https://doi.org/10.18485/iipe_ioscw.2022.2.ch19

THE EMERGENCE OF NEW ORGANIZATIONAL FORMS OF INTERNATIONAL STRATEGIC COOPERATION IN CONTEMPORARY INTERNATIONAL RELATIONS

Alexandru GEORGESCU, Carmen Elena CÎRNU*

Abstract: The globalized world is characterized by the significant interdependence of states, international organizations, and other actors, as well as institutional forms of cooperation. Accelerated technological development has led to significant changes in the global power structure, resulting in the emergence of new forms of multidimensional cooperation and competition. New organizational forms of international strategic cooperation would therefore have to be adapted to the times in order to respond to all the challenges of the modern world. The emergence of new forms of international strategic cooperation should enable the development of the international legal order and the strengthening of institutional mechanisms for collective action. This paper considers a list of key issues that require prompt collective action based on a resilience perspective and critical infrastructure protection. The paper describes the actions that are currently taking place at the international level of international institutional evolution.

Keywords: Critical infrastructure, cyber diplomacy, collective action, competition, standards, resilience.

INTRODUCTION

The world is entering a new phase requiring collective action and decision-making, regardless of the underlying tensions and rivalries animating the principal subjects of international relations, the sovereign states. The long-running process of globalization, establishing global

* Expert, PhD. and Senior Researcher, National Institute for Research and Development in Informatics, Academy of Romanian Scientists, Bucharest, Romania. E-mails: alexandru.georgescu@ici.ro; carmen.cirnu@ici.ro

divisions of labor on the basis of differences between countries and regions and on the back of advances in transport technologies and techniques and communications technologies, has led to significant growth in trade in goods and services, the proliferation of technologies of all kinds, and the mobility of capital and people. However, this system has also proven to be prone to systemic shocks in recent decades, with crises that propagate outward from their point of origin and spread to other countries and regions, leading to escalating losses and uncertainty about their duration and impact. Other crises also originate from the functioning of globalized and interdependent systems and are the result of complexity, systemic stressors, and accumulated errors (Gheorghe et al., 2018). The former includes the global COVID-19 pandemic and the war in Ukraine, and the latter may include the global financial crisis of 2008. The effects of these transborder crises include uncertainty at multiple levels; the risk of knee-jerk national policies that aggravate situations; economic losses; human casualties; and supply and production chain interruptions, potentially with escalating results. While individual countries strive to protect their own citizens, prevent disasters and mitigate damage while anticipating future problems, the transborder and trans-sector nature of systemic crises means that solutions can only be found through collective decision-making and action (Georgescu et al., 2020, September). The manufacturing of new avenues towards prosperity is also impossible to do at a national level and requires a further international organization with the role of harmonization, resource concentration, complex project implementation, and the management and protection of the resulting interlinks in order to ensure resilience. This has usually been done within the framework of existing international organizations and bodies, taking advantage of their political capital, pre-existing organizational heft, and the habit of cooperation through them. This article argues that, increasingly, the complexity of the issues we are faced with and the vagaries of international cooperation and competition patterns are leading to the emergence of new organizational forms of international strategic cooperation for advancement and resilience – not as a replacement, but, more often, as an issue-specific addendum to the existing instruments of contemporary international relations.

These issues are analyzed and argued through the lens of the framework of Critical Infrastructure Protection, incorporating an emerging technology perspective.

A CRITICAL INFRASTRUCTURE PERSPECTIVE

At the foundation of the functioning of our societies lies an interlocking array of sociotechnical systems called infrastructures, composed of technical assets, organizations, regulations, and communication and coordination channels, involved in the provisioning of goods and services and in reducing the frictions of human activity (Gheorghe et al., 2018). They make the economic, political, and social lives of our societies possible and also facilitate interaction between different political units across vast distances, which is an important part of life in a globalized society. These infrastructures range from pipelines to power plants, ports, roads, water systems, financial systems, public administration, agriculture, and more. Their breadth and depth are determined by the economic and technological sophistication of the society they support, and they eventually incorporate a wide range of technologies in accordance with the rate of innovation, thereby allowing them to become more efficient, more interconnected, and more numerous. These infrastructures are critical if their disruption or destruction would cause significant loss of human life, material damage, loss of prestige, and loss of confidence in the authorities on the part of citizens, investors, partners/allies and markets (Georgescu et al., 2020).

