OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

Czech-German-Cross-Border Situational Awareness for Critical Infrastructures

Project manager: Prof. Dr. Markus Bresinsky (OTH)
Project assistant: Johanna Schröder (B.A.) (OTH)

Project partner: doc. Dr. Ing. Jan Voráček, CSc. (College of Polytechnics Jihlava)

University of Applied Sciences Regensburg (OTH)

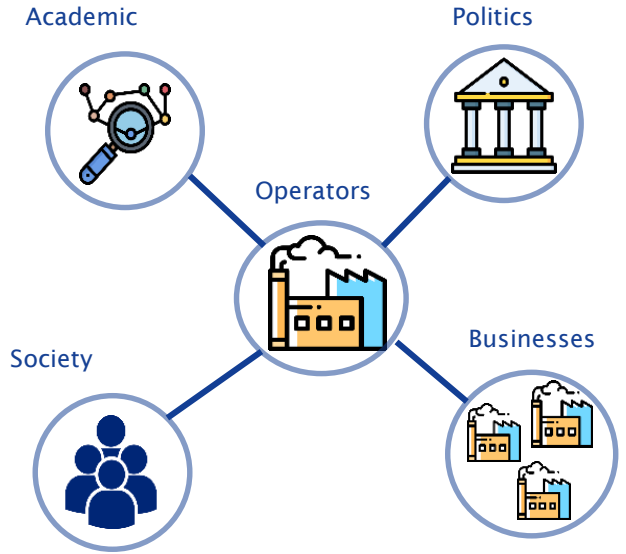
- Approximately **11.500** students, **225** professors and **530** employees
- active network of around **150** partners in industry
- **200** partnerships with universities

Project details

Title	Czech-German-Cross-Border Situational Awareness for Critical Infrastructures
Project manager	Prof. Markus Bresinsky
Project assistant	Johanna Schröder (B.A.)
Project partner	doc. Dr. Ing. CSc. Jan Voráček (College of Polytechnics Jihlava)
Topics	Critical Infrastructures, Cross-border situational awareness, Cybersecurity
Region	Easzern Bavaria, Czech Border region
Duration	1st of October 2019 to 31st of December 2012
Funding body	Bayerisch-Tschechische Hochschulagentur (BTHA) (Bavarian-Czech agency of higher education)

