Critical Space Infrastructures

13

Alexandru Georgescu

Contents

Abstract

Space systems are a key enabler for a wide variety of applications which have become critical to the functioning of modern societies. This chapter uses the Critical Infrastructure Protection framework to argue that space systems may constitute a new form of critical infrastructure, dubbed Critical Space Infrastructure, and traces the positive impact that such a perspective may have on space security governance. Critical Infrastructure Protection has developed a conceptual toolbox, as well as practical policy prescriptions, which may be of use to policy and decision-makers to increase resilience and meet future space security challenges.

Keywords

Critical infrastructure · Resilience · Space systems · Governance · Complex system

A. Georgescu (✉)
National Institute for Research and Development in Informatics (ICI), Bucharest, Romania
e-mail: alexandru.georgescu@ici.ro

K.-U. Schrogl (ed.), *Handbook of Space Security*,
https://doi.org/10.1007/978-3-030-23210-8_129

Introduction

Space systems have become a key enabler for a wide variety of applications related to command, control, coordination, data gathering, and communications. With their growing capabilities and numbers, the quantity and quality of applications also increase, while lowering access barriers, thereby improving usability and leading to an increase in the number of beneficiaries.

The Organisation for Economic Co-operation and Development (OECD) (2016) notes that the world is entering a fifth stage of space development, one in which we are witnesses to "growing uses of satellite infrastructure outputs (signals, data) in mass-market products and possibly for global monitoring of treaties (land, ocean, climate), third generation of space stations, extensive mapping of solar system and beyond thanks to new telescopes and robotic missions, new space activities coming of age (e.g. new human-rated space launchers, in-orbit servicing)." Space inputs permeate many of the products (tangible and intangible) that we consume, which are the result of extensive global supply and production chains or of the processing of information and the combining of symbols within globalized networks.

Therefore, space services may be consumed directly or indirectly through their role in the functioning of other systems on which we are dependent. The use of space capabilities in energy, transport, financial markets, agriculture, weather forecasting, and other fields is well-known. These latter systems represent a small cross-section of critical infrastructures (CI), sociotechnical systems whose disruption or destruction would generate significant economic damage, casualties, and loss of confidence (Gheorghe et al. 2018, p. 3). Their security is paramount and, therefore, we must consider the question of their governance. While government deals with decision-making, governance encompasses mechanisms, norms, and organizations that mediate the decision-making and implementation process.

The governance of the aforementioned infrastructures like energy and transport relies on Critical Infrastructure Protection (CIP), a comprehensive framework for managing the risk to the key infrastructures, assets, and resources on which our societies are critically dependent, which has been developed for the past two decades.

This chapter aims to introduce space systems into the CIP framework and define them as Critical Space Infrastructures (CSI), arguing that CIP can close some of the gaps that have manifested in the governance of space security and which are creating significant troubles from the perspective of sustainable exploitation of space. With the articulation of the existence of CSI, we follow up with a discussion on Critical Space Infrastructure Protection (CSIP) from the perspective of the specialty literature.

Critical Infrastructure Protection

CIP was first conceived during the Clinton Administration, but only came to the fore after the September 11 attacks, when the systemic impact of the attacks was noted and provided ample argument in favor of the defining trait of CIP, the

interdependencies between components, infrastructures, and systems which lead to the transmission of risk and the cascading disruption of critical infrastructures. Presidential Decision Directive (PDD)-63 (1998) identified critical infrastructures as being "those physical and cyber-based systems essential to the minimum operations of the economy and government" (The White House 1998). CIP did not stay confined at the national level. Later, the EU would create its European Program for Critical Infrastructure Protection (EPCIP) through which it set guidelines for improvement of national CIP governance and the identification, designation, and protection of European Critical Infrastructures. Directive 114/2008 established that European Critical Infrastructures are "essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people" and are distinguished from national CI through their impact on two or more Member States "as a result of the failure to maintain those functions" (European Commission 2008).

CIP works most often with the concept of resilience, which is the capacity or quality of a system to retain or rapidly regain an adequate level of functioning in the face of a crisis event, with minimal disruption, material damage, or loss of human life. Linkov et al. (2014) argued that resilience should be a priority from the design phase of new systems and of their regulatory frameworks, because resilience is the only consistent answer to the issues of uncertainty and complexity. CIP also works with numerous other concepts, which encompass different aspects of CI qualities, behavior, and interactions during crisis events (Table 1).

Interdependencies are a key feature of CIP systemic thought. Gheorghe and Schläpfer (2006) define interdependencies as bidirectional relationships wherein the status of one infrastructure affects the status of others and is affected in its turn by others. The topology of critical infrastructure risk is built also with the mapping of interdependencies. These are varied, being physical, sectoral, geographic, logical, social/political, cybernetic, or informational and with many taxonomies in existence. The other key features are the dynamics of cascading disruptions – "cascading disasters are extreme events in which cascading effects increase in progression over time and generate unexpected secondary events of strong impacts. These tend to be at least as serious as the original event and contribute significantly to the overall duration of the disaster's effect" (Pescaroli and Alexander 2016). They result from the vulnerabilities and rigidities that accumulate within a system-of-systems across multiple domains until a trigger event or mechanism manifests alongside the alignment of key breaking points. The absence of these alignments prevents the actual cascading disruption event, as it interrupts the vector for the transmission and escalation of the disruption. Pescaroli and Alexander (2016) distinguish between cascading effects and cascading disasters. The former are the multidimensional and complex dynamics which produce the latter.

