Structuring key partnerships in the field of critical infrastructure security systems

Valeri Panevski[1*], Lyudmil Nedelchev[2]
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[1]
panevski@ims.bas.bg
Kozloduy NPP EAD, 3321, Kozloduy[2]
lnnedelchev@npp.bg

Abstract: *Joint scientific and applied research occupies its place as a major innovation process in the activities of scientific, educational and business organizations. The purpose of this approach is to gain access to external sources of technology (or other assets) and their integration into products and services to build security of critical infrastructure and strategic sites of national importance.*

Partnerships in the development of security systems can bring added value to partner organizations, allowing them to use a wider network of promising assets and markets and helping them gain trust and prestige in society.

The presentation of a variant of structuring key partnerships in the development of security systems is the content of this paper.

Key words: *KEY PARTNERSHIPS, COMPETENCE CENTRE*

1. Introduction

The purpose of building key partnerships, within the scope of Competence Centers (CCs), is to establish relationships through which to gain access to external sources of high technology (or other assets) and their integration into products and services in the field of security systems for critical infrastructures and objects of national importance. The implementation of research and innovation (R&I) in the development of security systems and the related business model (BM) makes a significant contribution in this area.

R&I refer to that part of BM that represents the ability to acquire knowledge, design, develop and improve products, services, technologies or processes. For high-tech CC partners, R&I is number one on the list of opportunities that are critical to long-term success while at the same time being the key to improving business skills, expanding the portfolio of products and services and maintaining cutting-edge applied research in the interest of the country's security.

CCs are defined as "structured, long-term research and innovation (R&I) collaboration in strategically important areas between academia and industry with frequent interactions with the public sector. A CoC focuses on strategic research agendas, support strong interactions between science and industry and provides truly collaborative research with a medium to long-term perspective" **[1]**. They are usually located in research organizations and focus on national strategic sectors in applied research projects in collaboration with leading business organizations.

The establishment and operation of CC in our country, such as the Project BG05M2OP001-1.002-0006 Competence Center "Quantum Communication, Intelligent Security and Risk Management Systems (Quasar)", plays a leading role in planning, structuring and negotiating these relationships between research organizations, universities and high-tech companies.

2. Building key partnerships through competence centers

The CC's main operational objective is to strengthen partnerships between research organizations, universities and industry, thus accelerating the innovation process and leading to economic growth.

This is achieved through:

- the presence of the private sector in the management and leadership structures;
- provision of services to the private sector;
- directing the work of the academic circles to modern applied research;
- facilitating interregional relations through the participation of international companies.

Competence centers can apply good practices, separate from the work of the research and development program, with a focus on:

- use of research results through intellectual property rights and individual products;
- training of doctoral students;
- dissemination of research results through publications, conferences, etc.;
- stimulating networking and knowledge transfer;
- acquisition of funding from third countries (including EU sources);
- provision of research infrastructure;
- providing market information (TAFTIE, 2016) **[1]**

These good practices should offer key insights for CC management, namely:

- to be flexible in finding support and developing research projects with different funding mechanisms, for products and systems with different technology readiness levels (TRL);
- a market-oriented integrated CC must offer different types of services to promote cooperation between science and industry;
- international cooperation development through bilateral contractual applied research and development should be a strategic goal.

3. More on key partnerships

Organizations form partnerships for many reasons, and partnerships are becoming a cornerstone of many business models. Established partnerships help to optimize business models, reduce risk and acquire resources.

3.1 Motives for key partnerships

Optimization and economy of scale

The most basic form of partnership is designed to optimize the allocation of resources and activities. It is illogical for an organization (in this case a CCP) to have all the resources or to carry out every activity alone. Optimization and economies of scale partnerships are usually set up to reduce costs and often involve outsourcing or sharing infrastructure.

Reduce risk and uncertainty

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

Acquisition of certain resources and activities

Few organizations have all the resources or carry out all the activities described by their business models. Rather, they expand 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, licenses or access to clients.

3.2 Partnerships, the power of information sharing.

Despite the overall change in attitudes, key CC partners still have reservations about sharing information. The following main areas of concern can be identified:

- Partner organizations are concerned about the legal and regulatory implications of disclosing development information;
- Organizations are concerned about the public relations aspect;
- Organizations are concerned about the confidentiality of the data they work with.

Information security has become a risk management issue due to its potential effects. Leakage of information revealing potential results of scientific research can have legal consequences: the organization may be required to report related issues in order to comply with financial and confidentiality regulations **[2]**. If security issues become public, they can also harm the way the partner organization is perceived by customers and the business community, potentially affecting the profitability of the CC. For example, information sharing may reveal constructive and technological data that could potentially compromise the privacy of the affected partner organization.

The need to share security information is driven by rapidly changing businesses, technologies and threats. Increasingly, CC consists of a wide variety of key partners. We share business information and often use the same technology or sell or share technology with each other. As we do this, we also share the risks. Understanding the risks our partners face and how they manage those risks can help us protect our own organizations.