These infrastructures are interdependent, meaning that a change in the status of one will affect infrastructures that are dependent on it, which leads to the compounding of efficiency and productivity, but also to the propagation of risks and disruptions. These dependencies range from geographic (due to proximity) to physical (products and materials input and output), logical (as part of a functioning chain of systems) and informational (the information produced by one system serves as input for another and *vice versa*) (Gheorghe & Schlapfer, 2006). This is especially important since the advent of digital communications and the increased reliance on automated systems communicating online to enact minute and delicate coordination across infrastructure systems dispersed over large distances and multiple jurisdictions. Infrastructures may fail from common causes or can fail serially based on their interconnection map. They can also register an escalating failure if the relationship is bidirectional and they keep influencing each other for the worse during a crisis event. Ultimately, a sufficiently strong disruption event can lead to a cascading disruption that affects many more critical infrastructures than decision-makers could have anticipated, given the complexity of the interrelationship, compounding damage and prolonging crises (Pescaroli & Alexander, 2016). This is a critical issue for the subject of international relations as the economic organization

of the world entails flows of raw materials, capital, people, intermediary goods, finished goods, technology, and know-how mediated by critical infrastructures that are increasingly transborder and continental or global in scope. The previously mentioned trends of digitalization and automation have co-evolved with globalization to create an even greater fragmentation of global production and supply chains with the attendant complexity of infrastructures (Keating and Bradley, 2015), with critical products such as electronics and vehicles requiring inputs from dozens of countries to efficiently manufacture, deliver, and service. Since a chain is only as strong as its weakest link, it stands to reason that, no matter how strong national Critical Infrastructure Protection frameworks become, a weakness in another jurisdiction with corresponding infrastructure systems can vitiate system viability and sustainability. There is also the problem that even high-performing national CIP systems have problems dealing with the threats and vulnerabilities that appear in the interstices between national systems and awareness, especially from a lack of communication, coordination, and trust. The global nature and traceability problems of cyber-attacks are the best example, with national police and other response forces hampered by the need for cooperation and exchanges with counterparts in other nations and cultures, thereby forcing the creation of ad-hoc and then permanent structured cooperation to address these issues. Something similar is happening in the wider scope of CIP, since countries are "condemned to cooperate", regardless of geopolitical and systemic rivalries.

The following factors, as interpreted by the authors, have contributed to the creation of a dynamic, complex, and uncertain global security environment with regard to CIP:

- Greater economic integration between nations;
- A greater division of labor, which may lead to critical shortages during crises, as experienced during the pandemic;
- Digitalization and digital interconnectivity between critical infrastructure systems;
- The proliferation of weapons and advanced know-how among non-state actors, including terrorist groups which can attack critical infrastructure. These include not only cyber-attacks but also jamming and spoofing attacks with commercial-off-the-shelf hardware (Georgescu et al., 2019a);
- The rise of actors who are capable of disrupting CIs for pecuniary reasons, including transborder organized crime groups, lone wolves, activists, and state proxies with financial motivations. The rise in

ransomware attacks locking data and systems in exchange for cryptocurrency payments is a relevant example (Georgescu, 2018);

- The development of hybrid warfare, new generation warfare and war without limits theories that target not only enemy armies, but also civilian infrastructure systems, to degrade their capability to provide economically, disrupt supply chains, coerce adversaries and decrease their reliability in the eyes of citizens and partners (Georgescu et al., 2019b);
- The potential for high-impact, low-frequency events that manifest locally, like epidemics and natural disasters, to have global consequences;
- The high requirement for infrastructure investment to ensure convergence between the developing states and the global average, including through integration into global supply and production chains. Inadequate infrastructure and other stressors, such as "youth bulges", political instability, and water and food insecurity, combine to create crises with global reverberations;
- The manifestation of inter-state competition not just in the economic and technological fields, but also in the area of critical infrastructure design, construction, and management, as a new source of state influence and structural power.

An important factor is the role of emerging technologies, especially digital ones like Artificial Intelligence, quantum computing, 5G communications, and blockchain, as well as those in other fields, such as biotechnology (Musetescu et al., 2020). They create the premise for more equal competition between established powers and challengers, and their dual use becomes not just a source for economic growth, new efficiency, and domination of supply and production chains for advanced goods, but also a fundamental for greater state power. At the same time, emerging digital technologies especially have the capacity to lead to a redesign and reorientation of critical infrastructures, affecting the logic of international dependencies, the technical standards used, and the embedded advantages of first movers, which can give successful states an overwhelming edge in geopolitical competitions. One such example is the 5G communications revolution, which saw a developing "cyber diplomacy" battle between the US and China for the promotion of preferred standards and producers within international organizations and supply chains. In the words of a US Department of Defense report, "the rest of the world will likely be driven to implement the 5G network design and infrastructure of whichever country

leads 5G. China is the current leader, and U.S. allies have taken different stances on how to respond to the Chinese drive to set 5G standards" (Medin and Louie, 2019), linking critical information infrastructure security to economic, technological, and international relations issues.