Regionalization and globalization have brought these issues to the fore, as cooperation becomes a key facet of CIP efforts when global supply and production chains as well as globally synchronized databases and markets produce new risks, vulnerabilities, and threats which are beyond the ability of single jurisdiction authorities to tackle. If chains are only as strong as their weakest links, decision-makers and CIP practitioners cannot count on localized resilience and CIP success to

Table 1 An overview of concepts related to resilience. (Source: author compilation)

Concepts related to resilience in CIP specialty literature	
Vugrin et al. (2011)	
Absorptive capacity	An internal quality of the system that allows it to absorb the effects of systemic or environmental disruption with little degradation in functioning. It is associated with robustness and the presence of redundancies
Restorative capacity	The system recovers easily from the effects of a disruption and also experiences permanent modifications as a result of the episode (adoption of new technology, reorganization, etc.)
Adaptive capacity	The system reorganizes itself in order to maintain functionality, reduce disruptive impact, and rapidly recover full function levels. For instance, a factory may switch suppliers or modify its designs to limit the impact of resource scarcity
Jonkeren et al. (2012)	
Static resilience	The ability of a system to continue functioning after suffering a major shock
Dynamic resilience	The rapidity with which a system recovers from a disruptive event. It is related to repair and reconstruction times
Rockefeller and Arup (2014)	
Reflectivity	Such a system is conscious of the uncertainties and of the changes in the security environment
Robustness	The system actively eschews designs which render it vulnerable to cascading disruptions, catastrophic malfunctions, and overdependence on certain assets
Redundancy	Is found in the diversity of pathways and options for fulfilling system tasks. A system with redundancies can weather significant increases in pressure, upstream shocks, or the malfunctioning of individual assets and system components
Flexibility	The quality that a system possesses to change as a result of shocks and to even find benefits in those changes
Adaptability	The capacity to mobilize systems and resources during temporary stresses or shocks in order to attenuate the impact of the negative events
Inclusivity	The system seeks out and accepts inputs from all categories of stakeholders and includes it in the process of developing strategies, plans, priorities, and resource distribution patterns
Integration	An integrated system responds efficiently to challenges and features short and rapid feedback channels. The governance mechanisms transcend sectorial and other limitations in order to adequately reflect the complexity of the system and to adequately implement policies and decisions

maintain systemic integrity. Helbing (2013) emphasized that global critical infrastructure networks facilitate the propagation of risks and generate the potential for cascading disruption stemming not just from external factors (such as attacks, sabotage, natural disaster) but also from internal ones resulting from system errors, attrition, malinvestment, lack of maintenance, and, most important of all, the complexity of the system-of-systems (SoS). These disruptions within the SoS may lead to the contagion and the escalation of the effects, sometimes in a mutually reinforcing pattern. Perrow (1999) discussed the "normal accidents" or spontaneous malfunctions that arise from the complexity and tight couplings of a system, sometimes without the possibility having ever been foreseen. Eusgeld et al. (2011)

argue that a SoS perspective acknowledges that the components of infrastructure systems may be large-scale systems as well, sometimes operating autonomously from a legal, administrative, or governance standpoint, but linked to the wider system through dependencies and interactions which assign systemic consequences to localized disruptions through the propagation of risks and disruptions.

There was a tacit acceptance of these risks, to the extent to which they were anticipated, in exchange for the efficiencies and gain in well-being that accompanied them. If one were to describe the evolution of CI in the past hundred years, it is that formerly autonomous and vertically integrated infrastructure systems separated by geography, information lag, and risk aversion suddenly found themselves in much greater contact (Bucovețchi et al. 2019), a situation which Setola et al. (2017) called "rapid change in the organizational, operational and technical aspects of infrastructures." Cyber infrastructures and now space infrastructures are some of the initiators and facilitators of systemic changes which result in the increase in CI SoS surface contact and in the tightening of the couplings within the system that accelerate the transmission of risk. The systemic transformations give rise to new sources of added value, new functionalities, and also punctual increases in safety and security through higher governance capacity, but also new risks, vulnerabilities, and threats.

The field is constantly evolving to keep pace with the demands of a SoS beset by and in thrall to growing complexity. One of the recent evolutions, for instance, is complex system governance (CSG), which emphasizes complexity as a source of emergent and sometimes unanticipated behaviors and properties in the system not found in its individual components. A later section of the chapter will elaborate on this idea.

Critical Space Infrastructures

OECD (2019) defines space economy as the "the full range of activities and the use of resources that create and provide value and benefits to human beings in the course of exploring, understanding, managing and utilizing space. Hence, it includes all public and private actors involved in developing, providing and using space-related products and services, ranging from research and development, the manufacture and use of space infrastructure (ground stations, launch vehicles and satellites) to space-enabled applications (navigation equipment, satellite phones, meteorological services, etc.) and the scientific knowledge generated by such activities. It follows that the space economy goes well beyond the space sector itself, since it also comprises the increasingly pervasive and continually changing impacts (both quantitative and qualitative) of space-derived products, services and knowledge on economy and society."

Infrastructure serves not only the economy but also society, and we may draw on this definition to define a space infrastructure (SI) as a sociotechnical system whose main functional component is located beyond the arbitrary line separating the Earth's atmosphere from outer space. Critical Space Infrastructures have the added trait of criticality – their disruption or destruction would cause significant casualties,

economic damage, or loss of confidence. CSI have components that are also intra-atmospheric – for instance, ground stations and communication links (Fig. 1).

