Possible risks in implementing key partnerships to optimize critical infrastructure security

Valeri Panevski
Institute of Metal Science Equipment and Technologies with Hydro- and Aerodynamics Centre "Acad. A Balevski"
at the Bulgarian Academy of Sciences, 67 Shipchenski Prohod Street, 1574 Sofia, Bulgaria
panevski@ims.bas.bg

Abstract: *In international scientific circles, with a portfolio in the field of critical infrastructure security, there is consent that the main problem underlying the difficulty in securing critical infrastructure against various types of threats is the lack of a common understanding of what constitutes critical infrastructure. This challenge could hinder coordinated threat assessment, mutual assistance, and the implementation of key partnerships in prevention and response efforts, as intruders often define critical infrastructure based on its potential to cause maximum disruption.*

This publication presents in a systematized form some directions in the author's experience in developing approaches in building key partnerships for optimizing the security of critical infrastructure in the conditions of the QUASAR competence center.

Keywords: *POTENTIAL RISKS, KEY PARTNERSHIPS*

1. Introduction

One of the directions in implementing the collaborative research approach is the establishment of key partnerships in the development of critical infrastructure (CI) security systems, which creates the opportunity to gain access to external sources of resources and high technologies and their integration into applied scientific developments.

A successful practice over the last decade has been the establishment and operation of centers of competence (CCs), in which scientific research and innovation are the key to improving business skills, expanding the portfolio of products and services, and maintaining cutting-edge applied research in support of societal security. The establishment and operation of CCs in our country plays a leading role in planning, structuring, and negotiating mutually beneficial collaborations between universities, research institutes, and high-tech companies of various sizes, with the proper establishment and operation of appropriate business models playing a significant role in this regard.

Competence centres are defined as structured, long-term collaborations for research and innovation in strategically important areas between academia and industry with frequent interactions with the public sector **[1]**. Their activities are focused on strategic research programs and maintain strong links between science and industry, thus ensuring collaborative research with a medium and long-term perspective. They are usually located in research organisations and direct their activities in the interest of national strategic sectors through applied research projects in collaboration with leading business organisations.

An example of a modern approach to the implementation of key partnerships is Project BG16RFPR002-1.014-0008 "Sustainable development of Center for Competence "Quasar", which operates in accordance with the procedure through direct provision of grant aid BG16RFPR002-1.014 "Sustainable development of Centers of Excellence and Centers of Competence, including specific infrastructures or their associations by NRSI". The aim of this procedure is to support the sustainable development of Centers of Excellence and Centers of Competence, established under the SEGS, to "..stimulate their cooperation with business…" through technology transfer, their full integration into the research and innovation ecosystem of our country and increase their contribution to smart economic transformation.

2. Challenges in ensuring the security of critical infrastructure

Ensuring the security of CI is a difficult task due to the fact that CI systems are:

- highly interconnected and interdependent, so that an interruption in one critical system can cause a chain reaction or series of failures in other systems.
- often built on the basis of technological systems created years ago, which were not designed with security in mind, which is why they can have vulnerabilities that are difficult to detect and fix.
- subject to a wide range of threats, including cyberattacks, physical attacks, natural disasters and human errors, making it difficult to protect them from all possible risks.

To improve the security of CI, it is appropriate to use modern international practices, formulated and developed in the standards of ISO/TC 292 "Security and resilience" and ISO/TC 262 "Risk management", aimed at the following areas, but not limited to:

- *Risk Assessment:* Conducting a risk assessment is a key step in ensuring CI, which involves identifying and analyzing the threats and vulnerabilities of CI systems **[2,3]**.

ISO 31000 Risk management — Guidelines;

ISO/TS 22317 Security and resilience — Business continuity management systems — Guidelines for business impact analysis.

- *Threat Intelligence*: The collection and analysis of threat intelligence is essential for identifying potential threats to CI systems. This process involves monitoring the threat landscape - cyber, physical, and natural threats.

ISO 22342 Security and resilience — Protective security — Guidelines for the development of a security plan for an organization

- *Access Control:* Implementing strong access control systems can help prevent unauthorized access to critical infrastructure systems and allows access only to authorized personnel. Access control involves implementing strong authentication measures, such as multi-factor authentication, and restricting access to authorized personnel based on their job titles and responsibilities.

ISO 22340 Security and resilience — Protective security — Guidelines for an enterprise protective security architecture and framework

ISO 22342 Security and resilience — Protective security — Guidelines for the development of a security plan for an organization

- *Cybersecurity measures:* Adopted cybersecurity measures, such as firewalls, create the conditions for perimeter protection. Developed intrusion prevention systems and robust encryption protocols can help protect critical infrastructure systems from cyberattacks.

ISO 22340 Security and resilience — Protective security — Guidelines for an enterprise protective security architecture and framework

- *Physical security measures:* The use of physical security systems can improve the protection of critical infrastructure from physical impact.

