2018

New Dimensions for a Challenging Security Environment: Growing Exposure to Critical Space Infrastructure Disruption Risk

Adrian V. Gheorghe
Old Dominion University

Alexandru Georgescu

Olga Bucovetchi

Marilena Lazăr

Cezar Scarlat

Original Publication Citation

Gheorghe, A. V., Georgescu, A., Bucovețchi, O., Lazăr, M., & Scarlat, C. (2018). New dimensions for a challenging security environment: Growing exposure to critical space infrastructure disruption risk. *International Journal of Disaster Risk Science*. doi:10.1007/s13753-018-0197-2

Int J Disaster Risk Sci
https://doi.org/10.1007/s13753-018-0197-2

www.ijdrs.com
www.springer.com/13753

SHORT ARTICLE

New Dimensions for a Challenging Security Environment: Growing Exposure to Critical Space Infrastructure Disruption Risk

Adrian V. Gheorghe[1] · Alexandru Georgescu[2] · Olga Bucovețchi[2,3] · Marilena Lazăr[4] · Cezar Scarlat[3]

Abstract Space systems have become a key enabler for a wide variety of applications that are vital to the functioning of advanced societies. The trend is one of quantitative and qualitative increase of this dependence, so much so that space systems have been described as a new example of critical infrastructure. This article argues that the existence of critical space infrastructures implies the emergence of a new category of disasters related to disruption risks. We inventory those risks and make policy recommendations for what is, ultimately, a resilience governance issue.

Keywords Complex systems · Infrastructure disruption · Resilience governance · Space infrastructure · System interdependencies

1 Introduction

Certain categories of space systems, mainly satellites orbiting the Earth at various altitudes, have become components of critical infrastructures and critical infrastructure system-of-systems. They have done so through their capacity for the provision of unique services or of services that are difficult to substitute sustainably through non-space alternatives. These services are varied and include, in a rough breakdown, capabilities related to Earth observation, communications, command, control, and coordination, as well as navigation, positioning, and timing. Their applications are many and varied—from weather observations to data collection, from coordinating global supply chains to maintaining integrity for complex electricity grids or global databases. The users are numerous and, through interdependencies, the ultimate beneficiaries extend throughout the world, impacting individuals, businesses, and nations. Table 1 describes the applications of just one type of space system, a Global Navigation Satellite System (GNSS) constellation.

Mureşan et al. (2016) argued that space systems are a new type of critical infrastructure (CI), not just a distinct component of the CI categories identified in the legislative and administrative frameworks for critical infrastructure protection (CIP) developed in the United States or the European Union. This inclusion offers a toolbox for conceptualizing critical space infrastructures (CSI) in the wider system-of-systems, thereby establishing the premise for actual resilience governance efforts, keeping in mind two key criteria on which CIP theory is based:

- The scarcity of resources—material, computational, and organizational—to dedicate to the protection of infrastructures, thereby establishing the need for a methodology of assessing criticality and a framework for designating systems for protection;

✉ Adrian V. Gheorghe
AGheorgh@odu.edu

[1] Department of Engineering Management and Systems Engineering, Old Dominion University, Norfolk, VA 23529, USA

[2] Romanian Association for Space Technology and Industry (ROMSPACE), 061126 Bucharest, Romania

[3] University Politehnica of Bucharest, 060042 Bucharest, Romania

[4] Military Equipment and Technologies Research Agency of the Romanian Ministry of Defense (METRA), 077025 Clinceni, Ilfov County, Romania

Published online: 05 December 2018

Table 1 Generic applications stemming from GNSS capabilities

Space system category	Capability	Application examples
GNSS	Navigation	Road, air, maritime transport
	Positioning	Transport and general logistics (package tracking), precision agriculture
	Timing	Electricity grid operation, database synchronization, transaction dating and ordering in queues

- The interdependencies of CI, which lead to the propagation of risks, vulnerabilities, and threats (Georgescu and Bucovețchi 2017).

These interdependencies, according to Gheorghe and Schläpfer (2004), manifest through physical, cyber, geographical, and logical links. This means that, while there is an ample debate surrounding the resilience of CI, an all-hazards approach to CIP requires us to look at the risks stemming from expanding and deepening dependencies on CSI, which are easily transmissible through cyber and logical links. Mureșan et al. (2016) specifically dealt with critical energy infrastructure dependencies on space systems. The urgency of the inclusion of CSI into our calculus for dealing with crisis and emergency situations stems from the basic literature on CIP, which holds that a complex system-of-systems is subject to cascading failures (serial infrastructure disruption), escalating failures (the severity of disruption increases with mounting feedback loops), and common cause failures (multiple infrastructures fail from the same origin point; Rinaldi et al. 2001), thereby enhancing system impact.