The identification and designation of CI serves an important role in CIP processes, but this tendency may be muted in space. A country may have tens of thousands of miles of roads, serving a large number of settlements of all sizes, which makes the designation of the critical ones for national functioning and continuity in the face of attacks all the more important. However, SI do not have an especially large inventory, given the high number of functions they serve and the number of beneficiaries. For the rest of the chapter, we will discuss CSI primarily as a function of orbiting assets, or satellites. As the field develops, we will one day be able to talk about CSI composed of probes, research bases on other planets, and interplanetary transport networks. As of yet, a theoretical threshold of criticality will likely only be met by SI containing satellite components. The only other likely candidates are the various probes which measure the activity of the Sun and are part of early warning systems regarding solar flares that give CI operators opportunities to enter conservation states or initiate measures to safeguard system integrity. If we were to speculate on the criticality of early warning systems for another high-impact, low-frequency event – the collision of the Earth with asteroids – we would find that operational assets are also located on Earth or in orbit.

According to the frequently updated open-source database of the Union of Concerned Scientists, by 31 March 2019, there were 2062 satellites in orbit (UCS 2019). Table 2 breaks down that number.

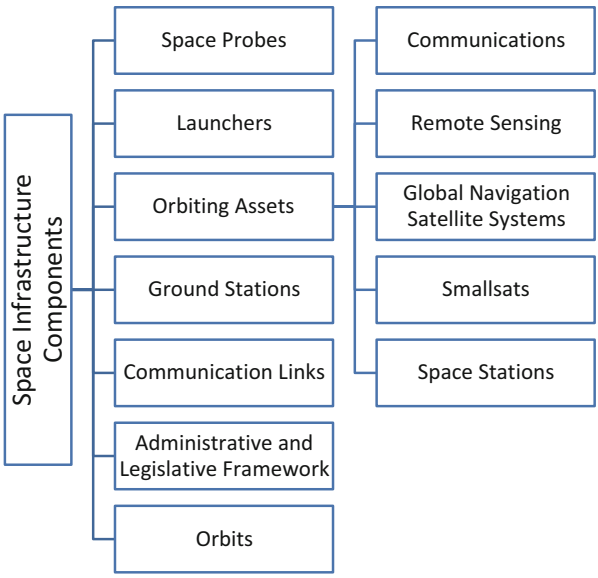

Fig. 1 Space infrastructure components. (Source: author)

Table 2 Breakdown of orbital asset inventory, compiled by author with data from UCS (2019)

Total number of satellites = 2218 by 30 September 2019				
By country	United States 1007	China 323	Russia 164	Other 724
By orbit	Low 1468	Medium 132	Geostationary 562	Elliptical 56
Total estimated number of US satellites = 1007				
By character of owner	Civil 35	Commercial 620	Government 163	Military 189

Distinguishing Characteristics of SI and CSI

The extreme technical, operational, and financial constraints under which satellite operators labor have significant results on the characteristics of CSI and the subsequent emerging risk profile, as opposed to terrestrial CI.

Firstly, their main distinguishing characteristic is, as mentioned, their low numbers. This is compounded by the size factor. While the correlation is waning with the advances in miniaturization, the larger satellites (by mass) will tend to be the most critical, because the expense needed to develop and launch them must be justified by their function and capabilities. However, according to Ambassador Sorin Ducaru, Director of the European Union Satellite Centre, speaking on 4 October 2019 in Bucharest during the International Eurodefense Conference, only half of the existing assets weigh more than 1000 kg (wet mass). Niederstrasser (2018) pegs this as the upper bounds of the smallsat category of system size, and Bryce Space and Technology (2019) confirms that around half of launched systems were in this range in 2018.

Secondly, the larger systems are more likely to be one of a kind, designed specifically for the respective mission, resulting in little interoperability with other systems or opportunities for stakeholders reliant on them to substitute for any lost capacity.

Thirdly, the cost structure and technical barriers make system replacement an expensive, long-term, and uncertain proposition, one that governments are more likely to find palatable. The CSI are also less likely to feature intermediate thresholds of functioning, where partial utility may be maintained in the event of the materialization of a risk, unlike many terrestrial CI, for whom total disruption is just one end of a long spectrum of partial disruption states (transport network carrying capacity, processing power, public services delivery rate and area coverage, partial production of energy and of goods, etc.).

These barriers are being subverted by the wider application of new technologies, like CubeSat architecture and by miniaturization, which are also an initial enabler of convergence with terrestrial CI in another important way – preponderance of ownership or operation by private entities. In Europe and the United States, the estimates of this rate are very high and vary between 60% and 85%, depending on source, and where the upper bound is set by the United States (Cellucci 2018). Bryce's annual State of the Satellite Industry reports have noted the increase of CubeSat numbers

among launches, as well as the preponderance of nongovernmental entities (commercial, academic) among the owners. Bryce (2019) noted that 1300 smallsats (according to Bryce definitions, up to 600 kg) were launched between 2012 and 2018, of which 961 were CubeSats. And half of all of these provide commercial services, especially in remote sensing. This trend accounts for the high use of low Earth orbit, and the differences in inventory breakdown would be even starker, if orbital dynamics and atmospheric drag did not lower the mission time of such satellites.

CSI are expected to function in a very challenging security environment, featuring both natural and man-made threats, the latter divided into unintentional and deliberate. The Royal Academy of Engineering (2013) notes the high likelihood of spontaneous malfunction from environmental pressures, derived also from mass and cost constraints for the engineering of more robust systems, though this is also proceeding apace. Terrestrial CI do not generally feature such high background risk levels, since existing regulations regarding resilience from the design phase, on a sectorial and national basis, attempt to reduce the impact of background factors (geology, hydrography, etc.) or include them in decision-making regarding critical infrastructure commissioning. The space-specific threats of debris collisions and extreme space weather phenomena also significantly impact CI, while the former also presents a significant collective action failure that any emerging governance framework will have to address. Moreover, from the beginning, the US National Security Space Strategy has defined space as a "congested, competitive and contested" environment (DoD and ODNI 2011).

