exploiting security vulnerabilities;
- The rapid development of new industries, markets, economic functions (e.g.: cryptofinance);
- Inter-state competition as a driver of new behaviors, some with negative outcomes (e.g.: hybrid warfare);
- The retrofitting of existing infrastructure systems with digital components, including digital industrial control systems, Internet-of-Things paradigms (billions of sensors), Industry 4.0 (automation).

Ultimately, CSG contributes to the formation of all-stakeholder leadership which, if possible, eschews brute force solutions to surface level problems that neglect systemic issues which cause dysfunctions in complex systems (Georgescu et al., 2019).

4. CSG and Cyber Diplomacy – Contributions

While the role of cyber diplomacy has been highlighted as justification for inclusion among the list of tools and concepts pertaining to the practice of CSG, the present section analyzes this contribution in more detail.

The process starts with listing the axioms for CSG defined by Keating and Katina (2016):

- All systems, whether natural or man-made, are governed by systemic laws which are not directly observable, but are directly responsible for their performance and their observed behaviors. 83 such laws or principles were defined by Keating et al. (2014), but their listing and analysis is beyond the scope of this paper;
- All observable systems perform the nine metasystem functions;
- When systems deviate in their functioning, they are suffering from pathologies making desired performance impossible. 53 system pathologies are detailed in (Katina, 2016);
- These pathologies represent violations of system principles, which lead to escalating performance loss and, if not corrected, can affect system viability;
- The object of CSG processes is to identify pathologies and define and implement measures for their elimination to maintain system viability.

The CSG approach works with four key concepts – context, environment, system, and metasystem (Katina et al., 2016). Context includes all of the underlying conditions, trends, factors which influence the running of a system, but also the leadership styles, political systems etc. The environment represents everything outside of the boundary of a system and which can affect it. The CSG practitioner defines the system boundary as the maximum extent of what he intends to model and govern through CSG. The environment will be everything outside of that line. The system is the inventory of assets and interrelations which come together functionally and with a distinct identity in order to achieve some goal or performance level.

It must conform to the principles of the system that were previously highlighted. The metasystem exists above the system and is the attempt of the CSG practitioner to abstract the system in such a way that he can analyze the system, devise measures and plan their implementation. It should be abstract enough to enable development given existing resources (computing power etc.), but also detailed enough to be relevant to reality.

Table 2 presents the nine components of a CSG, along with the link to cyber diplomacy, as interpreted by the authors from the specialized literature.

Keating et al. (2015) highlight nine metasystem functions of CSG:

- M5 – policy and identity – maintains system identity and trajectory, enables future orientation;

Table 2. CSG framework components (Keating et al., 2015)

The nine components of a CSG framework		
Component	**Explanation**	**Cyber Diplomacy connection**
Design	The deliberate design and architecture of a system to perform certain functions or produce a certain performance	Cyber diplomats actively engage with one another to set up specific initiatives, to harmonize regulations or to set up individual cross-border projects that add up to exercises in deliberate design on top of a chaotic system.
Execution	System operation in its specific context, also in conjunction with other systems	Cyber diplomats attempt to smooth over the functioning of systems in an environment beset by security issues and to promote the standards and common procedures which make inter-system cooperation possible or more fluid, usually as a contribution to facilitating cross-border investment or service trade.
Evolution	Planned changes, as well as ones resulting from external or internal factors	Cyber diplomats are actively engaged in developing visions of future mechanisms for coordination among sovereign actors, such as through confidence building measures, the exchange of information or the building of physical infrastructure supporting cyber systems.
Metasystem	The nine system functions ensuring its operation	Cyber diplomacy often relies on abstracted, high-level assessments of the complex global cyber domain, in order to drive common planning, common investment, action and regulation.
Control	The levers at the disposal of controllers to maintain viability and minimize disturbances, both from internal and external factors. Levers are instruments to be used and authority to be exerted legitimately by controllers to enact their plan. The development of ways, means, and tools, and the obtaining of the requisite authority to wield them should be of great interest to system managers.	Cyber diplomacy is part of a high-level governance apparatus for sovereign actors. They can communicate information on incidents, set up intelligence exchanges, set up coordinating bodies below the level of the political decision makers, plan or coordinate interventions following a successful disturbance etc.
Communication	Basing decision making processes on the gathering, exchange, and processing of information continuously or on an ad-hoc basis	One area of application for cyber diplomacy that has been continuously highlighted is the issue of information asymmetry between actors such as states, which are often reluctant to share information on cyber-attacks or even disclose them, even though this could lead to the prevention of future ones. Increasingly, inter-state cooperation also includes access to specialized services and capabilities such as modelling and simulation for systems, cyber ranges (such as the one of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia) and automated data sharing among trusted allies.
Coordination	The interaction between SoS components or between them and the environment has to take place with minimal frictions or avoidable collisions	This is a core task for diplomats, especially since their principals often have different priorities, background cultures, perspectives and weights of previous interactions, not all of them positive.
Integration	A dynamic equilibrium between system components that results in a unique overall complex system identity. These components are still capable of independent or autonomous operations, but they also feature interdependencies	The cyber domain is already highly integrated, but states are sovereign in their governance decisions and their legislative/administrative frameworks. Cyber diplomacy provides a bridge towards international or global governance through the integration and gradual harmonization of national governance systems, especially in key parts (law enforcement, legality of cyber warfare, information sharing etc.).
Complex Systems	System-level interactions produce values which are not registered at the level of individual system components	Cyber diplomats are at the forefront of mediating new capabilities or new security performance, by addressing the global-level interactions between national governance systems.