Looking more broadly into the technological landscape, all systems and devices are to some extent connected, whether owned by businesses, individuals or service providers. Almost every aspect of society depends on a global, fast-growing, extremely complex network of devices and services. This provides the central nervous system that supports innovation, economic development and social interaction worldwide. But because we are all inherently interconnected, we share common risks. The landscape of threats is dynamic, global and increasingly complex. Threats can arise in any country and then spread rapidly across national and corporate borders, causing significant damage to organizations and individuals around the world. Because threats are spreading so fast and the landscape of threats is so complex, it is difficult for any individual organization to get a clear picture of all potential vulnerabilities, threats and attacks.

External partnerships can be useful, because they provide additional intelligence that can be used to improve the security position. By sharing information with other organizations, it can be achievedr a better understanding of what is happening outside of our own environment. We learn about new threats before they affect us directly. In this way information is obtained about how other organizations are dealing with these threats and we can touch to the best practices for managing security activities. By using the information we gather from external relationships, we can increase the partner organization's ability to feel, interpret, and act on risk.

Purpose of forming partnerships

There are a number of reasons why developing a key partnership in a CCP can be beneficial. Generally speaking, partnerships can focus on a specific problem, such as developing security systems, to maintain a consistent approach to problems **[3]**.

Some more specific reasons for forming a partnership may be:

- Achieve more efficient and effective implementation of development programs and eliminate any unnecessary duplication of effort. Gathering organizations involved in solving a problem can lead to more cohesive and comprehensive intervention. Instead of duplicating efforts, partners can share or coordinate responsibilities in ways that give more participants access to the programs and allow for a wider range of services.
- Pooling resources. Many organizations together may have the resources to accomplish a task that none of them could accomplish on their own. In general, organizations form partnerships to achieve together what they cannot do alone.
- To increase communication between groups and break stereotypes. Bringing together organizations from many sectors of the community can create alliances where there has been little contact before. Working together to achieve common goals can help organizations break down barriers and perceptions and allow them to trust each other.
- To build networks and friendships. Partnerships lead to social benefits for staff and customers, as people can build networks and friendships by participating in the organization.
- To revive the withering energy of key partners who are trying to do too much on their own. Partnerships can help step up efforts around a problem. For organizations that have worked too long in a vacuum, adding other hands to the task can be a huge source of new energy and hope.
- Planning and launching community-wide initiatives on various issues. In addition to addressing pressing security issues or promoting or providing services, partnerships can serve to pool long-term campaigns.
- To develop and use influence to obtain services or other benefits of the CC. The partnership can be more effectively advocated by different organizations working independently. In addition, a broad partnership can put pressure from all sectors of industry and have a large amount of power.
- To create long-term, permanent change. Real change usually takes place over a period of time through the process of gaining trust, sharing ideas and overcoming existing challenges in order to understand the real problems underlying the needs of industry and security. The partnership, with its structure of cooperation between different organizations and focus on solving security problems, can facilitate and accelerate the process of change, according to the dynamics of the security situation.

- To receive or provide services. A long-term partnership is needed to design, obtain funding within the scope of the CC's specialization.

4. Key partnerships in the QUASAR project

The partnership under the project for the Center of Competence "Quantum Communication, Intelligent Security Systems and Risk Management" (Quasar) comprises the following 8 organisations:

- Institute of Robotics "St. Ap. and Gospeller Matthew" at the BAS (Lead partner);
- Institute of Metal Science, Equipment and Technologies with Center for Hydro- and Aerodynamics "Acad. Angel Balevski" at the BAS;
- "Nikola Vaptsarov" Naval Academy – Varna;
- "Vasil Levski" National Military University – Veliko Tarnovo;
- Technical University of Gabrovo;
- Institute for Nuclear Researches and Nuclear Energy at the BAS
- Faculty of Geology and Geography of the Sofia University "St. Kliment Ohridski";
- Association "Advanced Flight Technologies", Sofia.

The concept for the construction of the Quasar competence center is aimed at creating a network of resources, forming a modern large-scale research infrastructure in the field of information and communication technologies, which will help achieve the goals of Bulgaria and the EU in the field of research and technological development.

The center is a set of facilities, resources and related services needed by the scientific community composed of CC researchers, but also other scientists, companies, organizations, including associate partners from our country and abroad, who will use the built infrastructure for conducting research in the relevant fields.

The research areas in which the QUASAR team specializes and work are information and communication technologies, sensorics and energy conversion, transmission of information through non-traditional channels and creation of models for events, phenomena and processes that pose a risk to the anthropogenic environment. Overcoming the interruption of radio waves and radio communications in major earthquakes, nuclear or nuclear accidents, volcanic eruptions or disasters can be overcome through the quantum communication of intertwined photons in the space-time continuum. Intelligent security systems will be able to predict accidents, disasters and prevent a terrorist threat.

Data collection will be done through micro- and nano-sensor systems based on the multisensor principle, operating in a wide temperature range. Increasing the conversion efficiency will be achieved both by lowering the operating temperature and by new modifications of the conversion elements. In general, QUASAR covers a wide market niche in communication and sensor technologies and systems

Within QUASAR, activities systematized in 4 work packages (WP) are in the process of implementation, namely:

- WP 1. Quantum communication (Leading partner: Institute for Nuclear Research and Nuclear Energy);
- WP 2. Intelligent security systems (Leading partner: Institute of Metal Science, Equipment and Technologies with Center for Hydro- and Aerodynamics "Acad. Angel Balevski";
- WP 3. Risk management (Leading partners: the Varna Naval Academy;
- WP 4. Innovative sensor technologies with multi-purpose application (Leading partner: Institute of Robotics "St. Ap. and Gospeller Matthew".

