Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P4930-cd

Space systems as critical infrastructure - A soft systems approach

Christine Große

Department of systems and space technology, Luleå University of Technology, Sweden.
Risk and Crisis Research Centre, Mid Sweden University, Sweden; E-mail: christine.grosse@ltu.se

Leif Sundberg

Department of Informatics, Umeå University, Sweden.
Risk and Crisis Research Centre, Mid Sweden University, Sweden; E-mail: leif.sundberg@umu.se

Adam Abdin

Department of Industrial Engineering, CentraleSupélec, University of Paris-Saclay, France
Risk, Resilience and Reliability Research Group. E-mail: adam.abdin@centralesupelec.fr

Technological developments have enabled private and public actors to access near-Earth space. Space systems are both critical infrastructure and important sub-systems of other critical infrastructures (e.g., GPS and weather forecasting) dependent on space technology. However, unlike other critical infrastructures, space systems are relatively unexplored from a security perspective. The paper presents a system model based on a synthesis of the current research front discussed in national and international research literature, reports, and studies. The soft systems methodology is used to develop the model useful for actors concerned with risk management to increase the understanding of systemic dependencies of space systems and strengthen the resilience in critical infrastructures and services. This paper provides insights into digital risks for space systems, highlighting serious societal consequences and areas for enhanced space security. Based on the system model and the analysis provided for a better understanding of the relationships among these systems, future research needs to strengthen cybersecurity in space systems as exemplified.

Keywords: Space, digital resilience, systemic thinking, SSM, governance, critical infrastructure, societal security.

1. Introduction

Technological developments have enabled many private and public actors to conduct a variety of operations in space by launching computing platforms into Earth orbit and beyond. As these platforms, or 'space vehicles' that constitute a part of a space system, are increasingly used to facilitate essential daily services for various stakeholders, they are considered critical infrastructure. However, the space system is both unprepared and understudied when it comes to cybersecurity threats, which is a serious knowledge gap in both practice and research (Oakley 2020). Recent disruptions to space systems in countries on NATO's eastern border highlight contemporary cybersecurity concerns as different actors, involved in geopolitical conflicts, aim to gain influence in space.

Space security has therefore become a major concern for societal protection. Space systems can be considered both critical infrastructure and important sub-systems of other critical infrastructures (e.g., GPS and weather forecasting) dependent on space technology (Fidler, 2018). However, unlike other critical infrastructures, space systems are relatively unexplored from a security perspective (Gheorghe et al. 2018). This is a serious knowledge gap as tensions are increasing due to geopolitical conflicts and the risks of the militarisation of space technology. In parallel, increasing commercialisation and interconnectivity of space systems with important services give rise to several challenges for societal resilience. By creating a better understanding of the relationships among these interconnected systems, this paper provides insights into digital risks involving serious societal consequences and areas for enhanced space security work.

To facilitate such understanding, this paper presents a system model based on a synthesis of

the state-of-the-art in academic literature on space systems and cybersecurity. The analysis seeks to emphasise relevant areas of security in space systems. The soft systems methodology (SSM) (Checkland and Poulter 2010) is used to develop a conceptual model useful for both risk management actors and as a stepping stone for further research. By doing so, the aim is to increase the understanding of systemic dependencies of space systems and contribute to strengthening the resilience of critical infrastructures and associated services. Based on the analysis and the system model, suggestions for future research to improve cybersecurity of space systems are provided. The presented study is a direct response to previous research indicating a need for measures to protect and create resilient development in space (Breda et al. 2023, Oakley 2020).

The paper proceeds as follows. Section 2 positions space systems as critical infrastructure and presents the paper's systems thinking perspective. Then, Section 3 provides materials and methods, followed by results from the synthesis of state-of-the-art in Section 4. Based on this synthesis, Section 5 presents the conceptual space system model. Section 6 discusses implications for research and practice in the area, and Section 7 concludes the paper.

2. Concepts and Context

2.1. *Critical infrastructure and space*

Infrastructure is characterised as an underlying basis that comprises 'fixed assets, service processes, formal rules and information flows' (Große 2023). This structure provides the preconditions for specific users on whom they act. This means that the user's perspective determines the critical process that infrastructure performs as a system and the product or service it delivers. A tripartite structure – physical/fixed assets, service provision, and expression of will – can therefore contribute to enhancing the understanding of the recursive multi-level character of systems (Große 2023), such as the space system as critical infrastructure. Infrastructure becomes critical if the survival, well-being and progress of a society depend on maintaining its ability to function (Cohen 2010).