CSI are also interesting for their limited current range of interdependency types. Until we have arrived at the level of space industrialization and active resource exploitation, there will be very few cases of physical interdependencies, or of bidirectional dependencies.

Critical Space Infrastructure Protection

Heino et al. (2019) argue, with regard to traditional CIP efforts, that “a severe disruption in the system can go beyond geographical, organizational, and administrative boundaries, thus activating a multifaceted set of actors whose ability to collaborate is required to restore the situation.” Stakeholders will have to engage in Critical Space Infrastructure Protection (CSIP) efforts in order to improve the resilience of CSI or of the system-of-systems in which it is operating. Starting from a common definition of CIP, CSIP efforts comprise all of the programs and activities in which stakeholders will engage in order to maintain the level of functioning of Critical Space Infrastructures above a predefined threshold in case of the materialization of a threat and to minimize the casualties, material damage, and systemic impact on other CI. The stakeholders run the gamut from manufacturers of components and providers of services to the owners/operators of CSI, the competent national authorities (civilian, military), and various international or supranational organizations. The latter is the case of the EU, which administers the EU space

program, comprising the Galileo/European Geostationary Navigation Overlay Service (EGNOS) global navigation satellite system, the Copernicus remote sensing program, and the future governmental satellite communications network for EU and EU Member State government communications.

While CSIP is a subset of CIP efforts, it is important to acknowledge the differences in approach which CSIP will entail, deriving from the specific CSI characteristics, the space security environment, and the actual ability of a respective stakeholder to govern and positively impact space security outcomes. CSIP is, from the start, a very international activity which will find distinct advantages stemming from the application of global solutions to persistent issues such as space debris, frequency fratricide (already governed globally), and hardening against space weather phenomena. Countries may not have any SI and still be critically dependent on those operated under the jurisdiction of others. Few countries have full spectrum capabilities, and none of them have total space autonomy so that their society and economy are exclusively provisioned with critical space services (and, in the future, goods) by systems under their jurisdiction. However, CSIP efforts start at the national level, which is the ideal starting point for relations with the lower orders of stakeholders involved in the process. What CSIP cannot do is solve the persistent and intentional gaps in the legal and administrative framework of space, as those are contingent on the political will of major spacefaring nations to agree to bind themselves with rules, as opposed to implementing their own programs for space security governance. CSIP can offer tools, mechanisms, and activities short of political action that can lead to an understanding of security issues, their proper communication to important decision-makers and other stakeholders, and their gradual amelioration through resilience-building measures.

It is important to note that designing CSIP governance mechanisms must also take into account the possible future state of the CSI system-of-systems and its environment. This estimate is not only technological but also social, legal, political, geopolitical, and economic. Exercises in strategic foresight like the one described in The Future of Space 2060 report released by Air Force Space Command in 2019 may hold particular significance for each organization, but they are ultimately developing scenarios for system contexts, infrastructure, and interrelationships that will determine the governance solutions necessary to maintain system viability (Air Force Space Command 2019), which is an almost exact description of complex system governance under CIP efforts.

What we can say with near certainty about the future is that we will have many more space systems in place, as well as space actors (especially private ones), that our dependence on them will have increased and new dependents will have materialized from the developing world. The potential results of the materialization of a negative event will have increased as well, maybe to the point of becoming an existential threat at systemic levels. Significant uncertainties will persist in the legal and administrative realm, as the best positioned countries to profit materially and strategically from this ambiguity will head off most efforts aimed at collective action toward positive security transformations. Just as in the steady globalization of CIP, CSIP will be an important vector for the coalescing of common concepts, definitions, toolboxes, practices, and standards, because of the previously stated need for

practitioners to cooperate because of interdependencies. The increasingly globalized private sector will act as a vector for the spread of these elements, as they will be able to cooperate with CSIP efforts and CIP efforts aimed at managing the exposure to CSI risk in each country in which individual companies are present and are regulated from a CIP perspective by the national authorities.

Results from Framework Application

If we were to apply the CIP framework to space systems, we would have to be careful to keep in mind the specificities of these systems, of their operating environment, and of their threat matrix, as mentioned in the prior sections. It would also require acknowledgment that some of the elements of a CIP framework may already be under development or in place, such as a space situational awareness program.

It is important to note that CIP also influences considerations on future SI design in favor of resilience and the achievement of acceptable levels of the qualitative and quantitative indicators of resilience listed in the CIP theory section.

The application of CIP would require competent national authorities to begin an identification and designation process for CSI, based on a methodology they have developed for this purpose, in order to allocate scarce security resources to where they would have the highest impact. Owners/operators (OO) of CSI would come under the purview of the competent sectoral authority and would have to conform to regulations regarding protection measures and coordination with the other stakeholders in the national CIP system. This varies on a state-by-state basis, but it generally entails the development of an operator's security plan (OPS) for approval by the competent authority, its regular update (on a set schedule or whenever the situation calls for it), and the implementation of a communication system or structure with the liaising authority. In the European system, this is achieved through security liaison officers embedded within the infrastructure operator and the competent authority, as well as mechanisms for the sharing of relevant information.

CI operators/owners in energy, transport, and other domains would also have to take note of their dependence on CSI, apply adequate methodologies to estimate it, and factor it into their respective OPS.

A generic OPS identifies vulnerabilities, describes existing security programs, and details the ones that will be implemented, as well as the gradual and permanent measures that are instituted with every increase in the alert level.

