A CRITICAL INFRASTRUCTURE PERSPECTIVE AND SYSTEMS PERSPECTIVE ON HYBRID THREATS IN THE BLACK SEA REGION

Adrian-Victor VEVERA, PhD, BEng

Alexandru GEORGESCU, PhD BEng

Carmen-Elena CÎRNU, PhD

National Institute for Research and Development in Informatics, Bucharest

DOI: 10.55535/RMT.2022.1.04

The Black Sea region features high complexity and other factors, such as the lack of a regional security architecture, which, in the current security context, result in a high effectiveness for hybrid warfare approaches. This has been proven by the track record of hybrid and unconventional warfare operations in the region, targeting also civilian infrastructure. The article proposes a Critical Infrastructure perspective on Black Sea insecurity, highlighting the potentiality for hybrid warfare but also measures which can increase resilience to hybrid threats on the basis of the Critical Infrastructure Protection framework. Lastly, the article highlights contributions which Romania can make on the basis of its experience and success in implementing CIP.

Keywords: critical infrastructures; hybrid threats; resilience; governance; Black Sea;

INTRODUCTION

The 2014 illegal annexation of Crimea by the Russian Federation brought to the fore an important development in the Black Sea region and in the realm of inter-state competition – the rise in the use of asymmetric, unconventional and hybrid means of warfare to replace or complement conventional means.

The actions of Russia but also of other actors in the wider region can be interpreted in terms of attempts at disrupting the functioning of critical infrastructures (CI) to cause human losses, material damage, loss of state prestige and confidence on the part of citizens, investors, partners and allies, as well as to coerce target entities into behaving in a certain way.

Hybrid threats have existed for a long time, but the various conflicts in the Black Sea, in the Middle East and elsewhere led to the codification of strategic thought on this issue as "hybrid warfare", "new generation warfare" and components such as "economic warfare" and "lawfare".

This has, arguably, always been the case, hybrid threats have existed for a long time, but the various conflicts in the Black Sea, in the Middle East and elsewhere led to the codification of strategic thought on this issue as *"hybrid warfare", "new generation warfare"* and components such as *"economic warfare"* and *"lawfare"*. The attention paid to these developments is resulting in increased awareness of the potential of hybrid warfare to damage, disrupt or coerce an adversary through measures short of war and with built-in ambiguities that hobble existing security governance frameworks.

Critical Infrastructure Protection provides concepts, strategies and tools to achieve resilience in the face of a complex and dynamic security environment which affects the functioning of socio-technical systems on which entities such as states are critically reliant for their functioning, for business continuity and for quality of life.

The present article argues in favour of a perspective on the Black Sea security environment based on the conceptual framework of Critical Infrastructure Protection (CIP), which is officially employed by all NATO and EU member states, as well as by NATO and the EU themselves (Caşin, 2018). However, the article does not aim

to approach the issue of hybrid warfare, but rather analyse the specificities of the critical infrastructure environment in the Black Sea and formulate recommendations for how Romania may contribute to the amelioration of the issues in the region from a CIP perspective.

CRITICAL INFRASTRUCTURE PROTECTION – A PRIMER

The functioning of all societies, but especially advanced ones, is reliant on goods and services produced through the operation of infrastructures. These are socio-technical systems composed of technical assets, organisations and communication links, in the abstract, and which include pipelines, power plants, water treatment plants, roads, ports, but also public administration, the financial sector, education and health. These infrastructures are critical if their destruction or disruption exceeds certain authority-defined thresholds in terms of damage and loss of functionality that represent a grave threat to the affected societies. Critical Infrastructure Protection provides a conceptual framework to consider these issues and to develop methodologies to identify and designate critical infrastructures, while planning for their protection in an all-hazards approach that should result in resilience (Gheorghe et al, 2018).

The resilience concept refers to a system's capacity to prevent the materialisation of a negative event and, should it occur, then a resilient system should minimise the resulting damage and restore a minimum acceptable level of functionality as quickly as possible, limiting the impact on society.

The resilience concept has become an important buzzword in many fields but, in this instance, it refers to a system's capacity to prevent the materialisation of a negative event and, should it occur, then a resilient system should minimise the resulting damage and restore a minimum acceptable level of functionality as quickly as possible, limiting the impact on society. CIP is important because criticality becomes a selection factor for the allocation of scarce security resources – we cannot protect every system 100% of the time and so we must optimise the allocation of limited protection capabilities on the basis of rationally proven need.