As Mureșan and Georgescu (2015) noted, space systems operate in one of the most challenging environments known and accessible to man. They are subject not only to manifestations of specific space phenomena, such as space weather and orbital debris impact, but also to the general harshness of their environment, in which temperatures, radiation, and other normal factors generate a high probability of spontaneous malfunction. At the same time, there are deliberate threats to space systems, facilitated by specific weaknesses and by an evolving international landscape of space actors, including not just rational states, but also rogue states and non-state actors with various levels of access to increasingly facile antisatellite weaponry (Gheorghe and Vamanu 2007).

This article briefly sketches three risks—space debris, space weather, deliberate threats—and formulates policy recommendations to address the wider challenges of resilience governance in the "orbital commons."

2 Space Debris

Space debris (Table 2) encompasses the natural and artificial fragments of varying sizes that, given orbital velocities, may damage or destroy space systems through impact. According to ESA (2018), of the 8650 satellites placed in space by 5400 launches since the dawn of manned exploration of space with the launch of Sputnik, 4700 were still present and 1800 were active systems by January 2018. The Space Surveillance Network tracks around 21,000 debris objects, with statistical models predicting the existence of the 29,000 objects over 10 cm, 750,000 from 1 cm to 10 cm, and 166 million objects from 1 mm to 1 cm (ESA 2018). Despite growing awareness of the issue and the progress on measures dedicated to limiting debris production (better shielding, better launch protocols, better end-of-life management for systems including reentry; Georgescu et al. 2016b), there are no means for cleaning up existing debris.

Salter (2015) estimated that there are 6100 tons of debris in orbit, with 2300 in low earth orbit (LEO). While space is one of the least regenerative environments known to man, LEO has, according to UCS (2017; Table 2), good reentry times for debris. However, due to ease of access and the high number of applications for space systems placed in that particular band, it is also a favorite for megaconstellation projects such as those envisioned by SpaceX or Facebook, which would severely increase the issues. Collisions between whole space systems are not unheard of.

3 Space Weather

Space weather phenomena encompass the conditions produced by the Sun or present in the ambient space environment, including radiation or charged particles, which may impact the functioning of space systems and, depending on severity, of Earth-based systems. Communications may be jammed, or equipment damaged and destroyed. Affected areas of human activity include the functioning of various satellites, manned spaceflight, but also terrestrial effects in communications, electricity grid operation, and even the safety of pipelines through subversion of anticorrosion mechanisms.

Table 2 Various statistics regarding space debris

Origin of debris (NASA 2014)	42% from space system disintegration
	22% as whole, but nonfunctioning, space systems
	19% from mission specific activities
	17% debris from launchers
Percentage of satellites in each major orbit category (UCS 2017)	49% in Low Earth Orbit (LEO)
	6% in medium orbit
	41% in geosynchronous orbit
	4% in other orbits, including elliptical orbits
Reentry time for debris (NASA 2008)	A few days, at lower than 125 miles altitude
	A few years in the 125–370 miles altitude band
	A few centuries, above 500 miles
	Going towards geosynchronous orbits, persistence times are so high that one can speak of permanent orbital presence
Countries of origin for debris (Kovalenko 2014)	China 40%
	USA 27.5%
	Russian Federation 25.5%

Source Georgescu (2017)

There is a significant literature attesting to the effects that extreme space weather phenomena may have on global society or on individual nations, as well as providing analyses of the impact of past solar storm activity in particular. Baker et al. (2011) linked a vulnerable, aging, and centralized US electricity grid to USD 2 trillion in damages in the first year for the United States alone in case of a solar storm comparable to the largest ever recorded, and recovery times between 4 and 10 years. This does not include the impact of disruption elsewhere, such as in Europe, or resulting losses to the United States. The number of US consumers that would be left without electricity would approach 130 million (Baker et al. 2011).

As with space debris, there are technological means to counteract the effects of space weather on individual systems—through shielding and resilient design, but these inflict costs that many actors seek to avoid, absent enforceable obligations or other stimuli—and also to handle primary risk, leaving the transmitted risk from other sources intact (Georgescu et al. 2016a).