For a CSI OO, the OPS would include not only references to background security levels but also readiness levels for expected threats such as space weather. The OO is tasked to articulate a security vision for its CSI, in order for the OPS to meet with approval from the regulator, such as plans for new satellite design policies that stress resilience through physical and electromagnetic shielding, for security through obscurity by using specially designed software and other systems, or for redundancy in the form of higher satellite counts, lower replacement times, and so on.

For an OO of an infrastructure dependent on CSI, the OPS would include its plans to mitigate the risk of disruption of critical space services. The possibilities are

varied – it may have contracts in place with alternate providers or even alternate system providers, who are not subject to cascading disruptions in the space environment (e.g., ground-based data collection as opposed to space-based remote sensing). The OO may also commit to a reduction in its dependence on CSI, though many entities have limited ability to negotiate and limit CSI risk from third parties (such as OOs of other CI on which they are dependent).

Depending on the country in question, it is possible that there are no CSI OOs within the national jurisdiction. These countries must manage their dependence on CSI without having the possibility of exerting influence to ameliorate their vulnerabilities and therefore face a slew of other challenges and uncertainties (including political) when compared to countries with partial or full spectrum space capabilities. These countries may become active in international fora (such as UN COPUOS – the Committee on the Peaceful Uses of Outer Space) and intergovernmental arrangements in order to pursue a part in collective governance efforts.

Georgescu et al. (2019, p. 272) speculated that one answer to the issue of space governance may lie in the change of incentive structure resulting from the formalization of the space governance issue, for instance, through the CIP framework. Whereas a collision in space or some other disruptive or destructive event may currently be written off as an "Act of God," the average CI operator on Earth finds himself under greater scrutiny when disruptions occur. The CI designation system formalizes a responsibility on the part of the OO, as well as the competent authority and the ultimate coordinating authority at higher levels (the Ministry of Interior in the European model, the Department of Homeland Security in the American one). A failure of due diligence, such as inadequate security measures, exposes the OO to liability issues, whose potentially significant costs may eventually make them more accepting of the higher costs of greater security. A market-centric governance model may also emerge, where unsustainable behavior in space, with impact on the security outcomes, may also be sanctioned in an emergent manner through market mechanisms – interest rates for funding new investment or insurance premia may be lower for security-conscious actors whose systems are less prone to disruption or destruction by design or through other factors.

Given the nature of the space environment, CIP efforts must also focus on cooperation between nations, as they are starting to do also on the ground, with the emerging coordination for the protection of transborder or global infrastructure chains in energy or transport (EPCIP's efforts have been mainly in the energy and transport areas, if one looks at the list of designated ECI). By stressing the mutual dependence of countries and the security gains from having a resilient CI system-of-systems, cooperation under a CIP framework, especially between different orders of stakeholders below the political level, may have far-reaching impact.

Principles of Resilience

As mentioned before, the application of a CIP framework seeks to increase the resilience of the system in question or of the wider CI system-of-systems. CSI would

also strive for resilience and thereby utilize the conceptual toolbox described in the previous chapter to plan for an increase in resilience. In this regard, Johnsen (2010) describes seven principles of resilience whose application to space systems may clarify the results of a CSIP framework.

Chief among these is the graceful or controlled decline, which is the result of competencies and capacities which arrest the quick decline of a system, for instance, through the prompt and efficient intervention of emergency response teams or other contingency measures. The system is also set up in such a way that the chance of catastrophic system degradation, such as a facility exploding, is minimized. Solutions may vary depending on the type of space system in question (single or constellation, for instance), but they generally rely on operators having identified key issues in the CSI functioning which may accelerate service degradation.

Key for CI resilience is also the management of margins, where operators do not just evaluate risks, but also acknowledge them when they occur, as they erode the system margins which allow a still acceptable level of functioning above the critical threshold for rapid system degradation. Systems are tested for their capacity to remain within safe operational margins, and operators use proactive indicators to measure the state of the system's margins. Such a principle may appear less applicable to space systems but one may find examples, such as the management of fuel for station keeping in the backdrop of the need to maneuver to avoid impact with debris, but also to maximize system lifespan and minimize debris creation upon mission end.

For CSIP efforts to work as a collective endeavor, they require common mental modes among the various categories of active stakeholders and *system governors*. The OOs must be able to communicate not only among themselves but also with the OOs of CI dependent on CSI and with the sectoral authorities and overall authorities, as well as the growing layer of global stakeholders, such as international institutions. This is an effective way to prevent accidents, mitigate their effects, and assimilate lessons from various disruptions.

Resilient systems are also flexible and redundant. The former is less applicable to space systems, which are generally path dependent on the specific architecture of the system in question, but flexible systems are also open to incremental improvements and improvisations, which are possible in the realm of cybersecurity, among others. The latter principle of resilience, redundancy, is also problematic with regard to the space component of a CSI, though it may be applicable elsewhere. Having reserves and multiple systems running in parallel are workable ideas, but one should remember that redundancy is also another source of complexity, which is a source of risks such as common cause failures. Diversity of systems, as a subset of flexibility, is also an option.

The issue of complexity is a permanent concern for CIP efforts, as its rise obscures interactions between systems that may result in new risks, vulnerabilities, and threats or paths for cascading disruptions. The reduction of complexity is, therefore, a common security concern, though it often develops into the management of the growth rate of complexity, since the prioritization of economic growth, efficiency, and development is a leading cause of complexity buildup. Space systems

are also subject to this "iron law," with systemic trends indicating that complexity will increase in the CSI operating environment through the rise in new systems, the rise in orbital crowdedness, the growing number of interactions between systems and system components, and, last, but not the least, the growing complexity of the individual assets themselves, which are on their way to integrating AI, blockchain, and other developments. An often-overlooked source of complexity when it comes to technological assets is also the organization behind its operation. Generally, a system becomes less complex as it reduces the possibility of feedback loops, as it segregates functions and creates direct lines of information with unique pathways for each.