The pandemic, with its impact on supply chains, production chains, existing cross-border investment projects, including infrastructure, and the general functioning of numerous infrastructure sectors, including finance, public administration, and education, underscored the global scope of CI dependencies and the need for collective action to avert the compounding errors of knee-jerk individual reactions. The issue of technology and international relations also came to the fore, as countries promoted their preferred vaccine technology and producers and worked together with blocs and through international organizations to establish restrictive vaccine approvals and regulations for the movement of people that favored certain vaccines and vaccination regimens over others. Just as importantly, the drawdown of the pandemic restrictions, which saw immense disruptions to economic processes, saw new issues stemming from lingering economic distortions, such as the impact of rapid contraction and expansion of demand on national and cross-border energy and logistical systems, among others. In conclusion, CIP and CI issues in general (involving resilient design, implementation, and operation), as well as emerging technology issues, are important subjects on the agendas of all stakeholders in the international community, and international organizations play a role in defining these agendas and catalyzing actions and norm/trust-building.

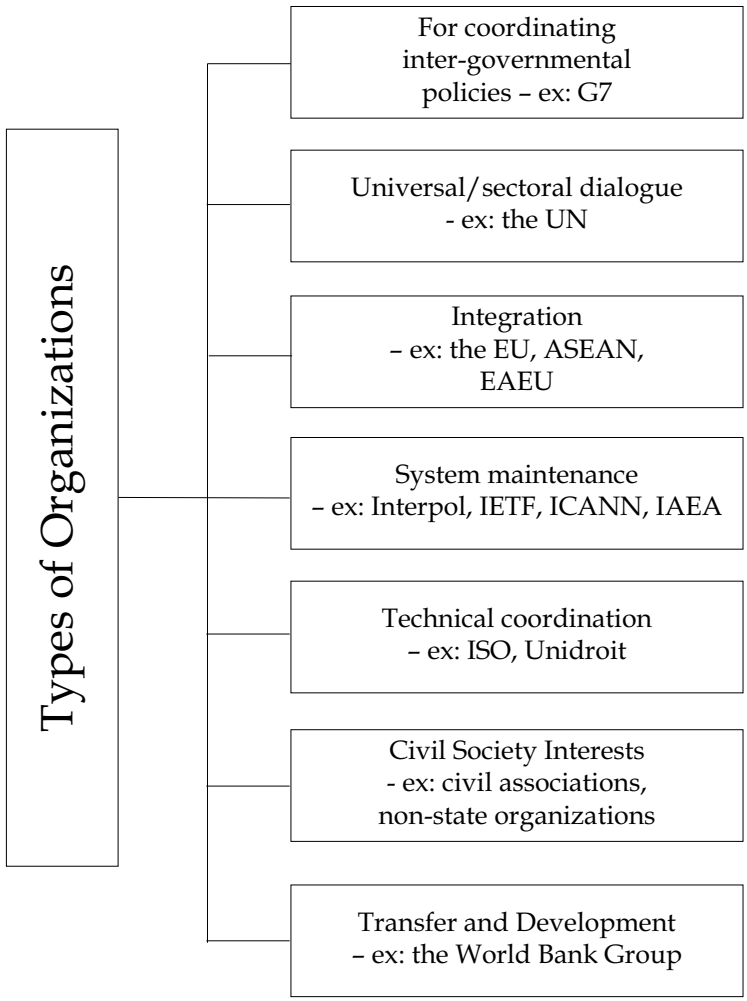
MANIFESTATIONS IN EXISTING ORGANIZATIONS

As mentioned in the introduction, at the forefront of dialogue, collective response, and decision-making on these issues have been the existing international organizations, on the basis of:

- Existing political capital;
- The ability to expand with new departments and working groups;
- The presence of core institutional expertise on various issues;
- Mandates that could be linked to issues related to CIP, such as counter-terrorism or technological issues;
- The convenience of introducing new topics into an already set agenda of discussions and schedule of meetings.

It should also be noted that both the states and the organizations find it useful to expand their work to include emerging issues.