CIP features several important advantages over other systemic frameworks:

❖ Critical infrastructures are characterised by relations of interdependence, in which changes in the state of one infrastructure affect the state of another in accordance with a series of criteria that define the topology of the system-of-systems and which emerge

from the patterns of production and consumption of critical goods and services at societal levels. These interdependencies can be geographic, physical, logical, informational, cybernetic and even political and social (Gheorghe and Schläpfer, 2006).

❖ Disruptions in the system feature not only first order effects, but also second, third and so on, in accordance with the interdependency relationships. These lead to phenomena which may amplify the duration and the effects of a disruption event in previously unanticipated ways, such as through common cause failures, escalating failures and, most importantly, cascading failures. The latter may be so complex that they defy accurate understanding and modelling and, therefore, prediction, especially since their appearance relies on the *"fortuitous alignment of breakages"* that enable the transmission of disruption across a system-of-systems (Pescaroli and Alexander, 2016).

❖ The development of the CIP framework is taking it in the direction of analysing the issues of complexity described above, which result in systems whose functioning is ambiguous and uncertain and which are greater than the sum of their parts in terms of phenomenology. They present emergent behaviours resulting from the interaction between system components and between components and the environment which could not have been anticipated from the analysis of individual components (Keating and Katina, 2016).

CIP can be described as a transatlantic framework of thinking. It was first developed by a Presidential Commission established by the Clinton Administration (PDD-63, 1998) and implemented in the wake of the 9/11 attacks which emphasised the problems stemming from interconnectedness and cascading disruptions (Department of Homeland Security, 2003).

The EU mandates that member states develop CIP frameworks while also building a European Programme for Critical Infrastructure Protection (EPCIP) whose remit are European Critical Infrastructures (ECI), whose disruption or destruction would affect two or more member states (European Commission, 2008). Initially, this European activity was limited to transport and energy infrastructure, to which cyber infrastructures were added later. The published drafts of Directives updating the CIP framework (the Critical Entities Resilience

The EU mandates that member states develop CIP frameworks while also building a European Programme for Critical Infrastructure Protection (EPCIP) whose remit are European Critical Infrastructures (ECI), whose disruption or destruction would affect two or more member states.

Directive and the NIS 2 Directive) update the CIP framework with the concept of critical entities, as opposed to owners/operators of critical infrastructures, and increases the number of European critical infrastructure sectors to 10: energy, banking, transport, financial markets, health, drinking water, waste water, digital infrastructure, public administration and space (European Commission, 2020c). This expansion, though long in the making, was validated by the experience of the pandemic, which caused European disruptions to CI which had previously not been considered in a European dimension.

BLACK SEA INFRASTRUCTURE CHARACTERISTICS

The Black Sea features peculiarities in terms of the critical infrastructure system-of-systems, arising from the interplay between historical specificities and recent experiences and policies.

Before we begin, we should underscore the fact that the Black Sea is a fluid space, promoting either confusion or ambiguity in its characterisation. We seem unable to ascertain whether the region is a border or a bridge between East and West and between civilisations, or to even define it properly. Triantaphyllou (2012) noted that the Black Sea is characterised by *"competing and conflicting narratives"* which undermine the possibility of effective transborder cooperation in various areas, which include environmental issues but also, as we contend, CIP. This becomes even more pronounced if we use the expanded formula for the region which is preferred by the EU and the Organization for Black Sea Economic Cooperation. In this case, rather than six littoral states, there are either four additional countries for the EU or six additional countries for BSEC.

It is also an especially diverse region from a civilisational perspective, which gives it transregional dimensions, leading towards the Eastern Mediterranean or the Caspian region, as well as subregional dimensions, such as the South Caucasus. Lastly, the Black Sea sits atop a series of fault lines, whether religious and civilisational (Christianity and Islam), as well as geopolitical (NATO/EU and the Shanghai Cooperation Organization).

The surface level analysis of the regions serves to outline the complexities – Romania, Bulgaria (and Greece if you include it)

are NATO and EU Members, Turkey is a NATO member that has become unreliable and has an acrimonious relationship with the EU and fellow allies while becoming a dialogue partner to the SCO, the Russian Federation is an SCO founding member and revisionist actor trying to maintain influence in its near abroad and fomenting conflict, Ukraine, the Republic of Moldova and Georgia are the sites of hybrid interventions aimed at triggering and maintaining frozen conflicts and so on.