Critical infrastructure is today largely dependent on well-functioning information and communication systems (ICS), which stresses their understanding as complex 'sociotechnical system-of-systems' (Gheorghe et al. 2006), These ICS involve a range of technologies, for example, wireless networks and remote-controlled systems. Space systems can be considered as (part of) ICS that include installations in space, such as geostationary satellites. Hence, space systems can be recognised both as a critical infrastructure in their own right and as an important component of other types of infrastructure that depend on space technology (Fidler 2018). However, unlike other types of critical infrastructure, space systems are relatively unexplored from a security point of view. For example, there are no overviews of cybersecurity measures for this type of system (Falco 2018). Despite a few studies of the space domain (e.g., Gheorghe et al. 2018), this is still a serious knowledge gap with increased tension in the area due to geopolitical conflicts, which risk escalating into a militarisation of space technology. This study contributes to enhancing the understanding of space systems as (part of) critical infrastructure.

2.2. *Systems thinking*

The term 'system' has been discussed for decades, which has given rise to a range of concepts and understandings (for a comprehensive review see, e.g. Große 2023). This article does not contain a complete definition of the term but emphasises important core aspects that guided the research.

Systems can be regarded as 'complexes of elements standing in interaction' (Bertalanffy 1968). Interactions in this quote indicate that the relationships between system elements are not linear, and by that trivial – rather, they are complex and not necessarily causally or deterministically interrelated. Such complex and adaptive systems have components that interact in parallel, build subroutines, base actions on conditional reasoning, and use adaption to improve performance (see e.g., Große 2023, Holland 2006).

A socio-technical system as a holistic system is able to achieve a better result than the parts on their own (Emery and Trist 1960). Particularly important is the ability of humans as part of the system to create improvements and add value to the system (Mumford 2006). Their adaptability of behaviour in emergencies is additionally a vital driver of system resilience (Boin and McConnell 2007). The complexity of critical infrastructure however requires a similarly complex system to organise and govern it (Ashby 1956).

3. Materials and Methods

This paper employs the soft systems methodology (SSM), developed by Checkland (1972) and revised by Checkland and Poulter (2010). The SSM is commonly used to explore complex situations and stakeholder needs, often in the early stages of system development (Große 2019, 2022, Sørensen et al. 2010). Thus, it is well suited for the aim of this paper, by allowing to structure a complex problem and to reach a shared understanding of relevant and necessary actions. The revised SSM (Checkland and Poulter 2010) consists of four activities – finding out, model building, discussing, and defining action – in an iterative cycle of learning. This paper aligns this cycle with the design-oriented research process used in information systems research (Österle et al. 2011) consisting of four steps – analysis, design, evaluation, and diffusion – as follows.

3.1 *Finding out – Analysis*

An analysis of a real-world situation perceived as problematic is central to this activity. First, we conducted a search for literature on cybersecurity and space systems and performed bibliometric analysis to extract relevant keywords. The aim of this activity was to create an initial overview of space systems and the wider effects of digital technology developments that provide vital functionality to dependent societies.

Table 1. Literature selection process.

Literature search	Articles
TITLE-ABS-KEY(cybersecurity OR "cyber security" OR "cyber-security") AND TITLE(space)	373
Selection by title and abstract	190

The literature was collected from the scientific database Scopus. Table 1 shows the search terms, hits and the number of articles selected. The selection used a step-by-step refinement process that examined titles, keywords and abstracts and identified the focus of the publications. Almost half of the found publications were discarded because they did not fit within the scope of this study, as they addressed other 'spaces' such as data, public, virtual or cyber spaces. Finally, 190 publications were exported and formed the basis for the analysis to inform an understanding of space systems as critical infrastructure.

Bibliometric keyword analysis provided an overview of the research area. Using the VOS viewer software (van Eck and Waltman 2014), network maps were created that facilitated the exploration and analysis of the selected literature regarding space systems as critical infrastructure.

