JYU. Since 1863.

Huoltovarmuuskeskus
Försörjningsberedskapscentralen
National Emergency Supply Agency

FACULTY OF INFORMATION TECHNOLOGY
www.jyu.fi/en/it

Hanna Paananen, University of Jyväskylä

Collaboration Practices in Inter-Organizational Cybersecurity Management

ABSTRACT

Cyberattacks against critical infrastructure can cause widespread shocks in society. Lately, these attacks have started to utilize the supply chain as a way to gain access. Legislation and standards are mandating actions to counter these risks. This challenges organizations to create ways to manage cybersecurity across organizational boundaries.

Managing cybersecurity in collaboration with partners may be uncharted territory in many organizations, and enabling structures have not been created. This research aims to identify the needed practices and how they could be fostered to generate mutually beneficial cybersecurity collaboration within a partner network.

KEEP YOUR FRIENDS CLOSE to avoid your enemies getting closer. When organizations produce goods and services in close collaboration, it can provide a strategic advantage while exposing them to new risks. Supply chain attacks may target weak spots in the shared processes, and access may be gained by utilizing a mix of different attack types. Preparing and responding to these attacks efficiently requires developing competencies for cybersecurity cooperation.

CONTROL OVER PARTNERS

Supplier relationships or strategic partnerships are formed to create value through a chain or network of companies. Cybersecurity has become topical in cooperation due to the increasing **digitalization of industries.** The most prominent form of control is contracts between buyers and suppliers. A supplement to the contract often covers cybersecurity requirements. Other forms of control include audits and testing, standards and governance models, technical controls, and training [1]. However, simplified views of the power relationships between partners and dismissal of the dynamic nature of cybersecurity can make these measures **ineffective**.