Figure 1 – Types of international organizations,
from the perspective of CIP and emerging technologies



(Source: Authors)

Figure 1 presents the authors' vision of what the taxonomy of international organizations would look like from the perspective of tackling systemic issues related to critical infrastructures and emerging technologies. While instruments may vary, from a CIP perspective, an organization can belong to multiple groups, especially if we look at component agencies. This section will give examples from each category and also indicate where emerging technologies are applicable.

Organizations that coordinate inter-governmental policies give center-stage to states and act as a venue for like-minded countries to discuss common interests and formulate priorities and policies without an actual organizational mandate to impose or enforce commitments on members. These institutions have limited formalization and often provide no more than a Secretariat and semi-regular conferences between state representatives on various issues. The G7 is an example, as is the OECD, which has also developed a significant research and publishing arm to support the Member States. Their influence has also been felt in CIP and emerging technology issues. The OECD has published research and recommendations on, for instance, "Good Governance for Critical Infrastructure Resilience" (OECD, 2019). This issue was a natural fit for an organization purporting to represent advanced states, which have, by extrapolation, higher inventories of critical infrastructure and greater local and global interdependencies. Following an initiative by Canada and France during their respective G7 Presidencies, a Global Partnership for AI was launched by the OECD with 13 other founding members and with a Secretariat hosted within the OECD (Plonk, 2020). Previously, the OECD had launched the "OECD AI Principles" (OECD, 2022) as a Recommendation during the OECD Council Ministerial Meeting on 22-23 May 2019 (OECD, 2019), which became the basis for the G20 AI Principles (*Ibidem*). The involvement of the OECD in governance issues for emerging technologies goes back further in time, with examples such as the 1980 "OECD Guidelines for Privacy" (OECD, 1980).

Organizations that foster universal dialogue, such as the UN, and sectoral dialogue, such as the Paris Agreement, have a role to play when they can achieve some sort of common position or consensus among their constituents, who are generally heterogeneous, with different backgrounds, interests, resources, and perspectives that affect the degree to which they are willing to commit to binding commitments. Either a decision is not forthcoming, or the act of large group compromise leads to a race to the bottom of the lowest common denominator, resulting in ineffectual

agreements that have been significantly criticized for their inadequacy (Barrett, 2016). These organizations may contribute voluntary technical guidelines or declarations and resolutions that become a part of the corpus of law on international relations, steadily developing into norms, customs, and shared perspectives. Resolution 2341 (2017) of the United Nations Security Council referred to Critical Infrastructure Protection through "the growing importance of ensuring reliability and resilience of critical infrastructure and its protection from terrorist attacks for national security, public safety, and the economy of the concerned States as well as the well-being and welfare of their population" and stated that "as a result of increasing interdependency among critical infrastructure sectors, some critical infrastructure is potentially susceptible to a growing number and a wider variety of threats and vulnerabilities that raise new security concerns" (UNSC, 2017). On the technical side, we can give the recent example of the technical guidelines to facilitate the implementation of Security Council resolution 2370 (2017) and related international standards and good practices on preventing terrorists from acquiring weapons (UNIDIR, 2022), which also included segments on the threat of unmanned aerial vehicles to critical infrastructures.

Integrative organizations, of which the most notable representative is the EU, provide inspiration and models to others, aiming to move many state functions to the supra-national level, harmonizing legal and administrative frameworks, establishing common policies, freedoms, and even common binding governance structures. Security, especially of the non-military variety, is a natural direction of expansion for an organization that unifies markets and trading zones with various types of free movement. At a systemic level, these generate new risks, vulnerabilities, and threats because jurisdictional issues limit national agencies within their borders, allowing for interstices into which accidental and deliberate threats may grow. The European Union initiated a European Program for Critical Infrastructure Protection through Directive 114/2008 (EC, 2008), which was transposed into the member states' legislation for national CIP but also enabled the identification and designation of European CIs in the fields of energy and transport. More recent evolutions, with the impact of the pandemic in hindsight, include the proposed Critical Entities Resilience Directive (EC, 2020), which enlarges the taxonomy of European CIs to ten fields. The EU has also been very active in developing internal capacity and external partnerships for the development and governance of all emerging technologies, under the banner of "European strategic autonomy", "European data sovereignty", and "European technological sovereignty"

(Csernatoni, 2020). To the extent that they can summon the political will to do so, other such organizations will follow in their footsteps.

