A critical space infrastructure perspective on Romanian national security

Olga BUCOVEȚCHI[1], Alexandru GEORGESCU[2], Marilena LAZĂR[3], Carmen CÎRNU[4]

[1] Romanian Association for Space Industry and Technology
[2] Romanian Association for Space Industry and Technology
[3] Equipment and Technologies Research Agency
[4] National Institute for Research and Development in Informatics
alexandrugeorgescu42@yahoo.com, olga.bucovetchi@upb.ro, mlazar@acttm.ro, carmen.cirnu@ici.ro

Abstract: Critical infrastructures are vital sociotechnical systems whose destruction or disruption would have a significant impact on the functioning of society on multiple levels. There is a growing body of literature which argues that space systems are a new category of critical infrastructures, with their own specific traits and exposure to a challenging security environment. This article presents the case for space systems as critical infrastructure and presents the relevance of these concepts to Romanian national security.

Keywords: space systems, critical infrastructures, resilience, national security.

Securitatea națională a României în contextul infrastructurilor critice spațiale

Rezumat: Infrastructurile critice sunt sisteme sociotehnice a căror distrugere sau întrerupere a funcționării ar avea un impact semnificativ asupra funcționării societății pe planuri multiple. Există o literatură științifică din ce în ce mai avansată pe tema sistemelor spațiale ca o nouă categorie de infrastructuri critice, având propriile specificități și expunerea la un mediu de Securitate provocator. Articolul de față prezintă argumentele în favoarea sistemelor spațiale ca infrastructuri critice și prezintă relevanța acestor noi concepte pentru securitatea națională a României.

Cuvinte cheie: sisteme spațiale, infrastructuri critice, reziliență, securitate națională.

Introduction

Space systems have become a key enabler for a wide variety of applications, through capabilities related to command, control and coordination, communication, data gathering, navigation, positioning, timing and others. These capabilities have increase in quality and steadily decreased in price, leading to new applications embraced by numerous beneficiaries on Earth, from individuals to companies running complex global supply chains or distributed databases. The figure below describes the applications of space systems with broad strokes.

Certain space systems end up performing vital functions, especially related to the upper levels of command and control, for critical infrastructure systems and systems-of-systems. Criticality entails that the disruption or destruction of the system would lead to material damages or even human losses, with the possibility of a propagated disruption through a wider system-of-systems based on the interdependencies between critical infrastructures (Katina and Hester, 2013). Critical infrastructures are generally thought of as pipelines, power plants, stock markets or hospitals, in accordance with the taxonomy developed by individual nations and the EU to classify these assets and develop sectorial protection policies. However, space systems have recently begun to be analyzed as critical infrastructures in themselves, not just critical components (Georgescu and Bucovețchi, 2017). This article briefly lists arguments in favor of this assertion and details trends in the field, after which it formulates the impact of critical space infrastructures (CSI) on Romanian National security.

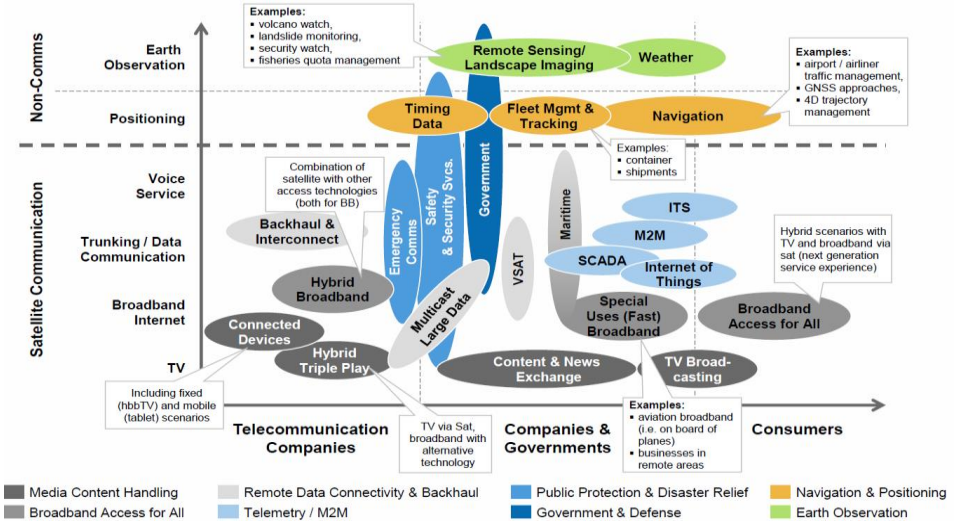

Figure 1. Chart of capabilities of space systems (Acker et al, 2011, pg. 80)

