A view of trust and information system security under the perspective of critical infrastructure protection

Bako Rajaonah

▶ **To cite this version:**

Bako Rajaonah. A view of trust and information system security under the perspective of critical infrastructure protection. Revue des Sciences et Technologies de l'Information - Série ISI : Ingénierie des Systèmes d'Information, 2017, 22 (1), pp.109. 10.3166/isi.22.1.109-133 . hal-01540678

HAL Id: hal-01540678
https://hal.science/hal-01540678

Submitted on 26 Jun 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A view of trust and information system security under the perspective of critical infrastructure protection

Rajaonah Bako

LAMIH UMR CNRS 8201 – Institut Carnot ARTS
Université de Valenciennes et du Hainaut Cambrésis
Campus Le Mont Houy, F-59313 Valenciennes, France
bako.rajaonah@univ-valenciennes.fr

RÉSUMÉ. Bien que la confiance soit reconnue comme importante dans les environnements numériques, peu d'études sur les systèmes d'information traitent à la fois de leur sûreté et de la confiance. Celles qui existent tendent à rester dans le périmètre étroit des interactions entre deux agents. Nous proposons de repenser la recherche sur la confiance liée à la sûreté des systèmes d'information à travers l'approche holistique de la protection des infrastructures critiques (IC). Après une introduction de la problématique, nous présentons les définitions nécessaires à une compréhension commune des concepts d'infrastructure critique et de confiance. Des travaux sur la sûreté des systèmes d'information menés dans le cadre de la protection des IC sont ensuite brièvement décrits. Enfin, nous exposons notre vision transdisciplinaire de la recherche sur la confiance dans les systèmes d'information vue sous l'angle de la protection des IC.

ABSTRACT. Although trust is recognized as important in security issues of computer networking environments, few studies on information systems deal with both trust and security, and those existing tend to remain within the short perimeter of two-agent interactions. We propose to rethink trust research on information system security by considering the holistic approach of critical infrastructure protection (CIP). After introducing the problem, we give the definitions that are necessary for a common understanding of the concepts of critical infrastructures and trust. Some works on critical infrastructure protection involving information systems are then described briefly. Finally, we present our transdisciplinary view of trust research on information system security under the perspective of CIP.

MOTS-CLÉS : confiance, protection des infrastructures critiques, sûreté, système d'information, transdisciplinarité

KEYWORDS: critical infrastructure protection, information system, security, transdisciplinarity, trust

1. Introduction

Trust is recognized as central to understand modern societies (e.g., Lewis and Weigert, 2012; Misztal, 1996, 2013) and is particularly important in security issues of computer networking environments (e.g., Lamsal, 2001). However, very little studies on information systems deal with both trust and security. Among existing works in the literature, one trend is acceptance studies involving end-users of IS-based services (e.g., Mangin *et al*., 2014) or of social networks (e.g., Fogel and Nehmad, 2009; Shin, 2010). Other works are centred on end-users trustworthiness (e.g., Aberer and Despotovic, 2001; Swamynathan *et al*., 2005). Finally, another trend focuses on the design of trustworthy information systems (e.g., Offor, 2013; Ruotsalainen *et al*., 2014; Truong *et al*., 2016).

Therefore, it seems that trust research related to information system security tends to remain within a short perimeter which is mostly that of trust-based two-agent interactions (humans – systems, systems – humans, humans – humans) mediating by a specific information system. This paper proposes to open the debate on rethinking trust research on information system security. In today's information-based world, it might be that the holistic approach of critical infrastructure protection would be more enriching rather than considering trust-related issues of information system security from only a per se perspective.

Indeed, firstly, information systems and the Internet are nowadays at the very core of most businesses and services in companies, organizations and institutions. Secondly, information and knowledge that are stored and/or exchanged in those information systems are of a great value, which attracts both well- and ill-intentioned people, especially cyber-attackers among the latter. Finally, the consequences of attacks on information systems might affect vital services. This third point is a strong argument in favor of studying information system security under the perspective of critical infrastructure protection (CIP). Indeed, the very definition of critical infrastructures involves vital services, i.e., that disruption or destruction of those infrastructures due to natural disasters, extreme weather conditions, industrial accidents, deliberate attacks, human errors, etc. would have a significant impact on vital societal functions, health, safety, security, economic or social well-being, which makes their protection of government concern. See, for example, the *Green Paper on a European Programme for Critical Infrastructure Protection*[1] (EC, 2005); the *European Programme for Critical Infrastructure Protection EPCIP*[2] (EC, 2006); and the European *New approach to EPCIP*[3] (EC, 2013).