Under these conditions, the most that CSIP practitioners may hope for is the reduction in system couplings, or the rate of transmission of disruption from one system or system component to another. For instance, fossil fuel-based power generation facilities may reduce their coupling with the mining asset or the transport infrastructure by having reserves on hand, granting autonomy during the initial phases of a crisis. With regard to CSI, we may consider reducing the rate of propagation of cyber threats, but other examples are possible. Overall, systems that reduce couplings are flexible in their operating manner and in the resources they use, and they have delayed or non-sequential functioning compared to their upstream CI influencers.

Johnson and Gheorghe (2013) added two more principles for resilience. The first is the reduction in system fragility, which is an endogenous factor in the system, and the opposite of vulnerability, which is an exogenous factor affecting the system. One may find many instances in the functioning of a CSI which may be assimilated to a state of fragility, but an often-overlooked factor is the organization of the OOs and, for instance, their financial vulnerabilities, cost structures, openness to subversion from abroad, etc.

The second, drawing from the financial sector, is the concept of anti-fragility, which is the quality of a system to be strengthened by the repeated application of small stressors. The classic example is of a forest experiencing regular small fires and then ceasing to do so, following human intervention. The accumulation of plant matter makes the inevitable future fire much more dangerous and stronger when compared to the strength of the smaller, regular fires. We may argue that this quality is also present in space systems, whose challenging security environment has led prospective developers toward increased robustness, within the financial and mass constraints of the launch systems. Baker et al. (2008) have noted that the various coronal mass ejections and other space weather phenomena that have been analyzed do not compare to the potential of the largest solar storm ever recorded (the Carrington Event – 1859), but they are sufficient to produce damage both in orbital and ground-based assets. However, no episode has, so far, been an existential threat, and this has also spurred research into hardening systems and into the development of early warning systems and mitigation measures. The system, overall, becomes stronger than it would have been under ideal conditions, when a Carrington Event-level solar storm would have much graver consequences (Hapgood and Thomson 2010).

Complex System Governance

As mentioned in the description of the CIP framework, CSG is an emerging field at the intersection of several disciplines that has the potential to resolve some of the issues inherent in the manner in which the governance of space systems has developed over time –piecemeal and self-organized, based on gradual accumulation. This organic development is sometimes satisfactory, but it often leaves important gaps in the space governance framework which CSG is uniquely positioned to address. According to Keating et al. (2014), CSG is the design, execution, and evolution of the metasystem functions necessary to provide control, communication, coordination, and integration of a complex system. Metasystems "are sets of related functions which only specify 'what' must be achieved for continuing system viability (existence), not specifying 'how' those functions are to be achieved" (Keating and Katina 2016). These include system identity, system context, strategic system monitoring, system development, learning and transformation, environmental scanning, system operations, operational performance, information, and communications. It is beyond the scope of this chapter to engage in detailed explanations of the underpinning of CSG, but it suffices to say that CSG focuses on system viability and purposeful design in that direction, through a loop of system analysis (*initialization*), readiness levels assessment, and governance development (Keating and Bradley 2015).

In the absence of a purposeful design, Georgescu et al. (2019, p. 323) diagnose the existence of *system drift*, a state in which the system accrues unintended consequences. These consequences are also the result of the emergent behaviors and phenomena of the system which could not necessarily have been anticipated from the analysis of its individual components. The deviations from healthy system conditions are termed "pathologies" (Keating and Katina (2016) mentioned 53 identified pathologies), and they result from a violation of one or more of the metasystem functions. They degrade system functioning to the point where viability becomes in doubt. Identifying these pathologies and resolving them is necessary for system health.

From a CSG perspective, the governance of CSIP has four key issues. The first is the increased complexity in design, execution, and development. The second and third are the importance of including a wide range of considerations from multiple fields in the development process while maintaining a design which offers direction, oversight, and accountability. Lastly, the stakeholders involved should have different worldviews and must participate voluntarily.

Many of the challenges in Fig. 2 will be present in the complex system represented by the space infrastructures and the interactions with their environment or the wider system-of-systems in which space infrastructures are embedded.

From the perspective of CSG, its application to CSI starts with the clarification and structuring of the problem matter around critical systemic issues from across the spectrum of relevant problems, from political to economic and strategic. It continues by mapping the CSI governance metasystem, with its contexts and the various interrelationships, which will allow for the discovery of profound systemic problems

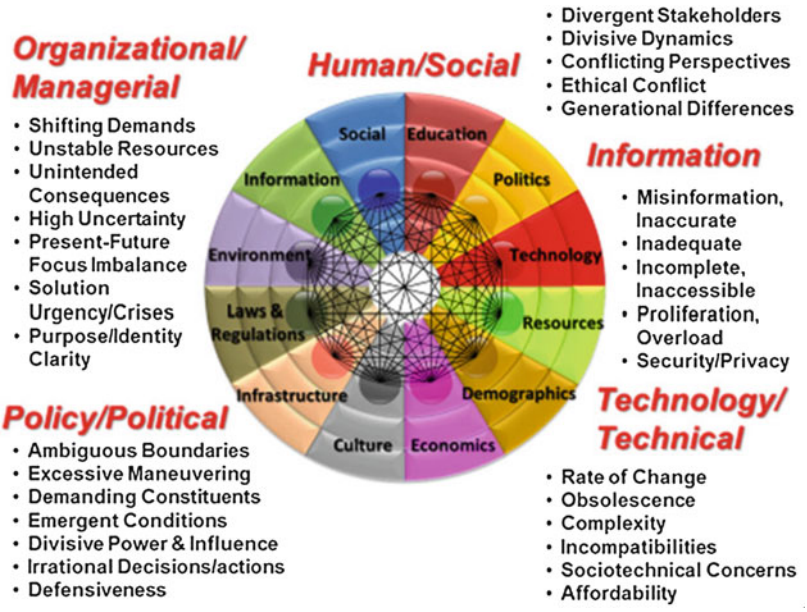

Fig. 2 The complex system problem domain and its five challenge fields for practitioners (Georgescu et al. 2019, p. 322)