Critical Space Infrastructures

Mureşan et al (2016) argued that CSI are a new category of critical infrastructures, which must be introduced into the general critical infrastructure protection (CIP) framework in order for governance processes to occur, but which must also be approached with important specificities in mind. Chief among these is the nature of the space environment, which resembles a "global orbital commons" where jurisdictional issues are complicated by the geography of orbital trajectories and the issue of ownership and liability. This is also one of the most hazardous environments known to man, with high cost barriers and other difficulties in the way of accessing it, as well as possessing specific factors (radiation, space debris) which may lead to the non-deliberate damaging or destruction of assets. Despite this, the space industry registers yearly growth rates in excess of the global GDP dynamic, with recent technological developments marking the beginning of a what appears to be a boom period. The figure below imparts some statistics regarding the components of the American satellite industry. Prior issues of the report underscored the impact of the maturing cubesat technology on launches, leading to a near doubling of the number of satellites launches over a short period of time.

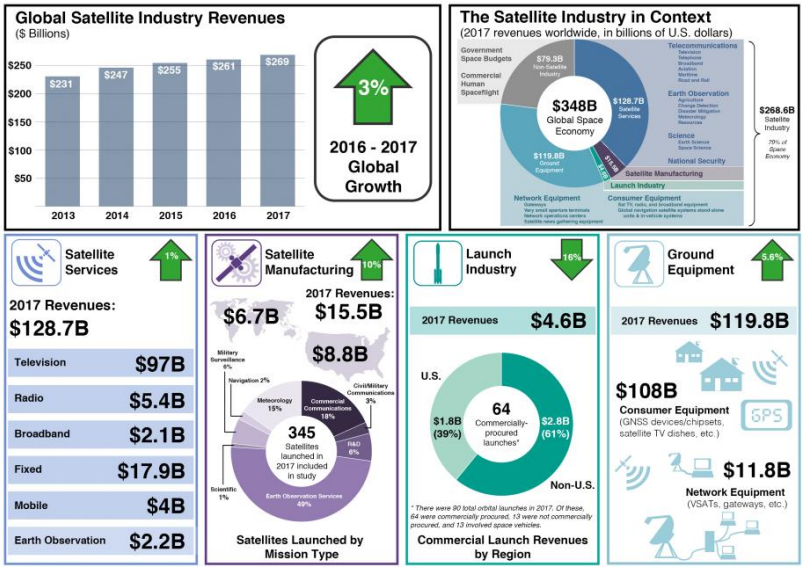

Figure 2. State of the Satellite Industry 2018 Report vital statistics (Bryce, 2018)

The growth of the industry reflects a dynamic which leads to the growth of dependencies on CSI and the modification of the general security environment, as crisis and emergency situation management becomes, itself, dependent on CSI for communication and data gathering. The dependencies are a notable feature of CI in CIP theory, which posits that these pathways, based on geographic, sectorial, logical, informational or cybernetic connection, are a medium for the transmission of risks, vulnerabilities and threats, leading to system-wide breakdowns in complex systems, which requires specific governance methods to address (Katina and Keating, 2015).

CSI are also afflicted by specific threats, of which we mention the collision with space debris, the effects of space weather, and the deliberate threats (anti-satellite weaponry). Unlike other threats to critical infrastructures, these present certain challenges related to the collective coordination to address the issues, prevent free riding and generate a consensus in favor of sustainable exploitation of space. The barriers to CSI protection are technological, financial, but also organizational and diplomatic, with gradual steps towards actual governance being taken slowly, in tandem with the general push for global CIP governance, since other terrestrial infrastructures are also taking on a global scope.