Regional stakeholders are divided by: the absence of a regional identity; strategic competition – Russia and NATO, SCO and NATO, Turkey's unpredictability; frozen and *"lukewarm"* conflicts; ethnic and religious conflicts; the absence of pre-existing institutions and arrangements that are functional and successful. *Figure no. 1* summarises some of these specific issues.

Regional stakeholders are divided by: the absence of a regional identity; strategic competition – Russia and NATO, SCO and NATO, Turkey's unpredictability; frozen and "lukewarm" conflicts; ethnic and religious conflicts; the absence of pre-existing institutions and arrangements that are functional and successful.

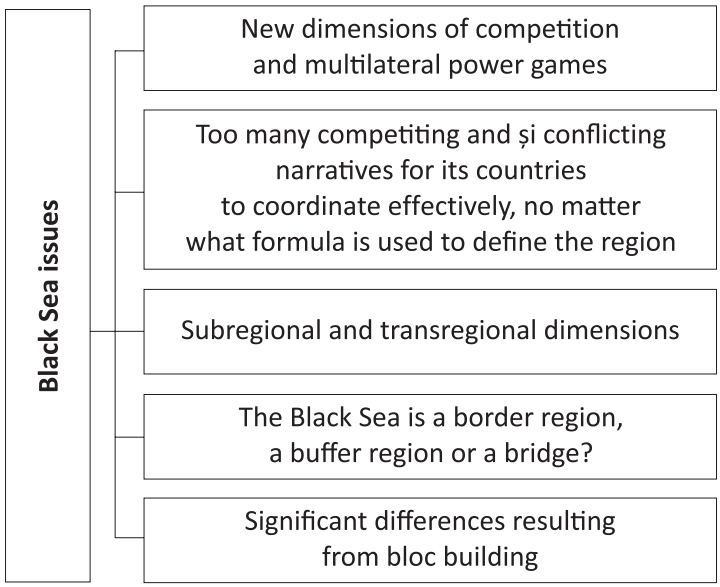

Figure no. 1: Main issues affecting the Black Sea Region

In turn, all of these affect the critical infrastructure landscape, as well as the security environment:

❖ the complex history of the region has led to a lack of an institutionalized security architecture which could have provided the basis for CIP efforts in the region and increased resilience.

On the contrary, geopolitical conflict has led regional actors such as Russia to undermine any possibility for the creation of the trust and political capital necessary for collective action in the region;

❖ the persistent instability, along with frozen and *"lukewarm"* conflicts, both old and new, have generated important issues with risk perception that affect local and outside players, as well as investors and citizens;

❖ the infrastructure topology is fragmented – there is a lack of regional interconnectors and a geopolitical difficulty in creating them (as shown by the various failed energy transmission projects or by the perennial Black Sea Ring Road proposal);

The infrastructure topology is fragmented – there is a lack of regional interconnectors and a geopolitical difficulty in creating them (as shown by the various failed energy transmission projects or by the perennial Black Sea Ring Road proposal).

❖ the infrastructures are heterogeneous – they were created by individual states in periods with vastly different economic and political regimes and in the context of significant persistent regional differences between regional players. The different railway gauges in standard use between the SE and NW sides of the Black Sea emphasise this, as well as other factors;

❖ the *sedimentation* of different generations of infrastructure layers creates a complex environment, featuring, for instance, oversized and undermaintained industrial capabilities, as well as undersized multimodal transport capabilities. The risks, vulnerabilities and threats created are heightened by the decades of neglect of infrastructure maintenance and of conflict in much of the region, as well as the attrition of existing infrastructures. Poverty and regional disparities also contribute to regional diversity in terms of infrastructure endowment and security;

❖ digitalisation, as a fundamentally transformative phenomenon in the CI topology, is proceeding with varying speeds in the region, but the capacity to secure digitalised infrastructures has been lagging behind, for economic and governance reasons. This provides a main avenue for hybrid warfare in the region, which is cyberattacks (Tatar et al, 2017);

❖ the region remains a critical crossroads and is, therefore, an important site for proposals for strategic infrastructure in energy and trade, as seen from developments in energy (TurkStream, the Trans-Adriatic Pipeline functioning since 2020), in transport

and in digital infrastructure (The Belt and Road Initiative, The Three Seas Initiative). These infrastructures are high-profile projects with geopolitical impact and are, therefore, both targets and elements of hybrid warfare in geopolitical competitions. *Figure no. 2* summarises some of these main points.