3.2. *Model building – Design*

The design of a conceptual system model is central to the second activity – model building. Starting with the 'Rich Picture', which is based on the results from the previous step, a root definition of a 'space system' is formulated, and an action model suggested. These three sub-models support a stepwise abstraction from the initial problem situation to a higher-level conceptualisation. To concretise the purpose and perspectives of the system, the root definition employs the following elements, collectively referred to as CATWOE (Checkland and Scholes 1999): customers (C), actors (A), transformation process (T), *Weltanschauung* (W) (worldview 'of the owner'), owner (O) and environment (E). The action model is then derived from the root definition, establishing a bridge between concept and practice.

3.3. *Discussing – Evaluation*

The evaluation of the created models is the focus of this activity. In this study, the evaluation includes both a discussion of the proposed system model and its usefulness and reflections on space systems as critical infrastructure and implications for future research and practice. In this paper, the activity *discussing* involves an argumentative approach that compares the sub-models with the findings presented in scientific literature. Based on the analysis and the system model, future research avenues to strengthen cybersecurity in space systems are exemplified.

3.4. *Defining action – Diffusion*

This conclusive activity concerns the search for accommodation between different worldviews on feasible and desirable changes in practice, which also includes the diffusion of research results among the target groups and the realisation of further studies. The findings of this study facilitate a constructive dialogue among concerned stakeholders about further actions to develop this complex system of critical infrastructure while emphasising societal resilience.

4. Finding Out: An Analysis of Space Systems

In this section, we present the results from the bibliometric analysis of literature that serves as a basis for conceptualising the space system and its interactions. The analysis aimed to support the modelling by providing information on which components, interactions and concerns exist and how they are relevant in the context of the space system in general and the subsystems in particular.

First, we created a network map (see, Figure 1) based on keyword co-occurrence (full counting, all keywords), with a minimum number of occurrences set to five. This analysis generated six clusters with a total of 75 keywords, as represented in Table 1. This step also involved an interpretation of what the clusters are 'about'.

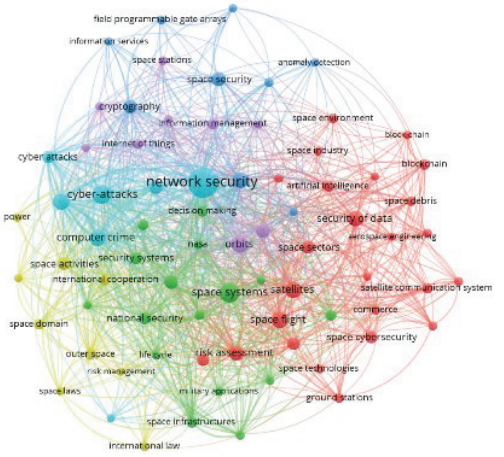

Fig. 1. Network map of author keywords.

The clusters provided insights about relevant dimensions, such as customers/actors, system functionality and owners, and key perspectives and conditions. For example, in addition to ground, orbit and space assets, the clusters 'red' and 'green' in Figure 1 highlight a range of actors from industry and government involved in using and forming the space system as critical infrastructure. Relevant keywords here include 'ground stations', 'satellites', space vehicles, 'aerospace industry', 'commerce', 'NASA' and 'public works'. These two clusters further indicate security-related concerns by keywords like 'space debris', security of data', 'life cycle' and 'security systems'.

Meanwhile, cluster 'blue' is directly associated with network security of space systems, signified by keywords such as 'authentication', 'cryptography' and 'space security'. The focus is on the technical part of the socio-technical system. Interorganisational or policy network issues are not similarly present in the selection of literature.

Cluster 'turquoise' involves various threats against space systems, represented by keywords such as 'computer crime', 'cyber attacks' and 'cyber threats. Cluster 'yellow' contains keywords related to ownership and regulation, given that space does not adhere to national borders, which provokes questions related to 'international cooperation', 'international law' and 'space laws'. It further indicates issues and considerations related to 'space activities', 'information dissemination' and risk management'. Finally, the 'purple' cluster in Figure 1 contains items related to operations in the earth's orbit, with keywords such as 'earth (planet)', 'orbits', 'space stations' and 'manned space flight'.

Table 1. Network cluster characterisation.