These factors paint CSI as an area of interest to security practitioners, but presenting significant difficulties even for established spacefaring nations, let alone simple space services consumers like Romania and many others.

Romanian exposure to CSI risk

Romania does not, to our knowledge, own and operate any space assets. However, it is wrong to assume that this does not imply a dependence on space systems which could be qualified as critical to the functioning of its society. On the contrary, it would not be too much of an exaggeration to assert that Romania is as severely exposed to critical space infrastructure disruption risk as any spacefaring nation, when controlling for general level of development. It is likely that Romania's exposure is even greater, as, by not owning space assets, it is exposed to the political risks of dependence on the assets of others.

It is difficult to estimate the level of such a dependence. We can infer its existence from a set of pre-existing factors. Firstly, Romania is an upper middle-income country with a relatively widespread availability of modern information and communication capabilities. The technological sophistication of its economy does not compare to that of other European nations, but there are segments which would engender a dependence on space systems. For Romania, the future is already present, but it is not evenly distributed geographically or by economic sector. It has significant commercial ties (and more) with other nations, as well as other close and growing interconnections with a globalizing world in general, and an ever more integrated European Union, in particular. Moreover, Romania is party to numerous organizations, treaties and other agreements which enable it to pursue aspects of its national interest, such as those related to security. For instance, its NATO membership and the requirement of developing its capabilities and its interoperability with other NATO militaries automatically entail a reliance on space systems, with both a permanent and a circumstantial component.

Finally, every indicator of the political preference of the Romanian people and the governing programs of its leadership highlights a path of development which inevitably leads to higher dependence on space systems, through better education, more interconnectedness with the European Union and NATO partners, and growing technological sophistication in order to generate higher added value.

Therefore, there is a case for arguing that Romania is already dependent on critical space infrastructures and its dependence is set to grow, barring sustained action in favor of reducing that dependence, which seems unlikely.

We can argue that there is a "risk mix" to Romanian dependence on CSI, as represented in the figure below.

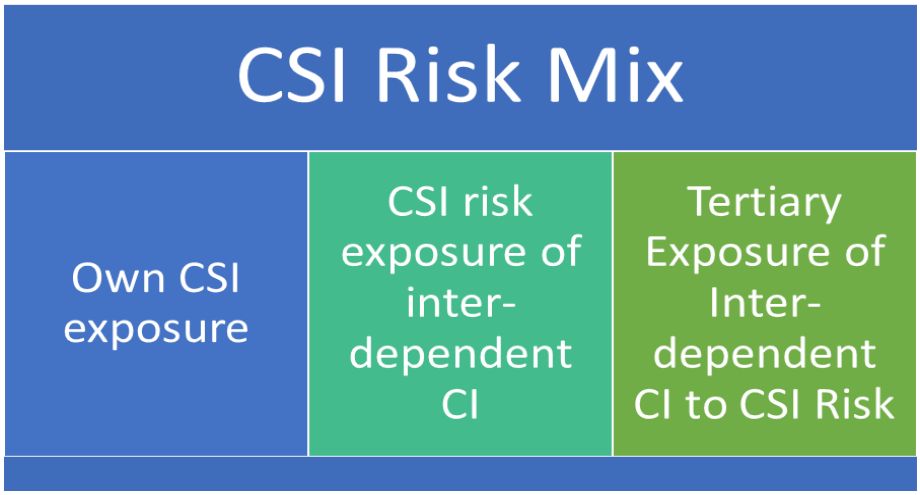

Figure 3. Critical Space Infrastructure risk mix (Mureșan and Georgescu, 2013)

Firstly, we have the aggregate exposure of Romanian CI to CSI disruption risk, seeing how we defined CSI as an upper layer of components for the system-of-systems which provides important services such as command, control, coordination, communication, data gathering etc. Secondly, we have the transmission of the CSI risk from interconnected critical infrastructures, through the interdependency trait of CI. These secondary CI may be Romanian in origin, thereby representing an "escalating failure" where a feedback loop develops within a system-of-systems (Rinaldi, 2001). They may also be CI from other European countries, with forms of interdependence other than geographic ones. While less suggestive, we may also think of exposure not in terms of individual CI, but with regards to other countries, at least for the purposes of public communication, just as the contagion of the 2008 economic crisis was described in terms of exposure to a particular country or another. Lastly, we have the tertiary risks, which are the hardest to model and which also feature significant intangible components, such as the reactions of markets to disruptions, which may heighten the impact tremendously.