once the practitioner has applied different CSG-specific methods and tools. These steps are done through extensive modeling and simulation, which relies on the systematic disassembly of the issues in the initial stage. Since "the map is not the territory," we must be careful with the biases and mistakes of our base definitions and functions. Following this, governance options can be formulated, designed, modeled, and tested before execution in the real world where they will hopefully increase system viability.

For instance, one important issue that affects the viability of the CSI complex system is the issue of space debris. The inadequate development of space governance in this field has led to a "tragedy of the commons" type situation, where a critical asset and resource (orbital bands) is steadily deteriorating. The risks of collision in these areas become ever higher (Salter 2015) and inflict steadily higher damages on the collective of users and possibly triggering also a cascading collision event once past a certain critical threshold (the so-called Kessler syndrome). This is a governance failure because system viability is imperiled and the makeup of the governance structure does not incentivize self-restraint in the creation of debris; does not punish the act of polluting, even deliberate pollution as part of anti-satellite weapon tests; and does not foster the financial preconditions for designing and deploying debris cleanup measures.

Following the CSG process outlined above, we might find something similar to the system briefly outlined in the previous section, where financial incentives are created for sustainable behavior, or something else entirely.

Conclusions

Over the course of this chapter, we have argued in favor of space systems as a new CI category and the potentially significant security benefits stemming from the application of the CIP framework in order to increase the resilience of CSI and of the societies which are critically dependent on them.

The significant advantage of the CIP framework is that it is already a debated and developed field, with significant impact on security policy and the legislative/administrative frameworks for security in the United States, the European Union Member States (as well as the EU itself), and other countries. Extending it to the space environment has the potential to improve security outcomes and to address some of the gaps stemming from the organic development of the space security governance framework under the unique conditions of the space security environment. Critical Infrastructure Protection provides a comprehensive framework for the management of key infrastructures, assets, and resources on which individual countries or the global community depends. Since space systems are already an acknowledged component of the existing critical infrastructure domains, the CSI concept is a natural outgrowth.

To sum up, the CIP framework provides tools and concepts with which to analyze space security and describe the relationships formed with terrestrial infrastructures. It is also a gateway to an extant governance framework which is in use at American and European levels, both for individual nations and collectively. It also provides a coherent vision for a holistic understanding of security, in which space security is not cordoned off into its own field, but is integrated in the wider security domain as befits the reality of the complexity of the critical infrastructure system-of-systems. The CIP framework has been working toward alleviating the impact of trends in terrestrial CI which are also present among space systems, most notably the growing rate of ownership by private entities of prospective CSI, but also the potential of counterspace operations within the hybrid warfare becoming the new normal among rival states (Robinson et al. 2019). In addition, the recent developments in the CIP field, such as complex system governance, are also applicable to CSI.

For these reasons, the concept of CSI and all that derives from it provides a useful perspective and roadmap for improving space security or at least mitigating the security impact of current space sector dynamics.

References

Air Force Space Command (2019) The Future of Space 2060 and Implications for U.S. Strategy: Report on the Space Futures Workshop, 5th, Sept 2019. http://www.spaceref.com/news/viewsr.html?pid=52822

Baker D, Balstad R, Bodeau JM, Cameron E, Fennell JF, Fisher GM, Forbes K, Kintner P, Leffler L, Lewis W, Reagan J, Small A, Stansell T, Strachan LS (2008) Space Weather Events – Understanding Societal and Economic Impacts: A Workshop Report, Space Studies Board,

National Research Council, ISBN 10: 978–0–309-13811-6, available online at http://lasp.colorado.edu/home/wp-content/uploads/2011/07/lowres-Severe-Space-Weather-FINAL.pdf

Bryce Space and Technology (2019) Smallsats by the numbers 2019, [Online] Available at https://brycetech.com/downloads/Bryce_Smallsats_2019.pdf

Bucovețchi O, Georgescu A, Badea D, Stanciu RD (2019) Agent-based Modeling (ABM): support for emphasizing the air transport infrastructure dependence of Space systems. Sustainability 11 (19):5331

Cellucci T (2018) Perspective: Innovative Public-Private Partnerships Help Secure Critical Infrastructure, published by the National Security Today, 27 Nov 2018. https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-innovative-public-private-partnerships-accelerate-technology-and-secure-critical-infrastructure/

Department of Defense, Office of the Director of National Intelligence (2011) National Security Space Strategy Unclassified Summary. Washington DC, https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2011/item/620-national-security-space-strategy

European Commission (2008) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

Eusgeld I, Nan C, Dietz S (2011) "System-of-systems" approach for interdependent critical infrastructures. Reliab Eng Syst Saf 96(6):679–686. https://doi.org/10.1016/j.ress.2010.12.010

Georgescu A, Gheorghe A, Piso M-I, Katina PF (2019) "Critical Space infrastructures: risk, resilience and complexity", topics in safety, risk, reliability and quality, series 36, eBook ISBN 978-3-030-12604-9. https://doi.org/10.1007/978-3-030-12604-9. Springer International Publishing