Black Sea Infrastructure Concerns	Lack of an institutionalized security architecture
	Risk perceptions in the area
	Persistent conflict and uncertainty
	Lack of infrastructure connectors around the Black Sea
	Aging and attrition in existing infrastructure
	Infrastructure heterogeneity, sedimentation and complexity
	Uneven and unsecured digitalization
	Geopolitical conflicts as instigators of hybrid threats
	Site for strategic infrastructure development

Figure no. 2: Main issues affecting the Black Sea infrastructures

Critical infrastructure governance is not the only area that has suffered, but also environmental protection and the fight against transborder organised crime, with Delanoë (2015) highlighting the region's role in the smuggling of nuclear materials and technology.

RECOMMENDATIONS ON ROMANIAN CONTRIBUTIONS TO COUNTERING HYBRID THREATS AT THE BLACK SEA

Romania, as an active player in the Black Sea region and with a significant exposure to the effects of the instability and deterioration of the security environment, has an incentive to leverage all of its advantages and tools in order to contribute to better security outcomes through systemic shifts in underlying risks, vulnerabilities and threats. This section deals mainly with the contributions that Romania can make outside its borders, in the context of critical infrastructure protection and system-of-system resilience. This is a challenging topic to approach, given resource constraints, jurisdictional issues, deficient toolboxes and the ebb and flow of will on the part of decision makers

Romania, as an active player in the Black Sea region and with a significant exposure to the effects of the instability and deterioration of the security environment, has an incentive to leverage all of its advantages and tools in order to contribute to better security outcomes through systemic shifts in underlying risks, vulnerabilities and threats.

to invest in projects with security outcomes which are hard to measure. *Figure no. 3* highlights the priorities for a Romanian approach to CIP in the region.

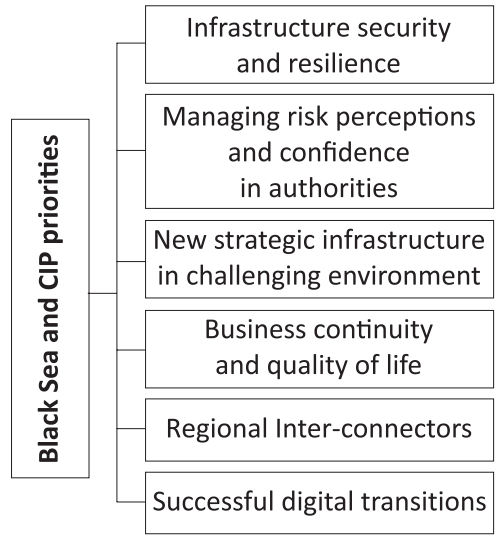

Figure no. 3: The CIP framework priorities for the Black Sea

The first contribution that Romania can make is in leveraging its own successful application of Directive 114/2008 to assist countries in the region to develop their own CIP frameworks which are compatible with the European approach and integrate best practices. This not only improves the underlying security of the individual countries, but also heightens their compatibility with the EU in favour of closer cooperation and integration.

Leveraging Romanian contributions to CIP to the benefit of other states in the region

The first contribution that Romania can make is in leveraging its own successful application of Directive 114/2008 (Lazari and Simoncini, 2016) to assist countries in the region to develop their own CIP frameworks which are compatible with the European approach and integrate best practices. This not only improves the underlying security of the individual countries, but also heightens their compatibility with the EU in favour of closer cooperation and integration. Romania may coordinate a multi-pronged approach towards experience transfer, involving both state institutions, but also academia (universities), the private sector (security companies) and civil society groups (professional associations), Romanian entities can also take a lead in serving as an interface between other European actors interested in contributing to CIP in the region and counterparts in individual nations, especially from the South Caucasus. Possible items on such an agenda include:

- assistance for the drafting of documents of reference in CIP;

- assistance in setting up continuing education programs for experts and decision-makers;
- contacts for knowledge transfers between counterpart institutions and for setting up CIP-related bodies such as Interinstitutional Working Groups, Technical Secretariats, Crisis and Emergency Management Centers and so on;
- cooperation in the non-governmental sphere, in order to set up national Critical Infrastructure and Services Protection Associations for experts and companies;
- fostering greater cooperation with the Romanian security industry, which may provide useful solutions to address specific security needs.

This is not a farfetched proposal, and its complexity stems from the high number of possible components we can define, not from intrinsic difficulty. One of the authors of this paper also contributed to Ukraine's Green Paper on Critical Infrastructure Protection after the organisation of a NATO Advanced Research Workshop in Kiev on this subject in 2015 (Mureșan and Georgescu, 2016).