All of these, put together, constitute an exposure to CSI disruption risk. It is important, when conducting a thorough assessment for the purpose of informing public policy towards future mitigation, to possess reasonably accurate information regarding the level of exposure and interdependency. Unfortunately, CI systems-of-systems are complex systems, whose combined resources and capabilities generate a new whole whose functionality, performance and capabilities exceed that of the individual components (Keating et al, 2003). This makes them very difficult to analyze from the perspective of modelling and simulation as a developing field within CIP. Any sort of simulation to determine actual dependency levels and behaviors will require a certain degree of abstraction. Software tools like TopEase can go through multiple levels of complexity in representing processes for the purposes of modelling (figures 4,5).

Shortcuts in modelling these relationships can be taken, especially if the results are intended for general policy making or to inform public discourse. For instance, one may analyze critical infrastructure interdependencies in terms of flows of information, materiel or even finance. One example in this regard is given by Nguyen et al (2013), who analyzed the dependence of the Australian critical food infrastructure sector on other infrastructures by equating inputs with financial flows in terms of acquisitions of services. This approach is best used to highlight the magnitude of the dependency, but it does little to show the criticality of the relationship, except to hint at it.

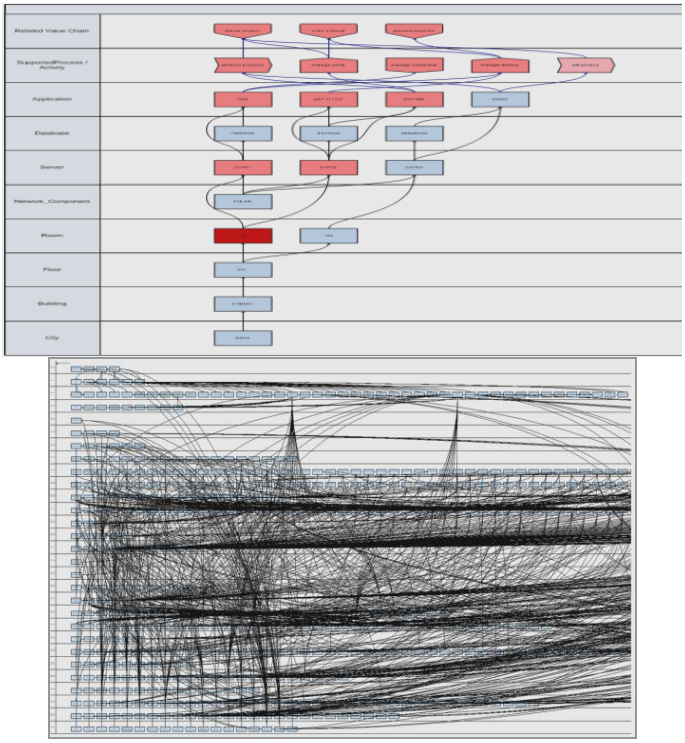

Figure 4. The difference between a simple and a complex set of relations between process components in TopEase