Focus

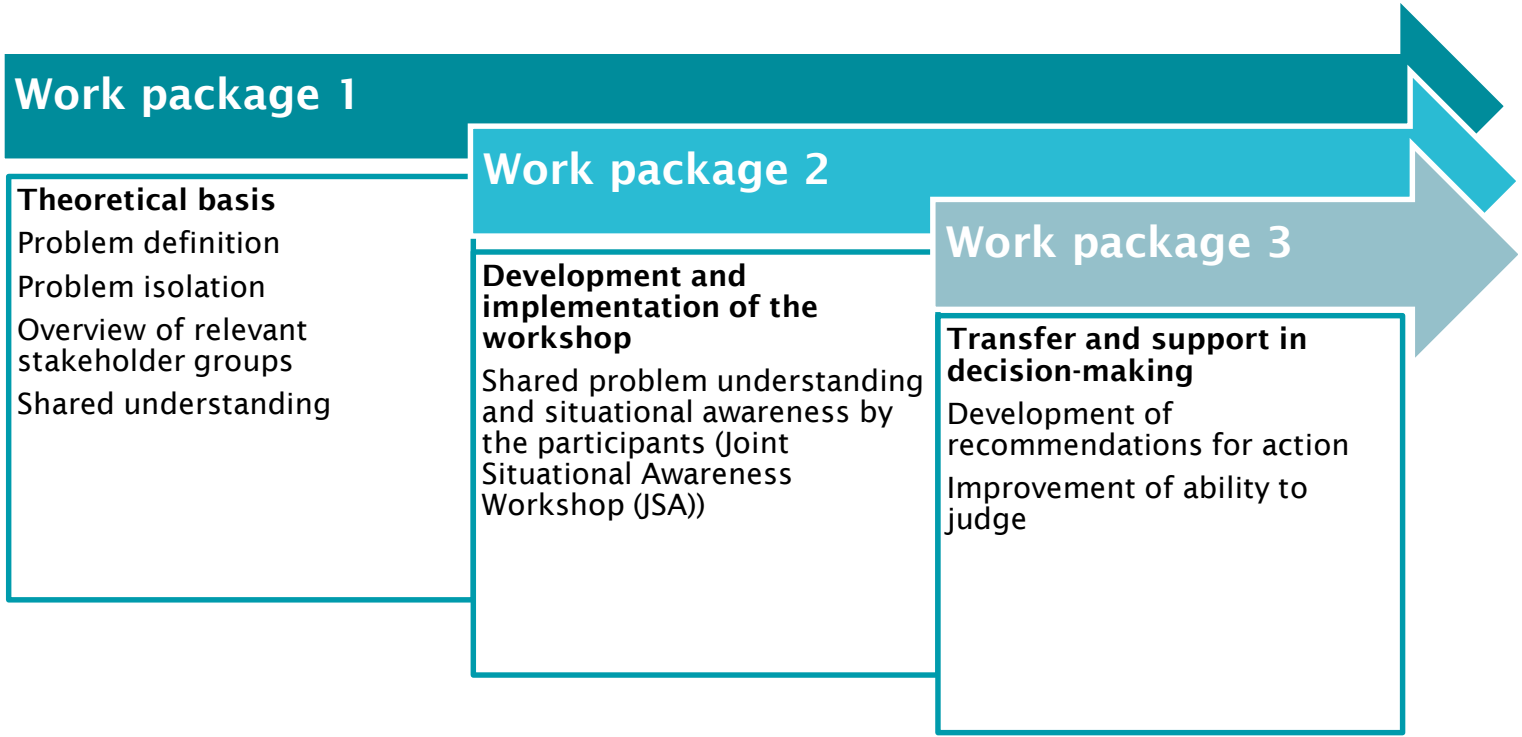
- Critical infrastructures, cyber security
- Dependencies, especially peripheral areas
- Creation of a shared problem understanding and situational awareness
- Preparedness, resilience



Characteristics:

- System-of-Systems Approach
- Cross-border (Eastern Bavaria Czech Republic)

Work packages



Project timeline

	2019	2020				2021			
	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
WP 1 (Problem definition, collection of stakeholders)									
WP 2 (Development and implementation of the workshop)						JSA			
WP 3 (Transfer and support in decision-making)									
Project report BTHA									
Project meetings	1 (CZ)		2 (GER)		3 (CZ)		4 (GER)		5 (CZ)
Publications									