Supporting EPCIP expansion in the Black Sea

A second contribution that Romania can make is to lobby for an evolution of the European Programme for Critical Infrastructure Protection (EPCIP) to start developing the protection dimension of European Critical Infrastructures (ECI) located in non-Member States. The definition of ECI as *"encompassing infrastructures whose disruption or destruction would critically affect two or more member states"* (OUG 98/2010, art. 3b.) would remain, but the EU should strive to address the non-European dimension of ECI, as a vector for the propagation of risks and threats. This would involve the mobilisation of European resources for the same actions described in the previous section. Since Romania and Bulgaria are the two EU MS on the Black Sea and are the first line of transmission for disruptions generated in the region, it stands to reason that they would be important beneficiaries of any EU efforts in this regard. Such an expansion of EPCIP can only be done on a voluntary basis and with the provisioning of significant incentives for cooperating states, however there is already a precedent,

most recently placed on display in the *North Stream 2* project, of the EU regulating infrastructure functioning (the unbundling of energy and transmission) in relation to a third-party state based on EU security interests.

In addition to expanding EPCIP, the EU could apply the lessons learned in the Western Balkans to the Black Sea region, by transferring expertise and tools related to the Western Balkans Strategy (European Commission, 2020a) or the Western Balkans Connectivity Agenda (European Commission, 2020b). Georgescu et al (2020) have underscored how these approaches can support CIP efforts in terms of capacity building, knowledge transfer and raising awareness.

Romania could advocate for a Black Sea Macroregional Strategy of the European Union. Macroregions are a new form of governance in the EU, which "incorporate (wholly or partially) the territories of multiple countries framed around common challenges and features, common identities, historical or cultural commonalities, as a discursive underpinning of functional cooperation and territorial cohesion in areas such as transport, infrastructure and environmental policy".

Advocating for the Black Sea Macroregional Strategy of the EU

Romania could advocate for a Black Sea Macroregional Strategy of the European Union. Macroregions are a new form of governance in the EU, which *"incorporate (wholly or partially) the territories of multiple countries framed around common challenges and features, common identities, historical or cultural commonalities, as a discursive underpinning of functional cooperation and territorial cohesion in areas such as transport, infrastructure and environmental policy"* (Gänzle and Kern, 2015).

Romania had been one of the initiators, alongside Austria, of the Macroregional Strategy for the Danube Region. Since there is no appetite to redefine the unwieldy Danube Macroregion to include a natural extension into the Black Sea, a new macroregion could be implemented for the Black Sea. Such a project can be proposed together with Bulgaria and, since macroregions encompass functional regions with transborder components, could automatically accommodate all Black Sea countries, plus even the wider region such as the South Caucasus. This initiative, based on the accumulated European expertise and resources, could provide a better institutional backdrop for cooperation in favour of resilience, in a way in which the Organization of Black Sea Economic Cooperation, the GUAM formula, the Community of Democratic Choice[1] and the much earlier EU Black Sea Synergy initiative have largely failed.

[1] The Community of Democratic Choice is an intergovernmental organisation established on 2 December 2005, by nine states of Northern, Central and Eastern Europe in Kyiv, Ukraine. Its main task is to promote democracy, human rights, and the rule of law throughout the region.

Figure no. 4 highlights the main components of the Danube Strategy, which includes also the Republic of Moldova and parts of Ukraine. In fact, a Black Sea Macroregional Strategy could encompass the Black Sea region at its largest extent, including Greece and the South Caucasus.

Figure no. 4: Map of the EU Strategy for the Danube Region
(the European Commission, 2021-a)

Figure no. 5 highlights the main components of the Danube Strategy Agenda, which could serve as the basis for a Black Sea Strategy Agenda. Many of these components have CIP dimensions related to achieving their goals, while the *"Strengthening the Region"* subchapter explicitly deals in security issues and could include a CIP component.

The development of a macroregional strategy would encompass a wide array of issues, such as economic, infrastructural, environmental and cultural projects, while Romania could also promote a stronger security component compared to the safety orientation of previous macroregional strategies. Such a security component could include cybersecurity, supply chain security and other novel aspects such as undersea infrastructure security, some of them specific to the Black Sea region.

The development of a macroregional strategy would encompass a wide array of issues, such as economic, infrastructural, environmental and cultural projects, while Romania could also promote a stronger security component compared to the safety orientation of previous macroregional strategies. Such a security component could include cybersecurity, supply chain security and other novel aspects such as undersea infrastructure security, some of them specific to the Black Sea region.