- M5* – system context – the totality of elements which can obstruct or aid the system;
- M5' – strategic system monitoring – performance indicators, expectations, evaluations to see whether desired system functioning is a success or a failure;
- M4 – system development – the current state of the system and the future desired one are imprinted by this function; transition from one to the other is facilitated;
- M4* – learning and transformation – learning from error resolution and facilitating metasystem transformation to better conform as a governing model, in an iterative process;
- M4' – environmental surveillance – develops and implements tools or methods for extracting data from the environment to identify important trends, threats, risks etc;
- M3 – system operations – facilitates routine system operation for optimal performance (including maintenance, upgrades, training etc.);
- M3* – operational performance – facilitates the monitoring of the system to identify errors, aberrant behaviors and other problems which may impact system viability;
- M2 – system communications – supporting metasystem functioning by developing channels of communication, procedures, methods, data flows, common modes of analysis etc.

Table 3 presents the nine metasystem functions of a CSG and the applicability to cyber diplomacy, as interpreted by authors from the specialized literature.

It may be observed that cyber diplomacy is compatible with the CSG framework in the context of complex, transborder cyber system governance. CSG, therefore, becomes a framework for the detailed analysis of cyber

Table 3. Metasystem functions for CSG (Keating et al., 2015)

Function	Cyber Diplomacy connection
M5 – policy and identity	Cyber diplomacy is predicated on an understanding of cross-border interdependencies which make a global cyber system a reality and require a coordinated response to address future challenges, some of which can be anticipated.
M5* – system context	Cyber diplomats are actively identifying and resolving hindrances in cross-border governance of cyber systems and facilitating helpful developments. They are both responsive to trends, new factors, and new developments, while also aware of their cross-border nature.
M5' – strategic system monitoring	Cyber diplomats frequently engage, on behalf of their principals, in analyses of the global system based on key indicators (economic, security etc.). Other cyber diplomatic entities explicitly engage in this, such as international institutions with specific remits (for instance, standards setting).
M4 – system development	Cyber diplomatic entities often employ a future state (whether negative or positive) to justify their activities in the present and to orient them towards achieving goals. Interactions between cyber diplomats can lead to harmonizing these views, whether at their level or that of the sovereign principals.
M4* – learning and transformation	Cyber diplomacy provides one part of a feedback mechanism which can facilitate the reduction of informational asymmetries, the sharing of experience and best practices, the spread of useful standards etc.
M4' – environmental surveillance	Cyber diplomats actively engage in the analysis of the environment and in setting up initiatives that facilitate information sharing and common analysis of the environment on behalf of their principals and sometimes utilizing each other's limited information and unique perspectives to build a clearer picture.
M3 – system operations	The haphazard nature of the development of the global cyber domain has made cross-border coordination for improving the vital performance, especially on security processes (prevention/prosecution of cybercrime, increased resilience, prevention/deterrence of cyber warfare etc.). Other issues include the sustainable mass adoption of emerging technologies, the improvement of security culture and more.
M3* – operational performance	Cyber diplomacy is often used to address proven challenges which cannot be handled by sovereign actors through action just in their sovereign space. Cyber diplomacy also contributes to situational awareness and to the early pinpointing of trends which may generate new risks, vulnerabilities and threats.
M2 – system communications	The basic application of cyber diplomacy is to facilitate communication and information exchanges among sometimes rivalrous actors, which are reluctant to share information for fear of incurring costs or losing an advantage. At the very highest level of cyber diplomatic success, mechanisms between actors are set up for the real-time sharing of cyber-related information and intelligence, with no human or organizational input delaying information sharing, as it exists within the Five Eyes group of countries (the US, Canada, the UK, Australia and New Zealand).