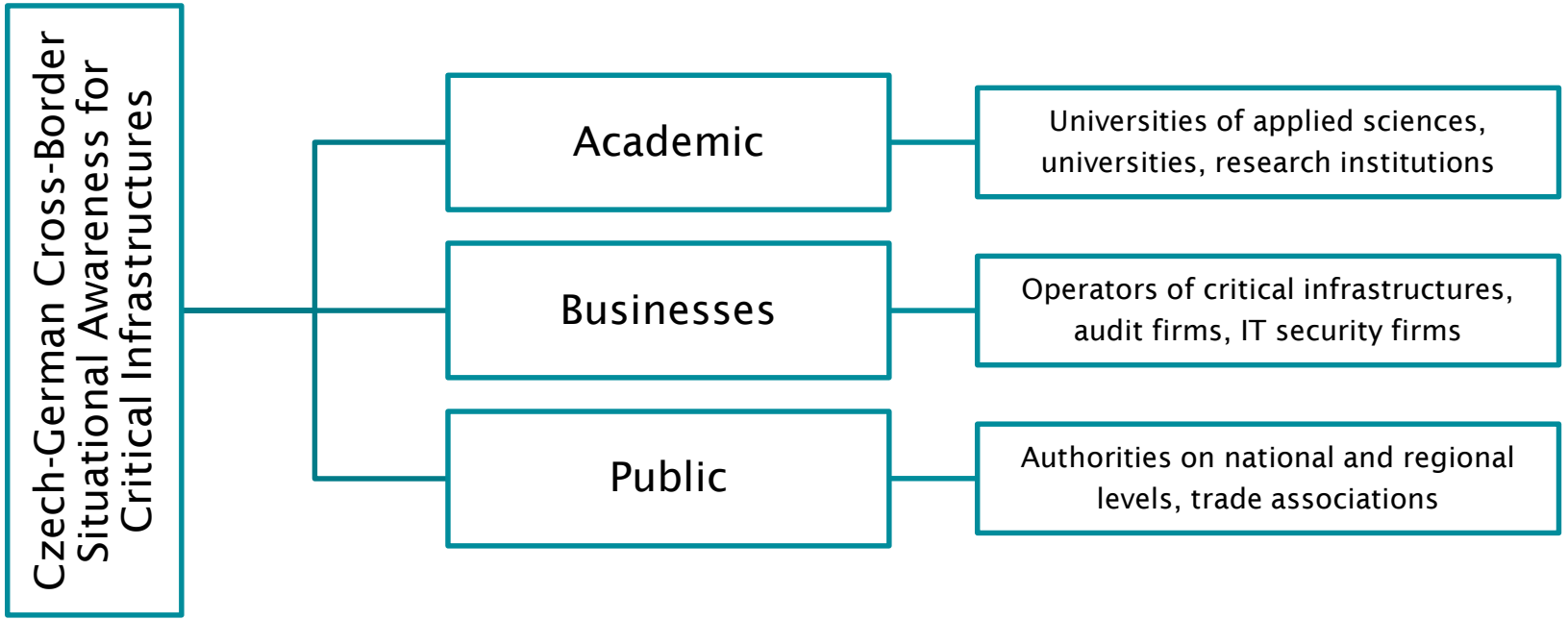
December 2019

Work hypothesis

Critical Infrastructures are more and more connected to information systems which increases their vulnerability towards cyber attacks. In order to achieve a high level of protection of Critical Infrastructures, not only single systems should be analyzed but also the bigger system in which they act. This means that the effects a disruption or a failure might have on other bodies need to be considered when developing measures to protect those infrastructures. This approach is called **Systems-of-systems Approach (SoS-Approach).**

In order to implement this approach, therefore, operators of critical infrastructures have to be connected with actors affected by a disruption or failure and those who have knowledge to develop approaches to increase protection of Critical Infrastructures. Thus, solutions can be jointly developed.

Stakeholder fields



Potential stakeholders Czech Republic

Academic field

University	Department	Field/Position
University of West Bohemia	Technology Transfer Office Pilsen	Chairman of the Technology Transfer Office
Charles University Prag	Institute of Political Studies, Department of Security Studies	Professor for Security Studies
Masarysk University Brno	Faculty of Social Studies	International Institute of Political Science
Brno University of Technology (BUT)	Business and Management – Institute of Informatics	Cyber criminology, cyber kinetics

Potential stakeholders Germany

Trade associations

Institution	Position	Field
Europa Region Bayerischer Wald - Böhmer Wald	Networking manager Bavaria	Connecting businesses and universities
Europaregion Donau-Moldau	Contact person for univeristy cooperation in the Danube and Moldova regoin	Connecting universities

Potential stakeholders Czech Republic

Trade associations

Institution	Position	Field
German/Czech chamber of commerce in Prague	Chairman of the Competence Center for future technologies	Connecting, network of Czech companies
Industrial chamber of commerce in Pilsen	Working at the chamber of commerce	Connecting with companies in the field of cybersecurity and critical infrastructures

Next steps

- Common problem definition and linguistic framework
- Overview of relevant stakeholder groups