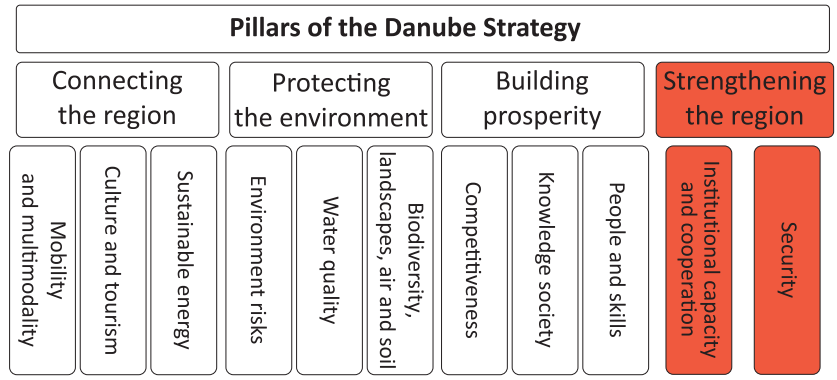

Figure no. 5: The pillars of the EU Strategy for the Danube Macroregion
(the European Commission, 2021-b)

This project would respond to multiple needs in the region, which had previously been alluded to – the need for coordinated investment in sustainable infrastructure, the need for a functional, results oriented forum of the regional countries in the context of the absence of a workable regional security architecture, targeted investments in resilience and the effect on morale of EU involvement in a concrete project with defined benefits, but also the possibility of a transatlantic contribution given NATO-EU cooperation on maritime security, hybrid threats and cybersecurity. Lastly, it should be kept in mind that a macroregional approach affords the opportunity for calibrated cooperation with the Russian Federation at a later date, should it prove useful (Gänzle, 2017). Prior to Russia's backslide into revisionism, irredentism and aggressive confrontationalism, the various transborder cooperation formulas of the Baltic Region, including the Baltic Macroregional Strategy and the Nordic Council, served a similar role in relation to the Russian Federation (Gänzle, 2017).

Actions under the *Three Seas Initiative*

Lastly, Romania should redouble its efforts within the Three Seas Initiative, an existing and established regional cooperation framework that is, nevertheless, in a phase of conceptual growth in which new dimensions and projects can be added (Żurawski vel Grajewski, 2017).

Mureșan and Georgescu (2017) noted that the *"Black Sea region, as a whole, is the least developed of the three seas, in terms of infrastructure and accumulated wealth. Political fractures have prevented the formation of pan-regional infrastructure networks and current conflicts and geopolitical hotspots are diminishing the region's wealth and attractiveness for investors"*.

The Black Sea lacks strong, technologically sophisticated and wealthy countries aligned to the West with an incentive for cooperating in multilateral frameworks for cooperation and coordination, for creating resilient institutions and for incentivising behaviour conducive to regional peace, stability, resilience and predictability. Romania must lean on the strategic partnership with Poland and the United States to accelerate specific projects with Black Sea-related security outcomes, in areas such as transport infrastructure with military mobility potential, cybersecurity and more. *Figure no. 6* summarises the proposals regarding Romania's regional contributions from a CIP perspective.

The "Black Sea region, as a whole, is the least developed of the three seas, in terms of infrastructure and accumulated wealth. Political fractures have prevented the formation of pan-regional infrastructure networks and current conflicts and geopolitical hotspots are diminishing the region's wealth and attractiveness for investors".

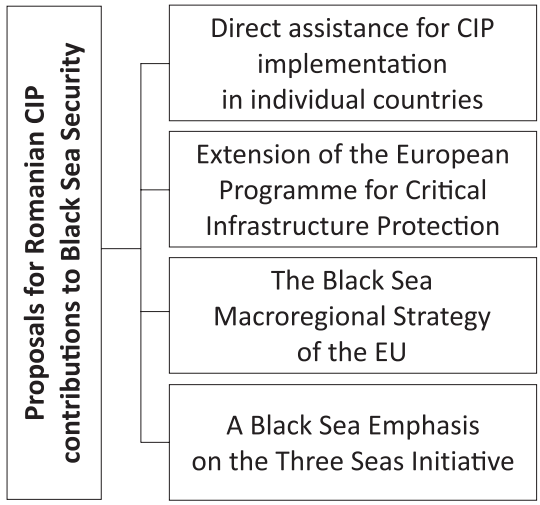

Figure no. 6: Proposal for Romanian contributions related to CIP in the Black Sea region

CONCLUSIONS

The Black Sea region presents a dynamic and challenging security environment, and its importance will grow, not just as a source of possible disruptions and instability, but also in economic terms, with energy and transport projects (like the planned Istanbul Canal).