ISO/TS 22317 Security and resilience — Business continuity management systems — Guidelines for business impact analysis;

ISO 22342 Security and resilience — Protective security — Guidelines for the development of a security plan for an organization.

- *Incident Response Planning:* Developing and implementing a risk event response plan is critical to the security of the CI. Conducting training and education with the security team to ensure that the response plan is effective is key to success against the possible impact of risk events.

ISO/TS 22332Security and resilience — Business continuity management systems — Guidelines for developing business continuity plans and procedures.

Solving this task is possible through the key partnerships created within the scope of the CCs.

3. Building key partnerships through the CCs

The main operational objective of the CC is to strengthen partnerships between scientific organizations, universities and industry, thereby accelerating the innovation process and leading to economic growth **[4]**. This is achieved by:

- the presence of the private sector in the management and leadership structures;
- the provision of services to the private sector;
- directing the work of academia towards modern applied research;
- facilitating interregional connections through participation in international projects.

CCs can implement good practices separate from the work on the R&D programme, focusing on:

- exploitation of research results through intellectual property rights and individual products;
- training of doctoral students;
- dissemination of research results through publications, conferences, etc.;
- stimulation of networking and knowledge transfer;
- acquisition of funding from third parties (including EU sources);
- provision of research infrastructure;
- provision of market information.

These good practices should offer key insights for the management of the centres, namely:

- CCs should be flexible in finding support and developing research projects with different funding mechanisms for products and systems with different TRLs;
- A market-oriented integrated *one-stop-shop* CC should offer different types of services to promote collaboration between science and industry;
- Developing international collaboration through bilateral contractual applied research and development should be a strategic objective.

More about key partnerships

Organizations create partnerships for many reasons, and they become the cornerstone of many business models. The partnerships they build help optimize BM, reduce risk, or acquire resources.

Motives for Key Partnerships

The following motives for establishing partnerships through CCs can be structured:

Optimization and Economies of Scale

The most basic form of partnership or buyer-seller relationship is designed to optimize the allocation of resources and activities. It is illogical for one organization to own all the resources or perform every activity alone. Partnerships for optimization and economies of scale are usually created to reduce costs and often involve outsourcing or sharing infrastructure.

Reducing Risk and Uncertainty

Partnerships can help reduce risk in a competitive environment characterized by uncertainty. It is not logical or common for competitors to form a strategic alliance in one area while competing in another.

Acquisition of certain resources and activities

Few organizations own all the resources or perform all the activities described by their business models. Rather, they extend their own capabilities by relying on other organizations to provide certain resources or perform certain activities. Such partnerships may be motivated by the need to acquire knowledge **[5,6]**, licenses, or access to customers.

Integrating Key Partners into the Business Plan

Integrating key partners into the business plan is a key aspect of building a robust and scalable business model. Within the business model, key partners are not just an afterthought – they are fundamental to delivering a value proposition, maintaining strong customer relationships, and unlocking new revenue streams. By carefully identifying and incorporating strategic partnerships, a business can gain access to key resources, specialized expertise **[7,8,9]**, and operational capabilities that would otherwise be unavailable.

When writing a business plan, it should clearly outline how each key partner will contribute to the success of the business. For example, a technology provider may provide the infrastructure needed to deliver your product, while a logistics partner ensures efficient distribution to your target market. These relationships can help reduce costs by allowing you to outsource non-core activities, streamline your supply chain, and focus on what your business does best.

4. Potential risks of key partnerships

Key partnerships can bring benefits, such as access to new markets, sharing resources and improving capabilities **[10].**

In the course of their implementation, risks may arise, namely:

- *Irrelevant between goals and values* – one of the main risks is the potential mismatch between the strategic goals, values, corporate culture of the partners, which can lead to conflicts, inefficiency of the activity and interruption of cooperation.
- *Dependencies* – dependence on a given partner can be risky, especially for partners experiencing financial difficulties, changing their strategic directions or becoming competitors*;*
- *Brand and reputational impairment* - associating with another organization may lead to the risk of brand dilution/distortion/reduction of brand value and reputational damage, in a way inconsistent with the organizations' values or the partnership is perceived negatively by customers or stakeholders.
- *Operational challenges* - integrating processes, systems and teams can be comprehensive and resource-intensive. Operational inefficiencies may increase, particularly if there are significant differences in the operating models and corporate cultures of the partnering organizations.
- *Risks related to intellectual property rights and sensitive information* - sharing with a partner may lead to the risk of intellectual property theft, leakage of confidential information or the partner acquiring sufficient knowledge to become a competitor.
- *Legal and compliance risks* – there are potential legal risks involved in forming a partnership, particularly when it involves different jurisdictions. Compliance with international law, industry regulations and antitrust laws can be complex and costly.
- *Financial risks* – there are inherent financial risks, including significant investments without the expected return. Financial obligations can strain the budget and the allocation of commitments to returns can lead to disputes.
- *Performance risks* – there are always risks that one or all parties may fail to meet their obligations, which could impact the partnership and its strategic objectives.
- *Conflict of Interest* – Strategic partnerships can lead to situations where the interests of the partner organizations may conflict with each other, especially in decisions that affect the direction of the partnership or the allocation of resources.
- *Partnership exit difficulties* – This procedure can be complex, expensive, and have an impact on the reputation and operations of the partners. This is especially true when there are no clearly formulated exit clauses and if the partnership has highly integrated operations.