Cluster	Description	Exemplary keywords
Red (25 items)	Industry actors	aerospace industry, commerce
Green (16 items)	Space as critical infrastructure	space infrastructures, national security
Blue (9 items)	Networks	authentication, cryptography
Turquoise (9 items)	Threats	computer crime, cyber attacks
Yellow (9 items)	Regulation	international law, international cooperation
Purple (7 items)	(Earth) orbit operations	orbits, space stations, manned space flight

5. Conceptual Model of Critical Space Systems

5.1. *The Rich Picture of the systemic situation*

The first sub-model depicts the role of the space system as a hub of space and Earth observation and communication. Figure 2 shows the multitude of interconnected actors, assets and services that constitute the space system as well as relevant groups of customers. It also illustrates interfaces that connect this subsystem with other parts of the information (infrastructure) system. Adapting SSM, the picture includes various exemplary threats and concerns that represent a selection across a conceivable spectrum of relevant matters.

Preconditions, including possible threats, for space and Earth observation and communication appear around the ground station and space vehicle assets as well as their interactions, which are central to this *Rich Picture*, and include reliable energy supply, durable materials and secure components, and well-trained personnel. Moreover, the space system relies on secure data transmission, processing and storage, ground services and mission control to provide relevant services for various public and private actors. In addition to the harsh environmental conditions in the orbit and beyond that affect the various types of space operations, legal obligations impose further constraints.

Space and Earth observation and communication provided by the space system create several values for stakeholders at the global, national, regional and local levels, such as monitoring solar activity and climate patterns. Other benefits include the positioning of objects in space and on Earth, enabling, for example, navigation, transport automation and the mitigation of risks associated with asteroids. In addition, the ability to maintain a view from above not only facilitates landscape management, the monitoring of wildlife populations or the observation of weather and natural and man-made hazards but also contributes to safeguarding societal and national security. It also enables satellite-based communication which is essential for areas without other alternatives. Generally, the space system causes emissions, such as noise, pollution, and greenhouse gases during launch activities or production, which have varying levels of impact on stakeholders. Apart from the effects on Earth, one of the most pressing effects is the debris in orbit from the remains of various space vehicles, which in turn increases the collision risk for existing and new space vehicles, including the consequences for the services and consumers they support.

5.2. *Root Definition of the space system*

Derived from the literature analysis and the Rich Picture, the second sub-model formulates a root definition of the generic space system using the CATWOE elements (see Section 3.2) (Checkland and Scholes 1999). The core root definition (CRD) of the space system can be formulated as follows:

A world-community-owned system, staffed by qualified professionals from local, national and supranational organisations, which, considering