diplomacy in a theoretical sense. There are various reasons for this, beyond the matching of system components and functions. The principal one, according to Katina et al. (2016), are the characteristics of the cyber-physical system which are the foundation of cyber space as a usable (and ubiquitous) environment for all manner of applications. In extremis, all critical infrastructure systems today are actually better defined as cyber-physical systems (Gheorghe & Schlapfer, 2006). Katina et al. (2016) identified the key characteristics that make these systems amenable to a CSG approach:

- Responses to environmental shifts rely on input-output parameters;
- Multiple components, subsystems and systems act in parallel, and the main informational linkage is through cyber components;
- The main instrument for fine course corrections are feedback loops, which are integrated into the governance apparatus;
- Resource allocation and system viability are maintained through continuous monitoring in real-time, with data collection, processing, and interpretation being done continuously and integrated into sometimes automated response mechanisms;
- These cyber-physical systems are especially utilized in a critical context, where operational error correction and finetuning must take place in real-time, to avoid runaway system degradation and cascading disruptions.

Cyber diplomacy is a layer on top of the existing system, providing key coordination among sovereign or independent actors who are not coordinating in real-time, in order to facilitate the reduction of information asymmetries, to address outside and emerging threats, and to preemptively imprint a design or pattern on the system (through standards, common projects and collective decision making), that improve the operational environment for these cyber-physical systems.

5. Conclusion

The paper emphasizes a new perspective on the Complex System Governance paradigm. CSG is utilized to analyze the role of cyber diplomacy role in a system-of-systems approach. The results showed significant compatibility, enabling the use of CSG framework to systematize and further analyze cyber diplomacy. As an expanding international practice in a rapidly changing technological and security environment, cyber diplomacy represents a field of study of growing interest, which has not been analyzed using an SoSE type of approach. The results enable future theoretical development, especially as pertains to the intersection between cyber diplomacy and critical infrastructure protection, as well as other fields. The work also advances the possibility of modelling and simulating cyber diplomacy as a factor in SoS simulations, adding a new dimension for comparative analysis of security governance and opening up the possibility of using theoretical work to develop real policy proposals in the realm of cyber diplomacy. The next step in the research agenda envisioned in the present paper is to develop the cyber diplomacy theoretical framework for specific fields, such as critical infrastructure protection, energy issues, standards setting, and to utilize game theoretical approaches to model various outcomes, including through the use of open-source instruments for multi-criteria decision analysis.

Acknowledgements

The findings presented in this article are based on the research project *Cyber Diplomacy as a governance tool in the digital society* [*Cyber Diplomacy ca instrument de guvernanță în societatea digitală*]. The research work was supported by a grant of research project competition of the Romanian Academy of Scientists for young researchers AOSR-TEAMS 2022-2023, edition administered by Academy of Romanian Scientists – AOSR.

REFERENCES

Awwad, Y., Fletcher, R., Frey, D., Gandhi, A., Najafian, M. & Teodorescu, M. (2020) *Exploring Fairness in Machine Learning for International Development.* Comprehensive Initiative on Technology Evaluation – Massachusetts Institute of Technology (CITE MIT D-Lab). Report. http://d-lab.mit.edu/sites/default/files/inline-files/Exploring_fairness_in_machine_learning_for_international_development_04012020_pages.pdf [Accessed: 20th June 2023].

Baugh, D. (2015) Environmental scanning implications in the governance of complex systems. *International Journal of System of Systems Engineering*. 6(1-2), 127-143. doi: 10.1504/IJSSE.2015.068812.

Boardman, J. & Sauser, B. (2006) System of Systems-the meaning of *of*. In: *2006 IEEE/SMC International Conference on System of Systems Engineering, 24-26 April 2006, Los Angeles, CA, USA*. IEEE. pp. 118-123. doi: 10.1109/SYSOSE.2006.1652284.