This category is self-explanatory. Organizations with narrow mandates, most of them technical, are empowered by member states or by other stakeholders to fulfill, in an independent manner, an important systemic function for the stability of the interdependent world. The best examples are the organizations dealing with the Internet, such as the Internet Engineering Task Force, the Internet Corporation for Assigned Names and Numbers, and others; organizations dealing with non-proliferation (International Agency for Atomic Energy), or dealing with international crime, including cybercrime (Interpol). The extent of their authority differs, especially when intruding on sovereign executive power, with police organizations like Interpol and Europol facilitating communication and cooperation between national police forces. Interpol can also create Incident Response Teams for disasters that include terrorist attacks, potentially on CIs.

Governance refers to the mechanisms, norms, methodologies, and practices on which normal activity and decision-making are based. In the case of CIP and emerging technologies, governance also includes the setting of standards, which is why standards organizations have such an important systemic role. They do not monopolize the standard-setting agenda, which is also done by states with vested interests engaging in regulatory and cyber diplomacy on a multilateral basis, but they often provide the most widespread standards, borrowing from best practices in the field, ultimately affecting CIP and other areas of governance. Examples include the International Standards Organization in the widest possible variety of fields, Unidroit (the International Institute for the Unification of Private Law) in the area of commercial law, and many others. These have a systemic effect by enabling better system interconnectivity through similar procedures, technical standards, and governance models, thereby reducing friction between actors from different countries.

Civil society associations can also fulfill an important supporting role by acting as focal points for particular sectoral interests and perspectives, often as an alliance of national organizations that want to act globally or pursue goals directly or through advocacy. One less-known example is the International Association of Critical Infrastructure Protection Professionals (IACIPP), which organizes yearly specialty events in North America, Europe, and Asia, bringing together experts and companies to discuss the latest developments.

Entities engaging in financial transfers and in development feature an important component related to the funding of new critical infrastructures, the raising of capacity in existing ones, including in public services and administration (a CI field in European taxonomies), and indirectly assisting in technology transfers and leapfrogging development by applying the latest technologies from the start. Organizations include those in the World Bank Group but also the various national development banks with an international outlook, such as the China Development Bank or the Development Bank of Japan.

It is important to note that many new entries on the list of international organizations with a CI or CIP orientation, including as part of strategies for the global advancement of states' interests, will fit into one of the categories, even as they are perceived to be in competition with them. A clear example stems from the institution-building undertaken by China under its Belt and Road Initiative, or the BRICS, which also included multilateral financial institutions such as the Asian Infrastructure Investment Bank (AIIB) and the New Development Bank (perceived as adversarial towards the supposedly Western-led World Bank) or the Chang Mai Initiative (an alternative to the IMF). Often, there is clear or hidden cooperation between such entities, at least in the beginning, as transfers of knowledge and best practices are required to improve outcomes. The World Bank and the AIIB signed a cooperation protocol in 2017 and are co-funding five projects (AIIB, 2017). Members such as Germany signed up for the AIIB, publicly stating, in the face of US opposition towards what it sees as a challenge from China, that its membership will allow the transfer of good practices in international project selection, funding, and management (Stanzel, 2017). Lastly, we should note that the inclusion of CIP and emerging technology issues in the purview of existing international organizations also involves new methods and instruments, such as cyber diplomacy, which is the use of traditional diplomatic tools to solve issues relating to digitalization and cyber security and which is becoming a new field of study in International Relations (Georgescu et al., 2020).

NEW FORMS OF ORGANIZATION

In addition to the new individual entries into the roster of existing international organization types with systemic roles related to CIP and emerging technologies, there are also a series of new models for

international strategic cooperation on CI issues and emerging technologies. On average, we would summarize that these types of organizations are:

- Low on formality – they do not feature extensive attached organizations, with large departments and permanent expert contributors;
- Non-exclusive – in the fluid state of international relations following the rapid advancement of technology and the changes in the source of state influence and power, the most powerful states have only a limited ability or willingness to coerce absolute adherence to their preferred models and development tracks. States can, and often do, try to play various sides off of each other to get better funding opportunities, bespoke attention and other concessions, as well as try to balance various interests to maximize economic gains;
- Multistakeholder – state-only forms or venues of cooperation are possible, but only as a component of a wider system that inevitably has to include other stakeholder types, from the business world, academia and civil society, especially where these bring to the table expert knowledge and insight into the problems at hand, where they are necessary for legitimizing measures, and where they are powers unto themselves when it comes to the technological issues (ex: the tech giants or large industrial concerns which are key to the rapid adoption of emerging technology – ex: automotive companies and AI) (Musetescu et al., 2022);
- They are often spearheaded by a state but become multilateralized – states may formulate competing visions, standards, and projects in fields that are still open to this competition to generate advantageous path dependencies, but they find it difficult to unilaterally achieve technological domination or other forms of exclusive influence when peer states can mobilize similar resources. Attracting and retaining partners becomes vital, not just in terms of resources but also for credibility and, ultimately, international backing. The US Department of Defense warned that, on the 5G issue, the US would not be able to sustain by itself the level of investment necessary in maintaining innovation rates should it fail to achieve domination or at least parity in market control with the Chinese-preferred standards – that "China is on track to repeat in 5G what happened with the United States in 4G" and "Chinese internet companies will be well-positioned to develop services and applications for their home market that take advantage of 5G speed and low latency. As 5G is deployed across the globe in similar bands of spectrum, China's handset and internet applications and services are

likely to become dominant, even if they are excluded from the US" (Medin & Louie, 2019). It would inevitably fall behind, with an impact on security capability, not just economic outcomes, similar to how the field of operating systems for personal computers and smartphones (and other devices) has registered a growing concentration. Another example is that of the Belt and Road Initiative becoming, gradually, more multilateral as other sources of capital are required to maintain capital allocation and investment growth rates, provide credible governance, and reduce criticism (Ding et al., 2020). The founding state's influence will probably remain very strong in how the organization views things and plans its approach;

- Single issue – except for strategic infrastructure expansion and integration initiatives, which cover geographic areas (like the Belt and Road Initiative), most new forms of strategic cooperation will tend towards being single-issue organizations because their agendas, instruments, and action plans will require highly specialized knowledge and multistakeholder bases, which are not always compatible with generalist organizations and oversight.

We can give the following examples of new forms of international strategic cooperation, without attempting to formulate an encompassing taxonomy to cover them all:

- The Belt and Road Initiative – while strongly hampered by the pandemic effects and by Western political maneuvering that rightly sees a very strong systemic value, the BRI is a multi-sector strategic initiative for Eurasian integration (although it now touches on East Africa as well) which relies on the Chinese capacity for long-term mobilization of resources to achieve technically complex tasks, such as infrastructure design, funding, technological sourcing, building and operation, through comprehensive partnerships with numerous state and non-state stakeholders (Caba-Maria et al., 2021). It is designed to leverage Chinese advantages in these fields and to support internal Chinese goals, such as shifting the economic development model to avoid the "middle-income trap", exporting excess infrastructure building capacity, becoming an exporter of technology, capital, and innovation, and securing critical resources and markets (Caba-Maria et al., 2021). It has an extensive diplomatic and international relations background, relying on integrating visions for Chinese regional initiatives and promoting lockstep cooperation along its mainland corridors and maritime belt in order to increase connectivity. With the launch of the Health Silk Road,

Digital Silk Road, and the BRI Spatial Information Corridor, a strong emerging technology component has been introduced to the practice of comprehensive partnerships (Liu, 2017);

- The Blue Dot Network – the main US answer to the Chinese BRI, leveraging US strong points in the creation and maintenance of international partnerships to influence governance at a strategic level. The network does not aim to build infrastructure but rather to create a set of standards in terms of sustainable infrastructure creation in areas such as labor, environmental impact, resilience, and sustainable financing that incorporate its criticisms of Chinese-led projects, forcing standards-adopters to limit cooperation with China or forcing China to adapt its projects to these new requirements. A prior example of this is how China is trying to green the Belt and Road Initiative project, in response to European criticism and pressure over the funding of polluting energy projects;
- 3GPP – the 3rd Generation Partnership Project is an umbrella organization for standards groups in the communications industry which has a growing influence over the 5G standards competition;
- The Partnership for Defense initiated by the US includes an AI dimension and partners with NATO states (the UK, Canada, Denmark, Estonia, France, and Norway) as well as non-NATO like Australia, Japan, and South Korea in the Indo-Pacific region and Israel, Finland, and Sweden in the general European area (the latter two prospective NATO members). Drake (2022) noted the overlap with the EU, relevant to the following point, and suggested that this useful cyber diplomacy tool can be extended towards Africa, as a foil to Chinese efforts, including on emerging technology issues;
- We would also include here the EU-US Trade and Technology Council, as a transatlantic forum that has to manage entrenched differences and leverage common perspectives to achieve collective action on issues such as supply chain security and communications technology, related to critical infrastructure protection, but also emerging technologies, like AI (which has a dedicated working group) (Muşetescu et al., 2022).

