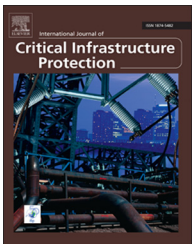
Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



Trust building and the European Reference Network for Critical Infrastructure Protection community

*David Ward**, *Naouma Kourti*, *Alessandro Lazari*, *Piotr Cofta*

Institute for the Protection and Security of the Citizen, Joint Research Centre, via E. Fermi 2749, 21027 Ispra, Italy

ARTICLE INFO

Article history:
Received 20 November 2012
Accepted 7 July 2014
Available online 17 July 2014

Keywords:
Trust
Confidence
Governance
Information sharing
Trust framework
ERNCIP

ABSTRACT

This paper discusses trust building within the European Reference Network for Critical Infrastructure Protection (ERNCIP) Project, in which a network of experts are building and promoting the first community focused specifically on European critical infrastructure protection research and practice. To this end, the paper examines the concept of trust and its many dimensions, how trust can be monitored, and how trust relates to networks of people and the technologies and mechanisms that they use to cooperate.

The paper begins by providing an overview of ERNCIP and discusses trust, confidence and trust development as community building concepts. Following this, experiences related to nurturing, seeding and promoting trust while developing the ERNCIP community using a participatory and voluntary approach are detailed. The paper closes with a review of trust by design, commitment and governance and a look at the future of ERNCIP.

1. Introduction

More and more communities are emerging to address the myriad, complex and interconnected issues in the important domains of critical infrastructure protection, resilience and crisis management. The intent of these communities is to share knowledge, develop best practices, drive a common understanding, build awareness and improve decision making within the community of experts. Often these communities take the form of public-private partnerships (PPPs) [20] and represent networks of specialists or experts (i.e., communities). Such networks rely on a trusted environment of cooperation and the success of a new community like the European Reference Network for Critical Infrastructure Protection (ERNCIP) [26] depends on how behavioral trust and community are fostered and managed. Indeed these communities depend on adequate governance, approved and binding agreements, and the application of clear rules in a trustworthy environment.

While virtual and real communities are fundamentally different, they have commonalities in their evolution, administration and functionality. They flourish or fade depending on the trust and confidence their members have towards and within the community: the ERNCIP community is no exception to this rule and is the subject of this paper. The intent of this paper is to provide a real (on-going) case study concerning the creation and operation of a trusted network or community, the primary reason being that there is very little, if any, published information on how to create and operate a trusted network, especially in the field of critical infrastructure protection.

This paper begins by providing an overview of the ERNCIP Project and proceeds to clarify the concept of trust and its relation to the ERNCIP Project. The building and management of trust and confidence are discussed in relation to

*Corresponding author.
E-mail address: david.ward@jrc.ec.europa.eu (D. Ward).

http://dx.doi.org/10.1016/j.ijcip.2014.07.003
1874-5482/

communities before moving to the areas of trust and trusted agents in ERNCIP. The development of trust is then tackled, and the paper shows how it has been seeded, grown and promoted so far in the ERNCIP community. The paper closes with a discussion on trust by design, commitment and governance as leveraged by ERNCIP and the future organization of ERNCIP as a vibrant community.

2. Overview of ERNCIP

Critical infrastructures are vital societal assets such as power plants, transportation systems, hospitals and communications networks that enable society to conduct day-to-day activities in all walks of life. Europe has an extensive and highly interconnected network of critical infrastructures whose disruption or, worse destruction, could have a significant impact on society [24]. Since critical infrastructures are interconnected, a failure in one critical infrastructure can induce risks to other critical infrastructures and lead to failures across national borders [13]. Securing critical infrastructures is crucial to protect them against the many threats and hazards they face and, thereby, make society more resilient. The disruption and failure scenarios include human-induced threats such as terrorism, technological threats such as chemical plant explosions and natural threats such as floods, earthquakes and forest fires.