DeLaurentis, D. (2005) Understanding transportation as a system-of-systems design problem. In: *Proceedings of the 43rd AIAA Aerospace Sciences Meeting and Exhibit, 10 –13 January 2005, Reno, Nevada*. American Institute of Aeronautics and Astronautics (AIAA). p. 123. doi: 10.2514/6.2005-123.

Eusgeld, I., Nan, C. & Dietz, S. (2011) "System-of-systems" approach for interdependent critical infrastructures. *Reliability Engineering & System Safety*. 96(6), 679–686. doi: 10.1016/j.ress.2010.12.010.

Filip, F. G. (2022) Collaborative Decision-making: concepts and supporting information and communication technology tools and systems. *International Journal of Computers Communications & Control*. 17(2), 732. doi: 10.15837/ijccc.2022.2.4732.

Filip, F. G., Zamfirescu, C. B. & Ciurea, C. (2017) *Computer-Supported Collaborative Decision-Making*. Cham, Switzerland, Springer International Publishing.

Georgescu, A. (2022) Cyber Diplomacy in the Governance of Emerging AI Technologies – A Transatlantic Example. *International Journal of Cyber Diplomacy*. 3, 13-22. doi: 10.54852/ijcd.v3y202202.

Georgescu, A., Gheorghe, A., Piso, M.-I. & Katina, P. F. (eds.) (2019) *Critical Space Infrastructures: Risk, Resilience and Complexity (Topics in Safety, Risk, Reliability and Quality, 36).* Cham, Switzerland, Springer International Publishing., pp. 321-343. doi: 10.1007/978-3-030-12604-9.

Georgescu, A., Vevera, V. & Cîrnu, C. E. (2020) The Diplomacy of Systemic Governance in Cyberspace. *International Journal of Cyber Diplomacy*. 1, 79-88.

Gharajedaghi, J. (1999) *Systems Thinking – Managing Chaos and Complexity*. Oxford, Elsevier, Butterworth Heinmann.

Gheorghe, A. V. & Schlapfer, M. (2006) Ubiquity of Digitalization and Risks of Interdependent Critical Infrastructures. In: *Proceedings of the 2006 IEEE International Conference on Systems, Man and Cybernetics*, *08 – 11 October 2006*, *Taipei, Taiwan*. USA, Institute of Electrical and Electronics Engineers (IEEE). pp. 580–584. doi: 10.1109/ICSMC.2006.384447.

Gheorghe, A., Vamanu, D. V., Katina, P. & Pulfer, R. (eds.) (2018) *Critical Infrastructures, Key Resources, Key Assets: Risk, Vulnerability, Resilience, Fragility, and Perception Governance (Topics in Safety, Risk, Reliability and Quality, 34)*. Cham, Switzerland, Springer International Publishing. doi: 10.1007/978-3-319-69224-1.

Hummel, P., Braun, M., Tretter, M. & Dabrock, P. (2021) Data sovereignty: A review. *Big Data & Society*, 8(1). https://journals.sagepub.com/doi/10.1177/2053951720982012 [Accessed 20th June 2023] doi: 10.1177/2053951720982012

Katina, P. F. & Calida, B. Y. (2017). Complex system analysis for engineering of systemic failures. In: Hopkins, M. (ed.) *Systems Engineering: Concepts, Tools and Applications*. New York, USA, Nova Science Publishers, pp. 105–132.

Katina, P. F. (2016) Systems theory as a foundation for discovery of pathologies for complex system problem formulation. In: Masys, A. J. (ed.) *Applications of Systems Thinking and Soft Operations Research in Managing Complexity*. Cham, Switzerland, Springer International Publishing, pp. 227–267.

Katina, P. F., Keating, C. B. & Gheorghe, A. V. (2016) Cyber-Physical Systems: Complex System Governance as an Integrating Construct. In: Yang, H., Kong, Z. & Sarder, M. D. (eds.) *Proceedings of the 2016 Industrial and Systems Engineering Research Conference*, *21 – 24 May 2016, Anaheim, California, SUA*. pp. 212-217.