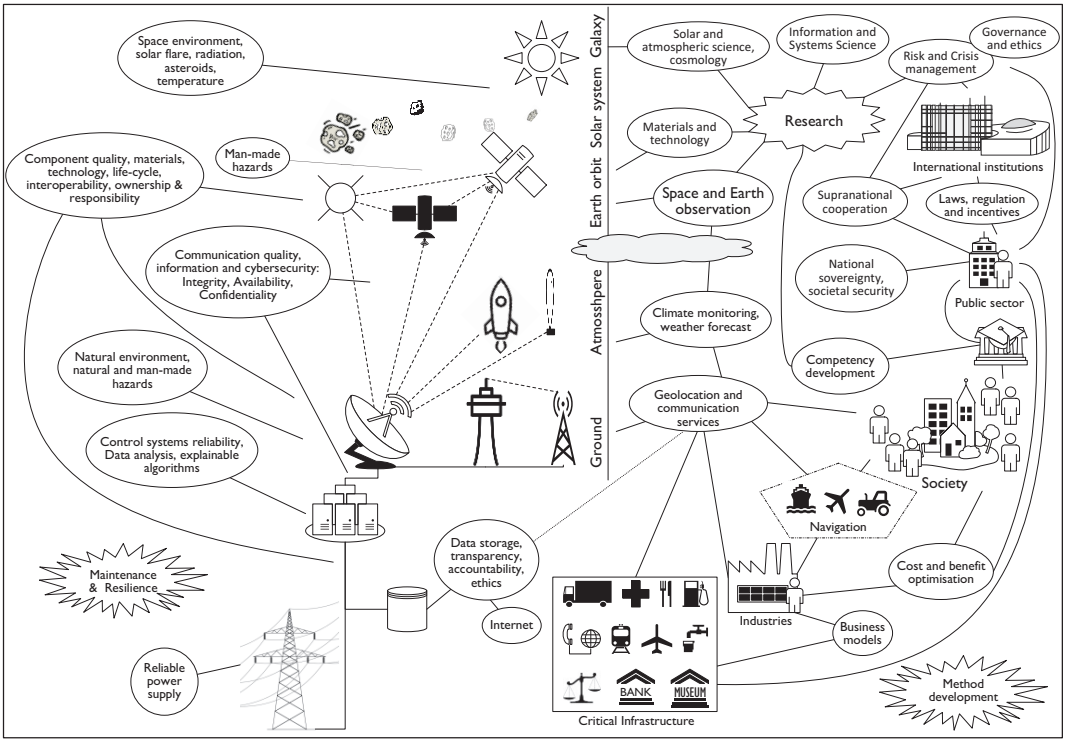

Fig. 2. Rich Picture of the space system as critical infrastructure.

legal regulations and technical limitations, supports secure and reliable space and Earth observation and communication. It collects and provides relevant data, samples and information for research, societal development and risk and crisis management.

(C) Customers of the space system and its services include public and private organisations as well as individuals which can be located elsewhere. Their needs are supported by suitable resources produced during the system's transformation process (T). However, how and for what purpose a customer uses the results of (T) is beyond the control of the space system and requires additional control mechanisms (see Section 5.3)

(A) Key actors are private companies and public organisations, such as manufacturers, research institutes, service providers, and various suppliers, that enable space and Earth observation and communication.

(T) The needs that the system addresses are associated with reliable space and Earth observation and communication, such as the positioning of near-Earth objects and objects on the Earth's surface, as well as the monitoring of solar or global phenomena, such as climate and natural and man-made hazards. It fulfils these needs by securely collecting, transmitting, analysing and storing data, samples and information in space, on Earth and in between.

(W) The *Weltanschauung*, justifying the system's activities, entails that the space system can ensure reliable, efficient and sustainable networks to provide space and Earth observation and communication that in turn benefit the people on Earth, in space and elsewhere.

(O) The owners of the space system are those who have the authority to cancel the entire transformation process (T). Disregarding the ownership of the multitude of sub-systems, only the World community could abolish the space system. Ownership of the space system is therefore not primarily a national matter but varies in form between contested and cooperative and is affected by geo-political circumstances.

(E) Environmental constraints, such as harsh conditions in space, legal regulations, and technical and societal limitations, are here seen as given and primarily beyond the system's sphere of influence. However, natural, scientific, technological and political progress will influence future system developments and operations.

5.3. *Model for Extended System Analyses*

The third sub-model follows the statements of the core root definition of the generic space system, which help to abstract thinking from the current realisation. It identifies purposeful activities that are necessary to carry out (T). The results of the literature analysis revealed tensions between (T) and (W) as well as between the objectives of sub-systems and the overall space system. Therefore, the activity model in Figure 2 includes space and Earth observation and communication considerations that should complement the current analyses to assess the cumulative value of this system as critical infrastructure.

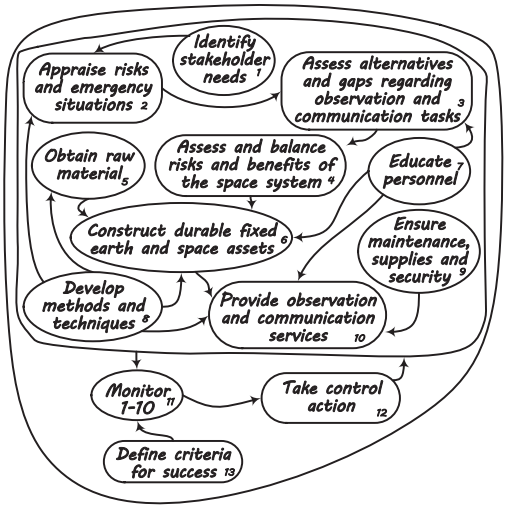

Fig. 2. Conceptual Activity Model.

The evidence emphasises that several services are of particular importance for society, such as geopositioning as a basis for maritime and aerial navigation and automated agriculture, monitoring of climate and weather on Earth and of solar activity and asteroids in space, and communication services for rescue and security purposes. Models that assess the value of space systems to society should thus account for the impact of disruptions to such services due to various causes, such as natural hazards, cyber-attacks, technical failure or material fatigue. The value of space and Earth observation and communication for knowledge development can be similarly considered as it consequently enhances other societal developments.