Needless to say, reducing the risk and vulnerabilities of critical infrastructures requires that all critical infrastructure stakeholders cooperate in a trusted manner and in a cooperative environment. Cooperation requires good faith with regard to the disclosure of information. The main benefit of such cooperation is a higher level of awareness gained by the stakeholders. Awareness is one of the key elements for building and maintaining strong and resilient infrastructures. Indeed, awareness increases the overall perception of the risks related to critical infrastructure protection, helping critical infrastructure operators and other stakeholders to prioritize the risks while enacting smoother and cost-effective policies and crisis management procedures. Hence, the general public, public authorities (e.g., law enforcement, emergency services and government) and critical infrastructure operators need to demonstrate confidence and trust in each other and ensure that their interests are aligned [27]. Increased awareness also raises the overall perception of the risks related to critical infrastructure protection, helping critical infrastructure operators and stakeholders to prioritize risks.

The provision of security-related solutions to reduce critical infrastructure vulnerabilities, including equipment, systems, services and applications, implies that manufacturers and suppliers must be aware of the risk and deliver appropriate solutions. Security solutions and relevant themes are very diverse, but manufacturers and suppliers still focus on traditional and mainly national market segments, and offer fairly standardized and domestically-certified security technologies and solutions.

Meanwhile, there is a growing need for internationally-recognized and certified security solutions. A recent example is the introduction of body scanners in airports and the accompanying concerns about health, safety and privacy [32]. The standardization and harmonization of test protocols and certification are, therefore, becoming a key competitive feature and an international security capability requirement [16]. This brings trust back into focus because internationally-accepted standards are contingent on trust in certification processes.

The lack of European Union (EU) wide conformity assessment of security-related equipment and systems, services and applications, including certified common testing and measurement methods and standards, is another barrier to developing security-related products. This hampers transition to market and hinders market acceptance. The EU member states (MSs) and the European Commission believe that this can be improved by the increased availability and networking of EU experimental facilities and laboratories, including experts and expertise. The ERNCIP Project was formulated to provide a trusted platform to satisfy this rationale [26]. Pursuant to this vision is the mission statement of ERNCIP (approved by its sponsors, which include the European Commission and EU member states): *To foster the emergence of innovative, qualified, efficient and competitive security solutions, through the networking of European experimental capabilities.*

ERNCIP seeks to provide a framework within which experimental facilities and laboratories can share knowledge and expertise in order to identify security products and solutions, harmonize test protocols and measurements, explore the possibility of EU-wide certification and make recommendations for research and investment. The scope is to improve the protection of EU critical infrastructures against all threats.

To this end, in 2009, the EU member states endorsed the Joint Research Centre (JRC) in Ispra, Italy to investigate the concept of ERNCIP and provide advice on setting up such a network. This advice culminated in a green light issued in November 2010 to progress to the implementation phase [26].

During the four year implementation phase, which started in 2011, the two key "tools" that have been used to build the ERNCIP network are the development and deployment of a web-based inventory of experimental facilities, and the setting-up and operation of thematic groups to tackle the issues (themes) related to critical infrastructure protection that were voiced by the project sponsors and stakeholders.

Each thematic group tackles a specific critical infrastructure theme or thematic area (e.g., explosives detection and water security) and comprises selected critical infrastructure protection experts and specialists who know each other and/or their organizations. Their work involves the exchange of data, information and knowledge, some of which may be sensitive and with limited distribution. The governance of thematic groups includes organizing venues such as group meetings and workshops, stipulating membership agreements, tackling intellectual property rights issues, and preparing terms of reference (ToRs) and reports. The ERNCIP inventory was launched in June 2012 and the first thematic groups were set up starting in February 2012. The inventory and thematic groups are both supervised by the ERNCIP Office. Table 1 summarizes the preparatory and implementation phases, which are discussed in more detail later in the paper.

This paper discusses the learnings and findings to date related to the creation and development of the ERNCIP