Future modes of organization of international strategic cooperation will have to be flexible enough to keep up with rapid technology-induced shifts in agendas, interests, and relative strengths while being strong enough to nevertheless establish norms, standards, and homogenize security

perspectives to promote cooperation despite rivalries and generate the premises for collective action.

CONCLUSIONS

Recent events, such as the pandemic, the energy and logistics volatility, and the serial financial contagions, have confirmed that a strongly interconnected and globalized world is not only a richer, more productive, and more efficient place, but also one exposed to new risks, vulnerabilities, and threats. These include both accidental ones derived from complexity and spontaneous malfunctions, but also deliberate ones coming from state actors and groups with the capacity and know-how to enact disruptive events for ideology and profit. The framework of Critical Infrastructure Protection allows us the concepts and tools to create a systemic view of world issues, which are undergoing rapid shifts, including as a result of emerging technologies. International organizations have to manage the challenges resulting from global interconnectivity and the challenges of sustainable adoption of emerging technologies in the context of inter-state rivalries. For the most part, existing organizations and organization types are handling these systemic roles. However, new forms of organizations are emerging, better suited to this specific type of international strategic cooperation in the current context. This article provides an overview of these issues and the current trends.

REFERENCES

Barrett, S. (2016). The Paris Agreement: We Can Do (and Have Done) Better. In: Stavins, R. N., Stowe, R. C. (eds), *The Paris Agreement and Beyond: International Climate Chang*. Harvard Project on Climate Change, Belfer Center. Retreived from: http://www.belfercenter.org/sites/default/files/legacy/files/2016-10_paris-agreement-beyond_v4.pdf. Accessed 4.03.2022.

Caba-Maria, F., Georgescu, A., Mureşan, L., Muşetescu, R. C. (coord.) (2020). Promoting the Belt and Road Initiative and 17 + 1 Cooperation in Central and Eastern Europe, from the Perspective of Central and Eastern European Countries, *Eikon.* Retreived from: https://mepei.com/report-policy-analysis-promoting-the-belt-and-road-initiative-and-17-1-cooperation-in-central-and-eastern-europe-from-the-perspective-of-central-and-eastern-european-countries/ Accessed 24.03.2022.

Csernatoni, R. (2021, August 12). The EU's Rise as a Defense Technological Power: From Strategic Autonomy to Technological Sovereignty. *Carnegie Europe*. Retrieved from: https://carnegieeurope.eu/2021/08/12/eu-s-rise-as-defense-technological-power-from-strategic-autonomy-to-technological-sovereignty-pub-85134. Accessed 1.02.2021.

Ding, Y., Xiao, A., Tian, E. (2020, June 15). China's Belt and Road initiative in a post-pandemic world. Invesco Limited Market Views. Retrieved from: https://www.invesco.com/invest-china/en/institutional/insights/chinas-belt-and-road-initiative-in-a-postpandemic-world.html. Accessed 24.01.2021.

Drake, B. (2022, June 1). Protecting American investments, In: *AI. War on the Rocks*. Retrieved from: https://warontherocks.com/2022/06/protecting-american-investments-in-ai/ Accessed 24.03.2022.

European Commission. (2008).Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Retrieved from: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32008L0114. Accessed 23.12.2008.

European Commission. (2020, December 16). COM(2020) 829 final – Proposal for a Directive Of The European Parliament and of the Council on the resilience of critical entities. Retrievede from: https://eur-lex.europa. eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0829& from=EN. Accessed 2.1.2021.

Georgescu, A. (2018). Pandora's Botnet – Cybercrime as a Persistent Systemic Threat. Future of Europe: Security and Privacy in Cyberspace, *Visio Journal*, (3).

Georgescu, A., Gheorghe, A., Piso, M.-I., Katina, P.F. (2019a). *Critical Space Infrastructures: Risk, Resilience and Complexity.* Topics in Safety, Risk, Reliability and Quality, Series 36, (eBook), DOI 10.1007/978-3-030-12604-9, New York, Springer International Publishing.

Georgescu, A., Vevera, V., Cirnu, C.E. (2019b). The Proliferation of Cyber Weapons -Theory and Mitigation, *Romanian Cyber Security Journal*, 1 (2), pp. 37-46.