Gheorghe A, Schläpfer M (2006) Critical infrastructures: ubiquity of digitalization and risks of interdependent critical infrastructures, *Systems Man and Cybernetics 2006*. SMC '06. IEEE international conference, vol 1, pp 580–584

Gheorghe AV, Vamanu DV, Katina PF, Pulfer R (2018) Critical infrastructures, key resources, key assets. Risk, vulnerability, resilience, fragility, and perception governance, topics in safety, risk, reliability and quality, series 34, eBook ISBN 978-3-319-69224-1. https://doi.org/10.1007/978-3-319-69224-1. Springer International Publishing

Hapgood M, Thomson A (2010) Space weather. Its impact on earth and implications for business, Lloyd's 360 risk insight briefing, available online at https://www.lloyds.com/~/media/lloyds/reports/360/360-space-weather/7311_lloyds_360_space-weather_03.pdf

Heino O, Takala A, Jukarainen P, Kalalahti J, Kekki T, Verho P (2019) Critical infrastructures: the operational environment in cases of severe disruption. Sustainability 11(3):838. https://doi.org/10.3390/su11030838

Helbing D (2013) Globally networked risks and how to respond. Nature 497(7447):51–59. https://doi.org/10.1038/nature12047

Johnsen S (2010) Resilience in risk analysis and risk assessment. In: Moore T, Shenoi S (eds) Critical infrastructure protection IV – fourth annual IFIP WG 11.10 international conference on critical infrastructure protection. IFIP Advances in Information and Communication Technology series (311), p. 215–227. Washington DC, SUA: Springer, ISBN 978-3-642-16806-2

Johnson J, Gheorghe G (2013) Antifragility Analysis and measurement framework for systems of systems. Int J Disaster Risk Sci 4(4):159–168

Jonkeren O, Ward D, Dorneanu B, Giannopoulos G (2012) Economic impact assessment of critical infrastructure failure in the EU: a combined systems engineering – inoperability input-output model, Joint Research Centre, 20th international input-output conference, Bratislava. https://www.semanticscholar.org/paper/Economic-impact-assessment-of-Critical-failure-in-A-Jonkeren-Ward/8682d0ef992243115196a66651f3d86483e37b3d

Keating CB, Bradley JM (2015) Complex system governance reference model. Int J Syst Syst Eng 6 (1/2):33. https://doi.org/10.1504/ijsse.2015.068811

Keating CB, Katina PF (2016) Complex system governance development: a first generation methodology. Int J Syst Syst Eng 7(1/2/3):43–74. https://doi.org/10.1504/ijsse.2016.076127

Keating CB, Katina PF, Bradley JM (2014) Complex system governance: concept, challenges, and emerging research. Int J Syst Syst Eng 5(3):263–288

Linkov I, Bridges T, Creutzig F, Decker J, Fox-lent C et al (2014) Changing the resilience paradigm. Nat Clim Chang 4:407–409

Niederstrasser C (2018) Small launch vehicles – a 2018 state of the industry survey, SSC18-IX-01, 32nd Annual AIAA/USU conference on small satellites, Northrop Grumman Corporation, publisher: Utah State University Research Foundation (USURF). https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=4118&context=smallsat

OECD (2016) Space and innovation. OECD Publishing, Paris. https://doi.org/10.1787/9789264264014-en

OECD (2019) The Space economy in figures: how Space contributes to the global economy. OECD Publishing, Paris, available at https://doi.org/10.1787/c5996201-en

Perrow C (1999) Normal accidents: living with high-risk technologies. Princeton University Press. isbn:9781400828494

Pescaroli G, Alexander D (2016) Critical infrastructure, panarchies and the vulnerability paths of cascading disasters. Nat Hazards 82(1):175–192. https://doi.org/10.1007/s11069-016-2186-3

Robinson J, Robinson R, Davenport A, Kupkova T, Martinek P, Emmerling S, Marzorati A (2019) State Actor Strategies in Attracting Space Sector Partnerships: Chinese and Russian Economic and Financial Footprints, Prague Security Studies Institute, Prague, available online at: http://www.pssi.cz/download/docs/686_executive-summary.pdf

Rockefeller Foundation, Arup Development Group (2014) The City Resilience Index. https://www.arup.com/perspectives/themes/cities/city-resilience-index

Royal Academy of Engineering (2013) Extreme space weather: impacts on engineered systems and infrastructure, ISBN 1-903496-95-0, designated (RAENG, 2013), available at http://www.raeng.org.uk/publications/reports/space-weather-full-report

Salter AW (2015) Space debris – a law and economics analysis of the orbital commons, Mercatus Center, George Mason University, USA, available at https://www.mercatus.org/system/files/Salter-Space-Debris.pdf

Setola R, Luiijf E, Teocharidou M (2017) Critical infrastructures, protection and resilience. In: Setola R, Rosato V, Kyriakides E, Rome E (eds) Managing the complexity of critical infrastructures: a modelling and simulation approach. Studies in systems, decision and control, vol 90. Springer open, ISBN: 978-3-319-51042-2/978-3-319-51043-9, https://doi.org/10.1007/978-3-319-51043-9

The White House (1998) Presidential Decision Directive/NSC-63 (as PDD-63), Washington DC. https://clinton.presidentiallibraries.us/items/show/12762

Union of Concerned Scientists (2019) UCS Satellite Database, accessed 12 Oct 2019. https://www.ucsusa.org/resources/satellite-database

Vugrin E, Wahren D, Ehlen M (2011) A resilience assessment framework for infrastructure and economic systems: quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane. Process Saf Prog 30(3):280–290. https://doi.org/10.1002/prs.10437