An analysis from the perspective of Critical Infrastructure Protection offers a partial picture of the region's issues and a coherent explanation for the form of hybrid warfare that has been practiced in the region by revisionist and ambitious actors from inside and outside the region.

Romania can greatly contribute to securing the region against hybrid threats by sharing its CIP experience with other EU member states and not only, by promoting the EU strategy for the Black Sea microregion and by carrying out actions under the Three Seas Initative.

The Black Sea region presents a dynamic and challenging security environment, and its importance will grow, not just as a source of possible disruptions and instability, but also in economic terms, with energy and transport projects (like the planned Istanbul Canal).

BIBLIOGRAPHY:

1. Cașin, M. (2018). *Understanding NATO's New CIP Policies: Common Efforts and Solidarity*. In Gluschke, G., Cașin, M., Macori, M. (Eds.). Cyber Security policies and Critical Infrastructure Protection. Institute for Security and Safety Press, https://uniss.org/cyber-security-policiesand-critical-infrastructure-protection/, retrieved on 12 September 2021.
2. Delanoë, I. (2015). *Weapons of Mass Destruction – a Persisting Security Challenge in the Black Sea Region*. Neighborhood Policy Paper, 16. Center for International and European Studies, https://www.files.ethz.ch/isn/193512/NeighbourhoodPolicyPaper(16).pdf, retrieved on 12 September 2021.
3. Eusgeld, I., Nan, C., Dietz, S. (2011). *"System-of-systems" approach for interdependent critical infrastructures*. Reliability Engineering System Safety 96(6):679–686, DOI: 10.1016/j.ress.2010.12.010.
4. Gänzle, S., Kern, K. (2016). *Macro-regions, 'Macro-regionalization' and Macro-regional Strategies in the European Union: Towards a New Form of European Governance?.* In Gänzle, S., Kern, K. (Eds.) A 'Macro-regional' Europe in the Making, Palgrave Studies in European Union Politics series. Palgrave Macmillan, Londra, doi: 10.1007/978-1-137-50972-7_1, https://link.springer.com/chapter/10.1007/978-1-137-50972-7_1, retrieved on 21 September 2021.

5. Gänzle, S. (2017). *Macro-regional strategies of the European Union, Russia and multilevel governance in Northern Europe*. In Journal of Baltic Studies, 48(4), 1-10. doi:10.1080/01629778.2017.1305201.
6. Georgescu, A., Vevera, V.V., Cirnu, C.E. (2020). *A Critical Infrastructure Protection Perspective on Counter-Terrorism in South-Eastern Europe*. In Čaleta, D., Powers, J.F. (Eds.). Cyber Terrorism and Extremism as a Threat to Critical Infrastructures. Ministerul Apărării din Republica Slovenia. SUA: Joint Special University Tampa. Slovenia: Ljubljana, Institute for Corporative Security Studies.
7. Gheorghe, A., Schläpfer, M. (2006). *Critical Infrastructures: Ubiquity of Digitalization and Risks of Interdependent Critical Infrastructures*. In IEEE International Conference Systems Man and Cybernetics – SMC '06, 1, pp. 580-584.
8. Gheorghe, A.V., Vamanu, D.V., Katina, P.F., Pulfer, R. (2018). *Critical Infrastructures, Key Resources, Key Assets*. Risk, Vulnerability, Resilience, Fragility, and Perception Governance. *Topics In Safety, Risk, Reliability and Quality*, 34. Springer. doi: 10.1007/978-3-319-69224-1.
9. Keating, C.B., Katina, P.F. (2016). *Complex System Governance Development: a First Generation Methodology*. In International Journal of System of Systems Engineering, 7 (1/2/3), pp. 43-74.
10. Lazari, A., Simoncini, M. (2016). *Critical Infrastructure Protection beyond Compliance. An Analysis of National Variations in the Implementation of Directive 114/08/EC*. In Global Jurist, 16(3), 267-289. doi: 10.1515/gj-2015-0014.
11. Maier, M.W. (1998). *Architecting Principles for Systems-of-Systems. Systems Engineering*. 1 (4): 267-284, https://doi.org/10.1002/(SICI)1520-6858(1998)1:43.0.CO;2-D, retrieved on 12 September 2021.
12. Mureşan, L., Georgescu, A. (2016). *Critical Infrastructure Protection – Romanian Contributions and Experiences* (in Ukrainian). In Biriukov, D., Kondratov, S., Sukhodolia, O. (Eds.). Zelena knyha z pytan zakhystu krytychoy infrastructuru (Green Paper for Critical Infrastructure Protection), 93-106. ISBN 978-966-554-258-2. Ucraina: Kiev, Institutul Național de Studii Strategice de sub Președintele Ucrainei.
13. Mureşan, L., Georgescu, A. (2017). *Non dimenticate il Mar Nero! La Romania e il Trimarium*. In Limes Rivista Italiana di Geopolitica, 12, https://www.limesonline.com/cartaceo/non-dimenticate-il-marnero-la-romania-e-il-trimarium, retrieved on 21 September 2021.
14. Mureşan, L., Georgescu, A. (2019). *A Critical Infrastructure Perspective on the Belt and Road Initiative and its Opportunities and Challenges.* In Jiemian, Y., Obradovic, Z. (Eds.). The Belt and Road and Central and Eastern Europe, 205-228. Shanghai Foreign Language Education Press.