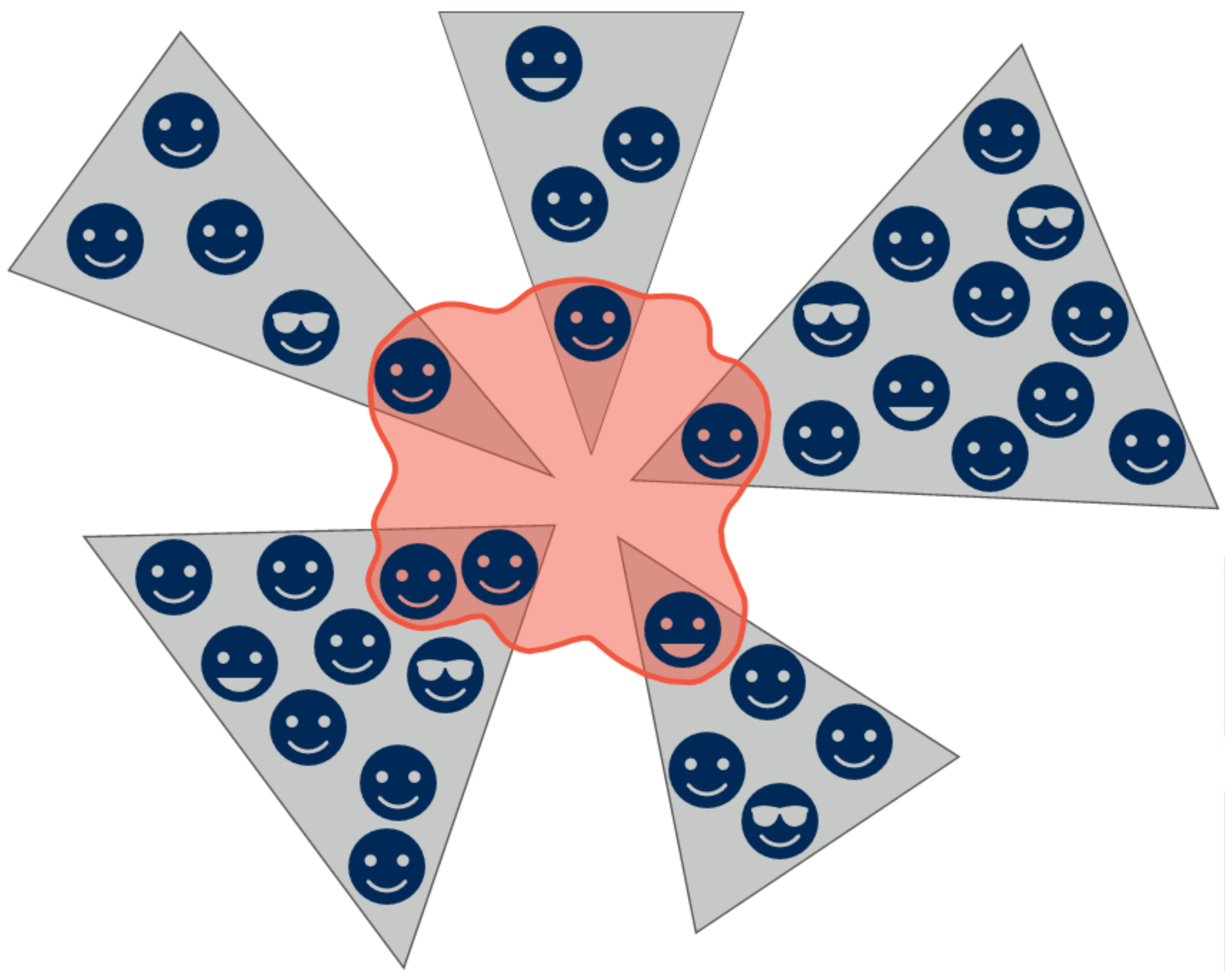
FROM CONTRACTS TO PRACTICES

Contracts and process diagrams are only higher-level abstractions of the actual work that must be carried out to manage cybersecurity across a partner network.

→ **The practices** of cybersecurity management entail explicit and tacit structure and meaning, which the people have formed for this work.

→ **Communities** form around the work and support people's abilities to repeat practices and learn from others.

→ **Boundary objects** help in describing and learning practices of communities other than our own. [2]



INTER-ORGANIZATIONAL COMMUNITY

Good cybersecurity posture may protect the value-creation across the partner network. Effective cybersecurity management does not need to be **constrained by the hierarchical or commercial** aspects of the partnership. However, these issues may hinder forming practices for inter-organizational work if conflicts between communities cannot be actively solved. People may experience the **burden of balancing** the needs of the organization and collaboration.

OBJECT FEATURE	AIM
Address competence building	Fix asymmetry of competencies Learning from others
Mandate for repeated practices	Connecting contracts and practice Ease adaptation to changes
Materia for practices	Makes conflicts explicit Helps translate meanings
Reificate goals	Reduce barriers Common line of defense

CYBERSECURITY COMMUNITIES FOR CRITICAL INFRASTRUCTURE

Developing and Managing Cybersecurity in a Partnership Network project aims to foster the creation of working communities for cybersecurity management in critical infrastructure partner networks. There is a need to complement the formal structures of partnerships with support for creating inter-organizational practices. This is achieved by building boundary objects that reduce conflicts and help in building a community.

The project includes three partnership networks in different sectors of critical infrastructure. Each network has workshops where the needs for collaboration are discussed and **principles** (objects) are outlined to foster the development of mutually beneficial practices. The project will continue until the end of 2024.

Strategic partnerships and complex processes

Community support for small organizations

Multiple actors in facilities and systems

CONCLUSIONS

- → **Inter-organizational practices must be supported and developed along with internal practices.**
- → **There must be constant negotiation of the relationship between the higher-level principles and the related practices.**
- → **Shared objects can help in this negotiation and reification of the collaboration practices.**

[1] J. Järveläinen, Information security and business continuity management in interorganizational IT relationships. Information management and computer security 20(5). 2012

[2] E. Wenger, Communities of Practice: Learning, meaning, and identity. Cambridge: Cambridge University Press, 1998.