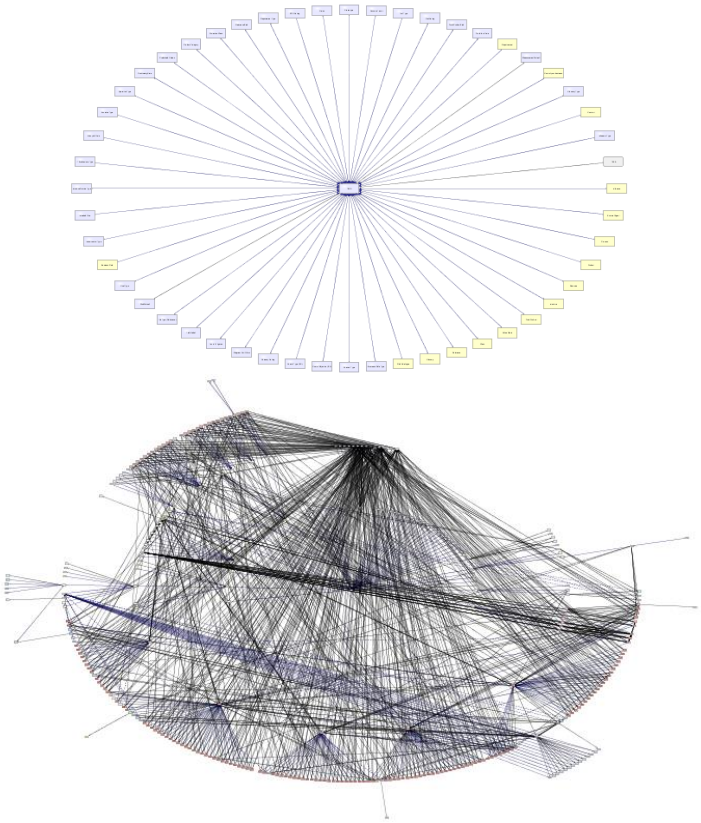

Figure 5. The difference the first and fourth levels of defined complexity in TopEase

Romania likely features a strong dependency on space systems in terms of communications, navigation, positioning and timing. To the extent of its partners' dependencies, it will also feature significant indirect exposure to CSI disruption risk. Its development over time will lead to space services being used in precision agriculture, energy transport networks/grids and crisis and emergency situation management, among other fields. In time, this will lead to the development of critical interdependencies. We must remark that, all things staying the same, Romania's openness to the outside world automatically engenders a growing dependence on space systems, since this is the obvious dynamic highlighted by studies in the field.

CSI and Romanian National Security

As mentioned, the absence of Romanian space assets does not imply the absence of dependence on CSI. Rather, Romania also faces exposure to political risks related to access to space systems. This may manifest as an inability to resolve what we will call the "trilemma" of access to space services – accessibility, affordability and sustainability of space services consumption – a concept initially developed to express concerns over energy. Basically, even with Romania's status as a respected member of the International Community, there may be circumstances when it will find itself with restricted provisioning of critical space services.

There are several scenarios for this happening. Firstly, there may be a unilateral decision on the part of a country with jurisdiction over a critical asset. For instance, the American GPS and the Russian GLONASS are both global navigation satellite systems (GNSS) which are owned and operated by their militaries, with civilian users as a secondary priority. The US Department of Defense maintains the right to unilaterally degrade the quality of GPS signal for any user, including civilian and including those from Allied countries. The manifestation of such a situation during a crisis event would place immediate difficulties on a whole host of critical application, from global supply and production chains to coordinating the functioning of electricity grids, databases or financial markets.

Secondly, there may be a situation where a deliberate, accidental or natural threat against a CSI or a critical space component of a CI will lead to diminished capacity to provide space services. This may lead to the curtailment or rationing of Romanian access to such services on political grounds or based on predatory pricing of access or even internal decisions on the part of affected companies, such as mobile communications providers.

Thirdly, the international space governance system may take a turn for the worst when it comes to the interests of small or non-spacefaring nations such as Romania. In particular, we can highlight the apparent trend of the militarization of space (de Zwart et al, 2018) which may lead to the normalization of the targeting of space systems for disruption, diversion or destruction. Given the nature of the space environment and the limited number of space assets, this may lead to collateral damage to countries such as Romania.

Therefore, Romania must undertake a sustained effort to manage its exposure to CSI disruption risk. The first and obvious measure is to gradually build up an inventory of its own space assets, to provide part or all of its required critical provisioning of space services, maybe even with redundancies in place. This is a policy which is more and more accessible today politically and cost-wise, as there is a growing list of space transporters and a trend towards lowering cost barriers to space access, including for satellite acquisition. The growing capabilities of cubesats means that even actors with modest means can afford not only basic space services, but also redundant capabilities. Japan is an interesting example, since, after the loss of its main Earth Observation satellite, ALOS 1, during the 2011 Fukushima Daiichi disaster, it replaced the satellite with a constellation of smaller ones with, overall, more capabilities, but also overlapping ones, to avoid "common point failures" for its crisis and emergency management system (Georgescu et al, 2015).