4 Deliberate Threats

Deliberate threats to space systems are numerous, diverse, and highly efficient. They are reliant on specific weaknesses of space systems, which include not only the individual space asset, but also the communication links, the control center, and the ties to other satellites in its constellation. According to Georgescu et al. (2015a), a taxonomy of antisatellite weaponry would consist of the following categories:

- Cybernetic attacks;
- Laser attacks;
- Signal jamming;
- Kinetic attacks with missiles;
- Electromagnetic attacks;
- De-orbiting by attacking with maneuver satellites;
- Passive attacks, by "mining" the space where that system orbits.

A number of state actors have developed antisatellite (ASAT) capabilities. While the public imagination is overcome with the idea of high-tech, antisatellite weaponry, such as lasers and interceptors fired from fighter planes, the truth is that ASAT capabilities are within the grasp of non-state actors of low sophistication and resources. As Gheorghe and Vamanu (2007) noted, an assailant with a laptop can make what he wants of a satellite, including veer it off course or compromise its functioning in some other way. The cost-to-benefit ratio of cyberattacks is very much in favor of the attacker, who requires only a skilled individual with basic equipment and an Internet connection. The difficulty in attributing an attack as well as the low cost of failure makes this option even more attractive. Other assailants may focus on jamming the communication between the control center and the satellite using off-the-shelf parts, and low-powered lasers can be used to temporarily blind satellites passing above an area that must be kept concealed.

The threats evolve to meet the constraints facing attackers with fewer resources. Given the significant

interdependencies of states utilizing the same space systems or orbital lanes for their critical space service consumption requirements, as well as the possibility of retaliation, there is a notable logic of "mutually assured destruction" in space warfare that deters outright hostilities.

There are also significant factors that increase the vulnerability of space systems to deliberate threats (Georgescu et al. 2015a):

- The predictability of CSI trajectory;
- The orbital dynamics of CSI relative to various regions of Earth;
- The difficulty of CSI replacement, in terms of costs, effort, and time;
- The efficiency of these attacks;
- The extraordinary cost–benefit ratios that some means of attack offer;
- The lack of restraining concerns on the part of non-state actors who do not care about retaliation in kind or the wide disruption of critical space services.

5 Specific Challenges to Governance

Having described the three main threats to space systems, we are now faced with the issue of tying these into a coherent framework of thought that provides for resilience governance. Resilience is the ability of a society or of a system to recover from the materialization of a negative event with minimum damage, in as little time as possible and with as much of its original functionality as possible. Governance relates not just to decision making, but also to the tools, mechanisms, organizations, and mental modes that influence that decision making.

Space systems in general and CSI, in particular, are also contributors to resilience governance and to the crisis and emergency situation management, providing valuable services such as data gathering, communication, and coordination for other disasters, thereby increasing the circumstantial criticality of space systems (Georgescu and Bucovețchi 2017). Critical space infrastructure integrates not just critical infrastructure, but also key assets and key resources (such as the orbital bands the assets inhabit; Gheorghe et al. 2018). As a subject and an object of crisis and emergency situation management, CSI provides a key to understanding one mechanism for crisis escalation, since CSI failure may lead to a common cause failure both of a series of infrastructures, as well as the capacity of the competent actors to manage the crisis, thereby enabling its escalation.

Governance is difficult in the space environment, since its "international" character lacks the clear jurisdictional boundaries that inform CIP processes on Earth. The emerging jurisdictional issue of transcontinental infrastructure protection (pipelines, trade routes, and so on), illustrates the inherent problem of CSI protection. The existing space governance framework, painstakingly built over decades, is geared towards consensus, making it unsuited for collective action. Without the ability to enforce technical standards, punish their violation, and extract the cost of externalities from the perpetrators through clear and enforceable assignment of liability, the "global commons" begins to suffer from a variant of the "tragedy of the commons." Polluters may continue to do so while sharing risks with nonpolluters. The material advantages stemming from underinvestment in system robustness confers an advantage that incentivizes a race to the bottom in terms of security investment and the maintenance of redundant capacity. And, overall, there is no clear body or a body of law for solving the disputes that inevitably arise not just between states, but between private parties. More and more of the identifiable CSI are owned, operated, and administered by private entities, increasingly mirroring the state of critical infrastructure in the West, where 70–75% of CI are in private hands. Specific developments in the space industry lower the barriers of access to space, inevitably promoting non-state involvement in space by universities, private businesses, and others.