Monitoring and documenting the prerequisites, activities and results of decisions made, are necessary to ensure the quality of the

process (T) and create a basis for improvement. Defined performance criteria, such as the secure and reliable functionality of the system, can help to evaluate the success of the approach and enable those responsible to take control measures in the event of unfavourable deviations.

As multiple public and private stakeholders are both involved in the system or use its functionality, individual objectives may vary and the system owner (O) may require an adequate control capability. This control subsystem can govern the activities performed during (T) by means of a feedback loop. In addition to taking measures towards the system to ensure its secure and reliable functioning as critical infrastructure, the control system must also act outwardly against (mis-)use on the customer side and to counter external threats. As mentioned, responsibility for the space system is thus a global issue and must involve a broad discussion of its conditions.

6. Discussion

The conceptual system model, presented in the previous section, constitutes a novel framework of the space system, including a representation of relevant stakeholders, interactions and concerns, which enables the system's recognition as critical infrastructure. The analysis of the literature and the space system emphasised several security issues, thus providing a basis for further improvements.

One aspect that needs to be considered is the definition of system boundaries, that is, what belongs to the system or goes beyond it (Ashby 1956). For example, space and Earth observation and communication can be used in different ways for different purposes. However, the customer-side utilisation as such is beyond the system's control, yet it remains an ethical dilemma to what extent the system is responsible for a customer's activities. In this context, higher-level control mechanisms are necessary, such as regulation and law enforcement, cultural changes and collective responsibility.

In this study, we used bibliometric analysis upon a relatively large corpus of papers to generate an overview over the space system and to identify keywords and clusters in the scientific literature on cybersecurity of space-related systems. The keywords and clusters were further used as a novel approach to inform a conceptual model using SSM for further analysis. While the bibliometric analysis alone does not allow for a deeper understanding of the literature, it is a suitable method to extract information about an emerging research area, such as security concerns related to space systems. Bibliometric analysis can be further extended with more in-depth reading of the literature and methods for system analysis, such as SSM used in this study.

The SSM is a useful approach to analyse, model and characterise the system of interest, such as the space system as critical infrastructure, and to outline its steering system at a general level. Although the steering or governance system can be included to a certain extent in the conceptual model, its detailed representation is not intended in SSM. Instead, it should be approached as the system of interest itself for a more detailed analysis. This constraint addresses the recursiveness of systems but leads to a seemingly (over-)harmonic representation of the space system that aggregates malicious customer intentions and antagonistic actors attempting to interfere with system functionality together with natural factors as environmental conditions. To account for this issue, the CATWOE-construct (see Checkland and Scholes 1999) could be usefully expanded with an additional T to include potential *threats* into system analysis, management and development by default.

Here, the analyses focused on the space system and its functionality. Therefore, security-enhancing measures are mainly directed towards the system components, interactions and environment(s). This involves ground and space assets, communication networks, organisational contexts, production and service processes, and environmental conditions on Earth, in the orbit and wider space. The bibliometric analysis pointed to several threats towards the system and solutions were sought to strengthen the system. However, systemic risk management should be expanded so that it includes the handling of consequences in addition to the mitigation of vulnerabilities and threats to strengthen societal resilience. Cyber resilience is one example of a research gap identified in the literature, especially considering the asymmetrical threats associated with space systems (Baylon 2014, Daxhelet 2023). The conceptual model stresses additional areas for future research, such as liability issues relating to the use of (scarce) resources, the management of space debris and the control of complex systems.

In sum, we see great opportunities for scholars to apply and extend our approach to other areas and domains of concern.

7. Conclusions

The study combined a literature review with conceptual modelling through SSM to examine current approaches to space security and develop a holistic view on space systems. The contribution is twofold: first, we conceptualise the space system as critical infrastructure and highlight security issues, stakeholders, assets, interactions and concerns related to this complex socio-technical system that necessitate further research. Second, we present a novel approach by combining bibliometric analysis and SSM. In this way, we open up for further research on the topic of space security, including the empirical validation of the proposed approaches and possible regulatory efforts, and for the application of our methodology to other domains. The paper thus contributes to a better understanding of systemic dependencies of space systems and to strengthening the resilience in critical infrastructures and services.