The second one is to work as part of a collective to ensure sustainable access to space services. For instance, as a member nation of the European Space Agency, Romania is a supporter

of the Galileo GNSS system, which does not feature civilian restriction operating procedures, unlike the GPS or GLONASS systems, and devices using the Galileo signal are also capable of utilizing GPS or GLONASS signals, thereby ensuring a built-in redundancy. Another ESA project is related to the COPERNICUS/GMES program which operates the Sentinel satellite systems which provides Earth Observation data at advantageous cost to members, and even free access for certain users with lower data quality.

Romania is also a member of the International Charter for Space and Major Disasters, an organization which mediates the provisioning of critical space services for Member States affected by disaster situations for the purpose of aiding crisis and emergency situation management efforts. Japan was a beneficiary of this agreement during the Fukushima disaster, and it is also a member of Sentinel Asia, a regional body with the same goal. It behooves Romania to also be a party to as many such organizations as possible, while also developing capabilities it may offer in its turn.

Romania must also work to ensure a stable, legitimate and predictable space governance framework that will ensure the security of the space assets on which it is critically dependent. Whether we are discussing legislation to minimize the creation of new space debris, alleviating the mounting tendency for militarization, coordinating the collective protection of the "global orbital commons" or contributing to projects such as ESA's Space Situational Awareness, Romania has an interest in space governance which it cannot and will not successfully pursue on its own and it must identify all opportunities to advance these interests.

Finally, Romania must harmonize its development needs with those of its CIP efforts, including with regards to CSI. It should work towards ensuring resilience, minimizing exposure to CSI disruptions, including through the use of terrestrial systems or backups, and reducing the general couplings between CI and CSI in society to reduce the risk of rapid cascading disruption.

In addition to these actions, Romanian stakeholders must undertake concrete steps to identify critical space assets, assess the actual level of dependency on CSI and determine what a critical minimum level of access to space services would entail for the continuity of government, for business continuity and for quality of life in the event of a disruption. Such an analysis implies not only an objective assessment, but also the formulation of specific policy preferences regarding the acceptable level of disruption and the anticipated time to recovery based on the willingness to allocate resources. It is only with the backdrop of this information that meaningful decisions can be taken regarding investment in National space services provisioning capacity or in increasing societal resilience to disruptions. Of course, special care must be taken with regards to National defense and its relation to CSI – the current and future dependence of the Romanian Armed Forces and the effect of disruption on its capacity to fulfill its main mission, to meet NATO obligations and those of other security cooperation formulas.

Conclusion

Space systems are a critical enabler for a wide variety of applications which are integral to the functioning of critical infrastructure systems in any advanced society. Romania is one such society, which already registers a dependence on space systems, despite lacking its own space assets, and whose dependence is set to grow as it develops and increases relations with other developed nations and the world in general. This leads us to the necessity of articulating the probability that Romania suffers from an exposure to critical space infrastructure disruption risk which, if materialized, would reverberate through the entire system-of-systems. This would result not only in material damages and possibly loss of life, but also in the reduction of confidence on the part of citizens and investors in Romania and the loss of prestige. Romania must find a way to manage and mitigate these risks, starting from modelling and simulation to understand the extent and specificities of its exposure, continuing with implementing mitigation measures such as investing in its own satellite capabilities and ending with an active presence in the collective bodies and initiatives which make up the emerging space governance framework.

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.