5. Conclusions

There are numerous reasons for selecting a key partner, some of which are essential for the success or failure of research outcomes. The right partnerships are crucial to the success of a project, as they drive the achievement of planned end results, scientific and operational support, and help achieve strategic objectives - development of a CI security model.

Partnerships can optimize resource utilization, improve supply chains, and reduce risk, particularly in the area of research to create or optimize CI security.

While successful partnerships can be established within the scope of the CC, it is important to recognize that not all relationships are beneficial to achieving planned outcomes, and careful evaluation is therefore necessary.

Last but not least, key partners may change throughout the life cycle of applied scientific developments, which necessitates an approach of continuous monitoring of the applied partnership model (including the business model of scientific research and development), as well as conducting a review and update.

Acknowledgments

I would like to express my gratitude to programme “Research, Innovation and Digitalisation for Smart Transformation” 2021-2027, funded by the European Union, Project BG16RFPR002-1.014-0008 “Sustainable development of Center for Competence “Quasar” for supporting this article.

References:

[1] TAFTIE (The European Network of Innovation Agencies), Future Competence Centre Programmes, “Report of the TAFTIE Task Force on Competence Centre Programmes CompAct”, May, 2016;

[2] Tumbarska A. Use of unmanned aerial systems as platforms for terrorist attacks. Proc. International Scientific Conference on Security "ConfSec 2024", 8, 1, STUME, 2024, ISSN:print 2603-2945, online 2603-2953, 33-36

[3] Tumbarska A. Non-lethal technologies for forced stopping potentially dangerous vehicles and vessels. International Scientific Journal “Security&Future”, 5, 2, STUME, 2021, ISSN:2535-0668, 71-74

[4] European Union, European Regional Development Funds, „Accelerating the Innovation Process through Centres of Competence“, 12/02/2020, Policy Learning Platform, https://www.interregeurope.eu/policylearning/news/7724/accelerating-the-innovation-process-through-centres-of-competence/ ;

[5] Dimitrov, D, Randelova N. Methods and approaches for the preparation of a comparative analysis of critical infrastructures. Analysis evaluation criteria. Criteria for evaluating the analysis. International Scientific Journal "Security&Future", 8, 3, STUME, 2024, ISSN:PRINT 2535-0668, ONLINE 2535-082X, 73-75;

[6] Dimitrov, D, Randelova, N. Introduction in the management system at Kozloduy NPP supporting Process 8 “Training and qualification”. International Scientific Journal "Security&Future", 8, 1, STUME, 2024, ISSN:2535-0668 (print); 2535-082X (online), 15-17;

[7] Nesterov K.N., Pehlivanski V.I., Lyaskov N.G., Penev N.P.. Research into the capabilities of a multi-channel radio frequency spectrum jammer used by UAVs. Proceedings XIII International Scientific Conference on „TECHNICS. TECHNOLOGIES. EDUCATION. SAFETY 2025”, 01-04.09.2025 VARNA, BULGARIA, ISSUE 1 (18), 2025, ISSN:ISSN 2535-0315(Print), ISSN 2535-0323 (Online), 142-144;

[8] Gueorgiev, Nikolay, Konstantin Nikolov, Albena Taneva. Algorithm for detection of low-flying small objects from background radar.. Proceedings of 13th International Scientific Conference “TechSys 2024 – Engineering, Technologies and Systems”, Technical University of Sofia. Plovdiv, 16-18.05.2024, Ref. Scopus, 2024, DOI:AIP Conf. Proc. 3274, 020002 (2025), https://doi.org/10.1063/5.0258670, SJR (Scopus):0.02;

[9] Nikolay Litchkov, Konstantin Nesterov, Atanas Nachev, Daniela Pavlova, Panayot Gindev, Yavor Boychev. Modeling of the Reflecting Surface for Bistatic Radars of Low-Flying Small Object. Proceedings of 13th International Scientific Conference “TechSys 2024 – Engineering, Technologies and Systems”, Technical University of Sofia. Plovdiv, 16-18.05.2024, Ref. Scopus, 2025, DOI:https://doi.org/10.1063/5.0258737, SJR (Scopus):0.2;

[10] https://entrepreneursmentor.co.uk/knowledge-base/what-are-the-risks-of-a-strategic-partnership/.