The literature in the field underscores the lack of preparedness of competent authorities and infrastructure operators during the materialization of phenomena like space weather. A crisis of capacity could easily be triggered in the space system-of-systems and transcends geographic or jurisdictional boundaries, making responses that much more difficult. They involve coordination and acting under incomplete information, not just situational, but also with regard to the actions of peer responders, compounding the issues stemming from a crisis and hindering efforts at breaking the chain of cascading disruption and returning to normality.

For this reason, we make the following policy prescriptions, based on issues of governance. Firstly, the main space actors must agree on key resilience measures, implement them and enforce them unilaterally on third parties, such as corporations or other states. This is especially important, since not only are more states trying to access space, but this may also encourage jurisdiction shopping on the part of established corporate space actors. The current UN body, the Committee on the Peaceful Uses of Outer Space (COPUOS), should be invested with the authority to monitor and recommend sanctions, since it already has policy-making and technical capacities.

Secondly, it is important to focus on changing the incentive structure and, therefore, the behavior, of private entities engaged in space, since the lion's share of CSI expansion will likely be a result of private development. Gheorghe and Yuchnovicz (2015) proposed a space vulnerability cadaster as a representation of risk to space systems that would be legible to private companies, banks, and insurance companies. Insurance premiums could favor companies that invest in shielding, or whose systems operate in, low-debris density orbits. Georgescu (2017) fits this proposal into a market governance model for space systems, which complements the state-driven models identified for the United States and the European Union by Akhtar et al. (2017). A market governance model provides an incentive structure for emergent behavior on the part of rational actors seeking to maximize utility. With such incentives in place, actors will find themselves more likely to consider the costs of compliance with standards and norms in a positive light, since it leads to indirect benefits from third parties basing a financially relevant assessment of that actor on security, as well as avoiding penalties.

Thirdly, it is vital to invest in measures that ensure a more coherent space environment, to enable states and companies to substitute one space system for another in terms of short-term provisioning of critical space services. This requires interoperability of systems and clear lines of communication, as well as preexisting agreements to more easily enable the system-of-systems to bring its extra capacity into play. Useful examples in this sense are the International Disaster Charter and Sentinel Asia initiatives, which focus on providing critical space capabilities in crisis situations. Georgescu et al. (2015b) recounted that, during the 2011 Fukushima Daiichi nuclear disaster, Japan was also faced with the spontaneous loss of its main Earth observation platform, Advanced Land Observation Satellite (ALOS), which was quickly mitigated by partner nations with their respective assets. Such ease of cooperation must be generalized, in order to ensure timely access to various resources. This should take place under the auspices of an existing and legitimate international organization or forum, whose remit would simply be expanded.

6 Conclusion

Space systems are an unalienable component of high-functioning system-of-systems, providing critical services for geographically and functionally expansive critical infrastructure systems, while also becoming critical infrastructures in themselves. This increasing dependence generates new risks, vulnerabilities, and threats, as well as new horizons for the scope of cascading disruption of critical infrastructures. The specificities of the orbital environment demand collective action to manage the new risks, which action is beyond the possibility of the current system of space governance. Therefore, after presenting the key specific threats to space systems, we advance proposals for the resilience governance of these systems and, specifically, of those designated critical space infrastructures.

Acknowledgements The findings presented in this article are based on a research project—"Software applications for modelling critical infrastructure dependency on space systems"—undertaken by the Romanian Association for Space Industry and Technology with the Military Equipment and Technologies Research Agency of the Romanian Ministry of Defense. The work was supported by a grant of the Program for Research, Development and Innovation for Space Technology and Advanced Research (STAR) administered by the Romanian Space Agency, project number 191/2017. A principal beneficiary of the project results is the SCIPRO Center—Space Critical Infrastructure Protection at the Romanian Space Agency.

References

Akhtar, F., S. Farthing, G. Greendyk, E. Hirwa, and E. Mast. 2017. A multi-criteria decision analysis of the problem: Establishing governance for critical space infrastructure. Norfolk, USA: Engineering Management and Systems Engineering Department, Old Dominion University.

Baker, D., R. Balstad, J.M. Bodeau, E. Cameron, J.F. Fennell, G.M. Fisher, K.F. Forbes, P.M. Kintner, et al. 2011. *Severe space weather events: Understanding societal and economic impacts*. Washington, DC: National Academies Press.