BIBLIOGRAPHY

1. Acker, O., Pötscher, F., Lefort, T. (2013) "Why satellites matter. The relevance of commercial satellites in the 21st century – a perspective 2012-2020", Booz & Company, Italy, https://www.esoa.net/Resources/Why-Satellites-Matter-Full-Report.pdf;
2. Bryce Space and Technology (2018), "2018 State of the Satellite Industry Report", report prepared for the Satellite Industry Association, https://brycetech.com/downloads/ SIA_SSIR_2018.pdf;
3. de Zwart, M., Hays, P., Jakhu, R., Jaramillo, C., Meyer, P., Stephens, D., Su, J., West, J. (2018) "Space Security Index 2018: Executive Summary", ISBN: 978-1-927802-21-2, http://spacesecurityindex.org/wp-content/uploads/2018/06/ SSIExecutiveSummary 2018. pdf;
4. Georgescu, A., Bucovețchi, O. (2017), "A generic flow based model for understanding critical infrastructure dependency on space systems", presented during IBIMA edition 29, Vienna, in May 2017, IBIMA Proceedings, ISBN: 978-0-9860419-6-9;
5. Georgescu, A., Jivănescu, I., Popa, Ş., Arseni, Ş.C. (2015) "Space Capabilities – assessing their Criticality as a Tool in Nuclear Guvernance", Technical Military Journal issue no. 3, Military Equipment and Technologies Research Agency, Romanian Ministry of Defense, ISSN 1582-7321.
6. Katina, P. F., Keating, C. B. (2015) "Critical infrastructures: A perspective from systems of systems", International Journal of Critical Infrastructures. 11(4), p.316–344;
7. Katina, P.F., Hester, P.T., (2013) "Systemic determination of infrastructure criticality", International Journal on Critical Infrastructures.9(3), p.211–225;
8. Keating, C. B., Rogers, R., Unal, R., Dryer, D., Sousa-Poza, A. A., Safford, R., Rabadi, G. (2003) System of systems engineering. *Engineering Management Journal*. 15(3). p.35–44;
9. Mureşan L., Georgescu A., Jivănescu I., Popa S, Arseni S (2016), "Charting Critical Energy Infrastructure Dependencies on Space Systems – New Frontiers in Risks, Vulnerabilities and Threats", published in "Critical Energy Infrastructure Protection and Cyber Security Policies", edited by Mesut Hakkı Caşın and Guido Gluschke of the Hazar Strateji Enstitüsü, Istanbul, Turkey, ISBN 978-605-83541-4-2;
10. Mureşan, L., Georgescu, A. (2013) - "Critical Infrastructure Protection and Systemic Emergent Risks, of interest to the intelligence community", Infosfera no.1/2013, Year 5, ISSN 2065-3395;
11. Nguyen, N., Hogan, L., Lawson, K., Gooday, P., Green, R., Harris-Adams, K., Mallawaarachch, T. (2013), "Infrastructure and Australia's food industry: Preliminary economic assessment", Australian Bureau of Agricultural and Resource Economics and Sciences, report 13.13, Canberra, http://data.daff.gov.au/data/warehouse/9aap/2013/ iafipead9aap_20131105/ infaAustFoodInd_prelimEcoAssess_v1.0.0.pdf;
12. Rinaldi, SM., Peerenboom, JP., Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies", IEEE Control Systems Magazine, 21(6), 11–25, 2001;

Olga BUCOVEȚCHI received her MSc in Economic Engineering (2006), PhD in Industrial Engineering (2014) from University POLITEHNICA of Bucharest. Now she is Assoc. Professor at University POLITEHNICA of Bucharest. She is a member of AMIER (Association of Economist Managers and Engineers in Romania) and ARPIC (Romanian Association for the Promotion of Critical infrastructure and Services Protection). While working at UPB she had several collaborations within national and international research projects. Her main research activities deal with risk management, critical infrastructure protection, education management and business continuity.

Olga BUCOVEȚCHI și-a obținut licența în Inginerie Economică (2006) și este doctor în Inginerie Industrială (2014) a Universității POLITEHNICA din București. În prezent este Profesor Asociat la Universitatea POLITEHNICA din București. De asemenea, este membră a AMIER (Asociația Managerilor și Inginerilor Economiști din România) și ARPIC (Asociația Română pentru Promovarea Infrastructurii Critice și Protecția Serviciilor). În timpul activității sale la UPB a avut mai multe colaborări în cadrul proiectelor de cercetare naționale și internaționale. Principalele sale activități de cercetare sunt reprezentate de managementul riscurilor, protecția infrastructurilor critice, managementul educației și continuitatea afacerii.