Kearns, M., Neel, S., Roth, A. & Wu, Z. S. (2018) Preventing fairness gerrymandering: Auditing and learning for subgroup fairness. In: Dy, J. & Andreas Krause, A. (eds.) *Proceedings of the 35th International Conference on Machine Learning, PMLR 80, 10 – 15 July 2018, Stockholm, Sweden.* USA, MLR Press. pp. 2564-2572.

Keating, C. B. & Katina, P. F. (2016) Complex system governance development: A first generation methodology. *International Journal of System of Systems Engineering*. 7(1/2/3), 43–74. doi: 10.1504/IJSSE.2016.076127.

Keating, C. B., Katina, P. F. & Bradley, J. M. (2014) Complex system governance: concept, challenges, and emerging research. *International Journal of System of Systems Engineering*. 5(3), 263–288. doi: 10.1504/IJSSE.2014.065756.

Keating, C. B., Katina, P. F. & Bradley, J. M. (2015) Challenges for developing complex system governance. In: Çetinkaya, S. & Ryan, J. K. (eds.) *Proceedings of the 65th Annual Conference and Expo of the Institute of Industrial Engineers, 30 May – 2 June 2015, Nashville, Tennessee.* USA, Institute of Industrial and Systems Engineers (IISE). pp. 2943-2952.

Maier, M. W. (1996) Architecting principles for systems-of-systems. *Systems Engineering*. 1(4), 267-284. doi: 10.1002/(SICI)1520-6858(1998)1:4<267::AID-SYS3>3.0.CO;2-D.

Martin, K. (2016) Understanding privacy online: Development of a social contract approach to privacy. *Journal of Business Ethics*. 137, 551–569. doi: 10.1007/s10551-015-2565-9.

Peterson, Z. N. J., Gondree, M. & Beverly, R. (2011) A position paper on data sovereignty: The importance of geolocating data in the cloud. In*: Proceedings of the 3rd USENIX Conference on Hot Topics in Cloud Computing, HotCloud'11, Berkeley, USA*. USA, USENIX Association. pp. 1-7.

Pulfer, R. & Bucovețchi, O. (2016) Modelling risk dependencies within complex situation management concept. *UPB Scientific Bulletin, series B*. 78(4), 139-146.

Sousa-Poza, A., Kovacic, S. & Keating, C. (2008) System of systems engineering: an emerging multidiscipline. *International Journal of System of Systems Engineering*. 1(1-2), 1-17. doi: DOI:10.1504/IJSSE.2008.018129.

Tarafdar, M., Teodorescu, M. H. M., Tanriverdi, H., Robert Jr., L. P. & Morse, L. (2020) Seeking ethical use of AI algorithms: Challenges and mitigations. In: *Proceedings of International Conference on Information Systems, ICIS 2020, 13 – 16 December, India.* ICIS. pp. 1-7

Tarafdar, M., Tu, Q., Ragu-Nathan, B. S. & Ragu-Nathan, T. S. (2007) The Impact of Technostress on Role Stress and Productivity. *Journal of Management Information Systems*. 24(1), 301-328. doi: 10.2753/MIS0742-1222240109.

Vevera, A. V., Georgescu, A. & Cîrnu, C. E. (2019) The paradigm of complex system governance, necessary in a cyber interconnected world. In: Badea, D., Bucovetchi, O. & Iancu, D. (eds.) *Capability Management and Managerial Capability within Critical Infrastructure Systems*. Sibiu, Romania, Land Forces Academy Publishing House, pp. 270-283.

Vevera, V., Georgescu, A., Cîrnu, C. E. & Nate, S. (2022) Critical Infrastructure Protection – resilience in an uncertain future. In: Ioanid, A., Fleacă, B. & Moiceanu, G. (eds.) *Business Change and Digital Transformation in A World Moving Through Crisis: Proceedings of the International Conference of Management and Industrial Engineering*, *ICMIE 2022, Faculty of Entrepreneurship, Business Engineering and Management, University POLITEHNICA of Bucharest, Romania*. Bucharest, Romania, Niculescu Publishing House. pp. 209-222.

Wilson, C., Ghosh, A., Jing, S., Mislove, A., Baker, L., Szary, J., Trindel, K. & Polli, F. (2021) Building and auditing fair algorithms: A case study in candidate screening. In: *Proceedings of the 2021 ACM Conference on Fairness Accountability, and Transparency*, *3 – 10 March 2021, Canada*. New York, United States, Association for Computing Machinery (ACM). pp. 666-677. doi: 10.1145/3442188.3445928.