Structured in this way, the Competence Centre QUASAR has no analogue at national and European level. This is a clear niche, through which the capacity built through a key partnership will become a leading area of multidisciplinary importance. The expertise of scientists and specialists involved in the CC is such that they successfully format the innovative space of the object area of specialization with new ideas, patents for inventions and prototypes of original products and systems.

The leadership role of the team is clear as an asset and as a future potential that combines avant-garde topics: quantum communication, sensory and risk management through intelligent systems. This scope is of multidisciplinary importance and is a generator of new ideas that can be protected by patents for inventions. This is one of the few cases where a fundamental result / fundamental results of theory can lead to specific engineering solutions with a clear commercial effect. The leadership role of the thus formed scientific team is definitely proven as a potential and opportunity.

Significant contribution, as a key partner in the development of security elements and systems, including ESC, has Institute of Metal Science Equipment and Technologies with Hydro- and Aerodynamics Centre "Acad. A. Balevski". Through its innovative developments, known and delivered to national and international partner organizations, the Institute contributes to the implementation of QUASAR activities.**[3-10]**

5. Conclusions

The key partnerships established through the centers of competence create relationships for the integration of the activity for the development of the products and services in the field of the security systems of critical infrastructures and sites of national importance.

Market-oriented and integrated structures, such as the QUASAR Central Committee, offer various forms of promoting structured cooperation between science, education and industry. With its organization of cooperation between different organizations and focus on solving security problems, QUASAR can accelerate the process of research and innovation, depending on the dynamics of the security environment, while helping to reduce risk in a competitive environment, characterized by uncertainty.

ACKNOWLEDGMENTS

This paper is the result of implementation of the scientific work of the IMSETCH-BAS team, participating in Work package 2. "Intelligent security systems", Project BG05M2OP001-1.002-0006 Competence Center "Quantum Communication, Intelligent Security and Risk Management Systems (Quasar)", funded by the European Regional Development Fund through the Operational Programme "Science and education for smart growth" (SESG), co-financed by the European Union through the European Structural and Investment Funds.

References:

[1] Michael Dinges, Michael Ploder, Marita Paasi, Future Competence Centre Programmes Report of the TAFTIE Task Force on Competence Centre Programmes CompAct, May 2016, DOI:10.13140/RG.2.2.24376.96009;

[2] https://link.springer.com/chapter/10.1007/978-1-4842-1455-8_4;

[3] Busch, Nathan E., and Austen D. Givens. "Public-Private Partnerships in Homeland Security: Opportunities and Challenges." *Homeland Security Affairs* 8, Article 18 (October 2012). https://www.hsaj.org/articles/233;

[4] Dimitar D., „Preventive and protective measures against insider threats in nuclear facilities", International Scientific Journal Security & Future, Vol. 5 (2021), Issue 3, International Scientific Journals of Scientific Technical Union of Mechanical Engineering „Industry 4.04, 2021, ISSN:Print ISSN 2535 - 0668, Online ISSN 2535- 082X, pp. 88-91;

[5] Dimitrov D., „Developing the opportunities for building nuclear security", Technics. Technologies. Education. Safety. 2021. , Military sciences and national security., Proceedings 3, 3(13), Scientific Technical Union of Mechanical Engineering "Industry - 4.0", 2021, ISSN:ISSN 2535-0315 (Print), 2535-0323 (Online), pp. 208-211;

[6] Dimitrov D., „Examples of nuclear security measures for nuclear facilities", Technics. Technologies. Education. Safety. 2021, Military sciences and national securityy, Proceedings 3, 3(13), Scientific Technical Union of Mechanical Engineering "Industry - 4.0", 2021, ISSN:ISSN 2535-0315 (Print), 2535-0323 (Online), pp. 212-215;

[7] Dimitrov D., „Basic regulations and associated administrative measures providing nuclear security", Proceedings of the Annual University Scientific Conference, 5, Publishing House of Vasil Levski National University, 2021, ISSN:ISSN 2367-7481, pp. 73-80;

[8] Georgiev N., Boychev Y., Kosev V., "Investigation of seismic fluctuations caused by a type of heavy chain equipment", Sb. reports of the XVIII International Scientific Congress "Machines. Technologies. Materials ", 1, NTS in Mechanical Engineering, 2021, ISSN: 2535-0315, pp. 23-26;

[9] Boychev, Y., Assenov S., "Sensors and systems for detection of improvised explosive devices", Proceedings of the Annual University Scientific Conference. 5, V. Levski National University, 2021, ISSN: 2367-7481, pp. 53-63;

[10] Tumbarska A., "Trends in the development of non-lethal technologies and protection systems" IMSETHC-BAS, 2020, ISBN: 978-619-7466-07-2, pages 402.