Alexandru GEORGESCU is working within the Department for Cybersecurity and Critical Infrastructure of the National Institute for Research and Development in Informatics. He has an eclectic background, having studied Economics, then Geopolitics, and has obtained a PhD in Risk Engineering for Critical Infrastructure Systems. He is actively involved in advancing Critical Infrastructure Protection and Resilience issues through cooperation at international level and has worked on international projects for the European Space Agency, the Shanghai Institutes for International Studies and others. He is also affiliated with the European Center for Excellence for Blockchain, with the Romanian Association for Space Technology and Industry, the EURISC Foundation and Eurodefense.

Alexandru GEORGESCU își desfășoară activitatea în cadrul Departamentului pentru Securitate Cibernetică și Protecția Infrastructurilor Critice din ICI București. A avut parte de o educație eclectică, studiind economie, apoi geopolitică, și obținând un doctorat în ingineria riscurilor pentru sisteme de infrastructuri critice. S-a perfecționat și în cadrul unor cursuri de pregătire organizate, printre alții, de către Colegiul European de Securitate și Apărare. Este implicat în mod activ în avansarea domeniului rezilienței și al protecției infrastructurilor critice prin cooperare la nivel internațional și a activat în cadrul unor proiecte susținute de Agenția Spațială Europeană, Institutele de Studii Internaționale din Shanghai și altele. Este, de asemenea, afiliat la Centrul European de Excelență în Blockchain, Asociația Română pentru Tehnologie și Industrie Spațială, Fundația EURISC și Asociația Europeană Eurodefense.

Marilena LAZĂR is a researcher with the Information Systems and Communications Test and Evaluation Scientific Research Center of the Military Equipment and Technologies Research Agency. She has a master degree in physics from Bucharest University and has obtained a PhD in Electronic engineering and telecommunications field. She has been involved as team member or project manager in multiple IT research projects that consisted in implementing various software applications. In addition, she was also involved in domains such as testing and evaluating hardware or software products.

Marilena LAZĂR este cercetător la Centrul de testare evaluare şi cercetare ştiinţifică sisteme informatice şi comunicaţii al Agenţiei de cercetare pentru tehnică şi tehnologii militare. Este absolvent al Universităţii Bucureşti având un master în fizică şi apoi a obţinut un doctorat în domeniul ingineriei electronice şi telecomunicaţii. A fost implicată ca membru în echipa de lucru sau ca director de proiect în numeroase proiecte de cercetare din domeniul IT care au implementat aplicaţii software complexe. De asemenea a fost implicată în activităţi din domeniul testare şi evaluare a produselor hardware şi software.

Carmen Elena CÎRNU graduated from the University of Bucharest, Faculty of Philosophy in 2003, and obtained her PhD in 2011. Currently she is a Senior Scientific Researcher II and Head of the Cyber Security and Critical Infrastructure Department at the National Institute for Research and Development in Informatics - ICI Bucharest, where she is involved in the development of research and development projects in the field of interoperability, cyber security and e-government. She has collaborated with universities and central public administration institutions over the years. In 2015 she was a Guest Researcher at the Global Security Research Institute at Keio University (Japan). She is the author or co-author of numerous articles, studies, and research reports.

Carmen Elena CÎRNU a absolvit Universitatea din București, Facultatea de Filosofie în anul 2003, și a obținut titlul de doctor în anul 2011. În prezent este Șef Departament Securitate Cibernetică și Infrastructuri Critice și cercetător principal gradul II, în cadrul Institutului Național de Cercetare-Dezvoltare în Informatică – ICI București unde este implicată în derularea proiectelor de cercetare-dezvoltare în domeniul interoperabilității, securității cibernetice și e-guvernării. A colaborat de-a lungul anilor cu universități și instituții ale administrației publice centrale. În anul 2015 a fost Cercetător Invitat al Global Security Research Institute din cadrul Universității Keio (Japonia). Este autor sau coautor a numeroase articole, studii și rapoarte de cercetare.