Acknowledgement

This research was financially supported by the Swedish Civil Contingencies Agency, 2024-06704

References

Ashby, W. R. (1956). *An Introduction to cybernetics*. Chapman & Hall, London.

Baylon, C. (2014). *Challenges at the intersection of cyber security and space security: Country and international institution perspectives*. Chatham House, The Royal Institute of International Affairs.

Bertalanffy, L. von (1968). *General System Theory: Foundations, Development, Applications*. George Braziller, New York.

Boin, A. and McConnell, A. (2007). Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. *Journal of Contingencies and Crisis Management* 15(1): 50–59.

Breda, P., Markova, R., Abdin, A. F., Mantı, N. P., Carlo, A. and Jha, D. (2023). An extended review on cyber vulnerabilities of AI technologies in space applications: Technological challenges and international governance of AI. *Journal of Space Safety Engineering* 10(4): 447–458.

Checkland, P. and Poulter, J. (2010). Soft Systems Methodology. In: Reynolds, M. & Holwell, S. (eds.) *Systems Approaches to Managing Change: A Practical Guide*. Springer, London: 191–242.

Checkland, P. and Scholes, J. (1999). *Soft systems methodology in action: A 30-year retrospective,* [New ed.]. Wiley, Chichester, Eng., New York.

Checkland, P. B. (1972). Towards a systems-based methodology for real-world problem solving. *Journal of Systems Engineering* 3(2): 87–116.

Cohen, F. (2010). What makes critical infrastructures Critical? *International Journal of Critical Infrastructure Protection* 3(2): 53–54.

Daxhelet, É. (2023). *The intersection between outer-space security and cybersecurity*.

Emery, F. E. and Trist, E. L. (1960). Socio-technical systems. In: Churchman, C. W. & Verhulst, M. (eds.) *Management Science Models and Techniques*, 2nd edn. Pergamon: 83–97.

Falco, G. (2018). The Vacuum of Space Cyber Security. In: *AIAA SPACE and Astronautics Forum and Exposition*. American Institute of Aeronautics and Astronautics, Reston, Virginia.

Fidler, D. P. (2018). *Cybersecurity and the New Era of Space Activities: Digital and Cyberspace Policy Program, April 2018*.

Gheorghe, A. V., Georgescu, A., Bucovețchi, O., Lazăr, M. and Scarlat, C. (2018). New Dimensions for a Challenging Security Environment: Growing Exposure to Critical Space Infrastructure Disruption Risk. *International Journal of Disaster Risk Science* 9(4): 555–560.

Gheorghe, A.V.; Masera, M.; Vries, D.L. and Weijnen, M. (eds.) (2006). *Critical Infrastructures at Risk: Securing the European Electric Power System*. Springer, Dordrecht.

Große, C. (2019). Airports as Critical Infrastructure: The Role of the Transportation-by-Air System for Regional Development and Crisis Management. In: *2019 IEEE Int. Conf. on Industrial Engineering and Engineering Management*: 440–444.

Große, C. (2022). Towards a Holistic Perspective on Future Transportation Systems: A Swedish Case and a Conceptual Framework. *Future Transportation* 2(4): 846–867.

Große, C. (2023). A review of the foundations of systems, infrastructure and governance. *Safety Science* 160(11): 106060.

Holland, J. H. (2006). Studying Complex Adaptive Systems. *Journal of Systems Science and Complexity* 19(1): 1–8.

Mumford, E. (2006). The story of socio-technical design: reflections on its successes, failures and potential. *Information Systems Journal*(16): 317–342.

Oakley, J. G. (2020). *Cybersecurity for Space: Protecting the final frontier*. Apress Berkeley, CA.

Sørensen, C. G., Fountas, S. and Nash, E. et al. (2010). Conceptual model of a future farm management information system. *Computers and Electronics in Agriculture* 72: 37–47.

van Eck, N. J. and Waltman, L. (2014). Visualizing Bibliometric Networks. In: Ding, Y., Rousseau, R. & Wolfram, D. (eds.) *Measuring scholarly impact: Methods and practice*. Springer, Cham.

Österle, H., Becker, J. and Frank, U. et al. (2011). Memorandum on design-oriented information systems research. *European Journal of Information Systems*(20): 7–10.