ESA (European Space Agency). 2018. Space debris by the numbers. http://www.esa.int/Our_Activities/Operations/Space_Debris/Space_debris_-_by_the_numbers. Accessed 8 Aug 2018.

Georgescu, A. 2017. Risk engineering in critical infrastructure protection—Applications to space systems. Ph.D. thesis. Bucharest, Romania: Bucharest Polytechnic University (in Romanian).

Georgescu, A., and O. Bucovețchi. 2017. A generic flow based model for understanding critical infrastructure dependency on space systems. In *Proceedings of the 29th international business information management association conference*, 3–4 May 2017, Vienna, Austria.

Georgescu, A., U.E. Botezatu, Ş.C. Arseni, A. Barbu, and L. Boiangiu. 2015. Deliberate threats to critical space infrastructure—ASAT and the strategic context. *Scientific Bulletin of Naval Academy* 18(2): 419–427. https://www.anmb.ro/buletinstiintific/buletine/2016_Issue2/FCS/419-427.pdf. Accessed 17 Nov 2018.

Georgescu, A., U.E. Botezatu, A.D. Popa, and Ş.C. Arseni. 2016. The threat of space weather to critical terrestrial and space infrastructure systems. *Technical Military Journal* 15(1): 44–53.

Georgescu, A., I. Jivănescu, Ş. Popa, and Ş.C. Arseni. 2015. Space capabilities—Assessing their criticality as a tool in nuclear governance. *Technical Military Journal* 14(1): 20–29.

Georgescu, A., A.D. Popa, Ş.C. Arseni, and A.C. Sava. 2016. An overview of the space debris threat to critical space infrastructures. *MTA Review* 26(1): 81–96.

Gheorghe AV, Schläpfer M (2006) Ubiquity of digitalization and risks of interdependent critical infrastructures. In *Proceedings of IEEE international conference on systems, man and cybernetics*, 8–11 October 2006, Taipei, Taiwan, China, 580–584.

Gheorghe, A.V., and D.V. Vamanu. 2007. Risk and vulnerability games: The anti-satellite weaponry. *International Journal of Critical Infrastructures* 3(3–4): 457–470.

Gheorghe, A.V., and D. Yuchnovicz. 2015. The space infrastructure vulnerability cadastre: Orbital debris critical loads. *International Journal of Disaster Risk Science* 6(4): 359–371.

Gheorghe, A.V., D.V. Vamanu, P.F. Katina, and R. Pulfer. 2018. *Critical infrastructure, key resources, key assets: Risk, vulnerability, resilience, fragility, and perception governance.* Switzerland: Springer.

Kovalenko, N. 2014. Space junk endangers mankind's usual course of life. http://www.spacemart.com/reports/Space_junk_endangers_mankinds_usual_course_of_life_999.html. Accessed 8 Aug 2018.

Mureşan, L., and A. Georgescu. 2015. The road to resilience in 2050. *The Royal United Services Institute Journal* 160(6): 58–66.

Mureşan L., A. Georgescu, I. Jivănescu, S. Popa, and S. Arseni. 2016. Charting critical energy infrastructure dependencies on space systems—New frontiers in risks, vulnerabilities and threats. In *Critical energy infrastructure protection and cyber security policies*, ed. M.H. Caşın, and G. Gluschke, 177–192. 2016. Istanbul, Turkey: Hazar Strateji Enstitüsü.

NASA (National Aeronautics and Space Administration). 2008. *History of on-orbit satellite fragmentations*. 14th edn. Orbital Debris Program Office, NASA/TM2008. https://orbitaldebris.jsc.nasa.gov/library/satellitefraghistory/tm-2008-214779.pdf. Accessed 17 Nov 2018.

NASA (National Aeronautics and Space Administration). 2014. *Monthly number of objects in earth orbit by type. Orbital debris quartely news*. http://orbitaldebris.jsc.nasa.gov/. Accessed 10 Aug 2018.

Rinaldi, S.M., J.P. Peerenboom, T.K. Kelly. 2001. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine* 21(6): 11–25.

Salter, A.W. 2015. *Space debris—A law and economics analysis of the orbital commons*. Mercatus Center, George Mason University. https://www.mercatus.org/system/files/Salter-Space-Debris.pdf. Accessed 17 Nov 2018.

UCS (Union of Concerned Scientists). 2017. Open-source satellite database statistics. http://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database.html#.Vg0BUCvkVTB. Accessed 6 Aug 2018.