Georgescu, A., Vevera, V., Cirnu, C.E. (2020, September). A Critical Infrastructure protection Perspective on Counter-Terrorism in South-Eastern Europe. In: Caleta, D., Powers, J.F. (eds), *Cyber Terrorism and*

Extremism as a Threat to Critical Infrastructures, Slovenian MoD and Special Forces University in Tampa, Florida, Ljubljana.

Georgescu, A., Vevera, V., Cirnu, C.E. (2020). The Diplomacy of Systemic Governance in Cyberspace. *International Journal of Cyber Diplomacy*, 1 (1), pp. 79-88.

Gheorghe, A., Vamanu, D.V., Katina, P., Pulfer, R. (2018). *Critical Infrastructures, Key Resources, Key Assets: Risk, Vulnerability, Resilience, Fragility, and Perception Governance*, Topics in Safety, Risk, Reliability and Quality. New York, Springer International Publishing. https://doi.org/10.1007/978-3-319-69224-1

Gheorghe, A.V., Schlapfer, M. (2006). Ubiquity of Digitalization and Risks of Interdependent Critical Infrastructures, In: 2006 *IEEE International Conference on Systems, Man and Cybernetics*, pp. 580–584.

Good Governance for Critical Infrastructure Resilience. (2019, April 17). OECD Reviews of Risk Management Policies, as OECD. Retrieved from: https://www.oecd.org/governance/good-governance-for-critical-infrastructure-resilience-02f0e5a0-en.htm. Accessed 2.02.2020.

Keating, C.B., Bradley, J.M. (2015). Complex system governance reference model. *International Journal of System of Systems Engineering,* 6, pp. 33–52.

Liu, Z. (2017). China-CEEC Cooperation: China [is] building of a new type of international relations. In: S. Šelo Šabić and V. Vernygora (eds), *Special Issue of Croatian International Relations Review* (pp. 19-34). Zagreb, Institute for Development and International Relations, 23 (78).

Medin, M., Louie, G. (2019, April 9). The 5G Ecosystem: Risks & Opportunities for DoD. Defense Industrial Board Report, US Department of Defense. Retrieved from: https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF. Accessed 2.02.2020.

Memorandum of Understanding. Asian Infrastructure Investment Bank – AIIB. (2017, April 23). Retreived from:https://www.aiib.org/en/news-events/news/2017/_download/world-bank-aiib-sign-cooperation-framework.pdf. Accessed 22.12.2020.

Mu□etescu, R.C., Volintiru, C.A., Georgescu, A., Fran□escu, D.P. (2022). The consolidation of the EU-US relationship in the new geopolitical context, including from the perspective of managing emerging technologies. Opportunities for Romania. *Studies in Strategies and Policies SPOS 2021*, European Institute of Romania. Retreived from:

http://ier.gov.ro/wp-content/uploads/2022/03/Studiul-5_Relatia-UE_SUA_final_site.pdf. Accessed 22.2.2022.

OECD AI Principles overview (2022). OECD.AI Policy Observatory, Organisation for Economic Co-operation and Development. Retreived from: https://oecd.ai/en/ai-principles. Accessed 22.2.2022.

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

Plonk, A. (2020, July 9). The Global Partnership on AI takes off – at the OECD. OECD. Retreived from: https://oecd.ai/en/wonk/oecd-and-g7-artificial-intelligence-initiatives-side-by-side-for-responsible-ai. Accessed 9.6.2020.

Preventing terrorists from acquiring weapons. (2017). Technical guidelines to facilitate the implementation of Security Council resolution 2370 and related international standards and good practices on preventing terrorists from acquiring weapons. UN Institute for Disarmament Research / United Nations. Retreivede from: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/cted_guidelines_2370.pdf. Accessed 18.03.2022.

Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. Organisation for Economic Co-operation and Development. (1980, September 23). OECD/LEGAL/0188. Retreived from: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188. Accessed 1.02.2022.

Recommendation of the Council on Artificial Intelligence. Organisation for Economic Co-operation and Development (2019, May 22). OECD/LEGAL/0449. Retreived from: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. Accessed 1.02.2022.

Resolution 2341 (2017, February 13). Threats to international peace and security caused by terrorist acts. S/RES/2341. Retreived from: http://unscr.com/en/resolutions/doc/2341. Accessed 1.02.2022.

Stanzel, A. (2017, April 23). A German view of the Asian Infrastructure Investment Bank. European Council on Foreign Relations. Retreived from: https://ecfr.eu/article/commentary_a_german_view_of_the_aiib_7275/. Accessed 18.03.2022.