15. Pescaroli, G., Alexander, D. (2016). *Critical Infrastructure, Panarchies and the Vulnerability Paths of Cascading Disasters*. In Natural Hazards, 82, 175-192. doi: 10.1007/s11069-016-2186-3.
16. Tatar, U., Geers, K., Georgescu, A. (2017). *A Framework for a Military Cyber Defence Strategy Workshop – Final Report*. In Tatar, U., Gokce, Y., Gheorghe, A. (2017). Strategic Cyber Defense: A Multidisciplinary Perspective (NATO Science for Peace and Security Series – D: Information and Communication Security), 48. IOS Press.
17. Triantaphyllou, D. (2012). *The Uncertain Times of Black Sea Regional Security*. In Euxeinos – Online Journal of the Center for Governance and Culture in Europe, 6, 4-10, https://gce.unisg.ch/en/euxeinos/archive/06, retrieved on 12 September 2021.
18. Żurawski vel Grajewski, P. (2017). *Trimarium: A View from the North*. In Redlowska, K. (Ed.), Adriatic – Baltic – Black Sea: Visions of Cooperation. Institute for Eastern Studies Warsaw, Poland, http://www.forum-ekonomiczne.pl/wp-content/uploads/2017/08/AdriatykBa%C5%82tyk-Morze-Czarne16x24_2017en_PDF.pdf, retrieved on 12 September 2021.
19. The White House (1998). *PDD-63 – Presidential Decision Directive/NSC 63*. Washington DC, https://clinton.presidentiallibraries.us/items/show/12762, retrieved on 21 September 2021.
20. The European Commission (2008). *Council Directive 2008/114/CE 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/legal-content/RO/TXT/PDF/?uri=CELEX:32008L0114&from=EL, retrieved on 21 September 2021.
21. The European Commission (2020-a). *The Western Balkans Connectivity Agenda*, https://wbif.eu/storage/app/media/Library/6.%20Connectivity %20Agenda/brochure_wb_connectivity_agenda_en.pdf, retrieved on 21 September 2021.
22. The European Commission (2020-b). *A Credible Enlargement Perspective for and Enhanced EU Engagement with the Western Balkans*, https://ec.europa.eu/neighbourhood-enlargement/system/files/2019-03/ western_balkans_strategy_brochure.pdf, retrieved on 21 September 2021.
23. The European Commission (2020-c). *COM/2020/829 final – Proposal for a Directive of the European Parliament of the Council on the Resilience of Critical Entities*, https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52020PC0829&from=EN, retrieved on 21 September 2021.

24. The European Commission (2021-a). *EU Strategy for the Danube Region. Map from the main page of the Danube Macro-region Strategy, the European Commission website*, https://ec.europa.eu/regional_policy/en/policy/cooperation/macro-regional-strategies/danube/, retrieved on 21 September 2021.
25. The European Commission (2021-b). *EU Strategy for the Danube Region*, document KN-06-17-230-EN-N, ISBN 978-92-79-74482-2, doi:10.2776/56371, https://danube-region.eu/wp-content/uploads/2021/01/EUSDR-EN.pdf, retrieved on 12 September 2021.
26. Department of Homeland Security – DHS (2003). *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf, retrieved on 21 September 2021.