Critical Information Infrastructure Protection (CIIP), that is a part of CIP, refers to the protection of critical infrastructures related to information and

1. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576&from=EN
2. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF.
3. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/docs/swd_2013_318_on_epcip_en.pdf.

telecommunication technologies (ICT) (see EC, 2005). The sector of ICT includes the Internet, information systems, industrial control systems such as Supervisory Control Data Acquisition (SCADA) systems and Distributed Control Systems (DCS), fixed and mobile communications, satellite communication, radio communication and navigation, and broadcasting (Luiijf and Klaver, 2015; Zio, 2016). This sector is particularly sensitive because nearly all critical infrastructures have components that rely on ICT (e.g., Hämmerli, 2005). Cybersecurity –defined as the process of protecting information by preventing, detecting, and responding to attacks[4]– is therefore particularly important in CIIP. For instance, Article 22 of the 2013 *French Military Programming Law*[5] is specifically dedicated to the security of vital information systems; see also the 2016 *Stocktaking, analysis and recommendations on the protection of CIIs* of the European Union Agency for Network and Information Security (ENISA, 2016)[6] and the 2014 *Framework for improving critical infrastructure cybersecurity* of the US National Institute of Standards and Technology[4] (NIST, 2014).

In fact, research on cybersecurity undertaken from the perspective of critical infrastructure protection is growing across the world (Gonzalez *et al*., 2006; Grimsman *et al*., 2016; Karabacak *et al*., 2015; Ten *et al*., 2010; Thakur *et al*.; 2016, Zhou *et al*., 2011; etc.). Nevertheless, little of that research has focused on trust-related issues despite the multidisciplinarity characteristic of trust, which is a concept used in both soft and hard sciences, and the multifaceted nature of critical infrastructures, which include machines, technologies, humans, organizations, and institutions. Moreover, as emphasized by Dunn (2005), not much work has focused on the social and political dimensions of CIP/CIIP although they are of central importance. Concretely, debating the question of trust and information system security under the perspective of the protection of critical infrastructures would be highly relevant to find global solutions; but it would be even better to include all human and social sciences.

The paper is organized as follows. In order to facilitate common understanding of critical infrastructure protection and trust, these topics are tackled from definitions in Chapter 2 and Chapter 3. Chapter 4 describes briefly some works on CIP/CIIP involving information systems in order to show the trend of research. Finally, in Chapter 5, we present our human and social scientist's view of CIP-based research on trust-related issues of information system security.

2. Critical infrastructures

An **infrastructure** can be defined as a "framework of interdependent networks and systems comprising identifiable industries, institutions (including people and

4. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.
5. https://www.legifrance.gouv.fr/eli/loi/2013/12/18/DEFX1317084L/jo/texte
6. https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis/at_download/fullReport

procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defence and economic security […], the smooth functioning of government at all levels, and society as a whole" (Moteff and Parfomak, 2004, CRS-3). This definition that explicitly includes people as part of infrastructures is very important for our purpose on trust. It echoes the definition of Bouwmans *et al.* (2006) who consider infrastructures as socio-technical networks combining physical networks (man-made systems and processes) and actor networks (people, institutions, and companies). Infrastructures can be viewed as complex adaptive systems (e.g., Rinaldi *et al.*, 2001) or as systems-of-systems (e.g., Eusgeld *et al.*, 2011). The common assumption behind those points of view (those of Bouwmans *et al.*, Eusgeld et *al.*, Rinaldi et *al.*, and others) is that an infrastructure is a whole that exhibits emergent properties and behaviors which do not result from the sum of its components' properties and behaviors. That point is important for research conducted under the perspective of critical infrastructure protection: enhancing the security and/or safety of one element of the infrastructure does not necessarily ensure the security and/or safety of the whole infrastructure. The difference between safety (*sécurité*) and security (*sûreté*) which is adopted in this paper is that the former refers to accidental harms and the latter to malicious ones (e.g., Firesmith, 2003).

As for **critical infrastructure**, the definition adopted by the European Council is that an EU critical infrastructure is "an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State"[1] (EC, 2008). Another definition specifies that European critical infrastructures are those "which are of the highest importance for the Community and which if disrupted or destroyed would affect two or more Member States, or a single Member State if the critical infrastructure is located in another Member State"[2] (EC, 2006). Although definitions of both infrastructure and critical infrastructure have evolved over time, even depending on nation states (e.g., Dunn, 2005; Galland, 2010; Moteff and Parfomak, 2004), there is a consensus on the fact that critical infrastructure protection is essential to the survival of populations and environments.

Critical infrastructure protection (CIP) aims at increasing CI resilience and ensuring that vital services continue to function (EC, 2013). Resilience can be defined as the ability of those infrastructure "to anticipate, cope with/absorb, resist and recover from the impact of a hazard (technical) or disaster (social)" (Kröger and Zio, 2011, p. 4; see also Geoffroy *et al.*, 2017; Haimes, 2009). Concretely, the protection of critical infrastructures consists in preparing for, protecting against, mitigating, responding to, and recovering for critical infrastructure disruptions or destruction (EC, 2005), which requires to understand the physical, functional, and organizational aspects of CI (Zolesio, 2010). These tasks are arduous because of the diversity of critical infrastructure sectors, the nature of their environment and of their interdependencies. An indicative list of **critical infrastructures sectors** is provided in EC (2005): *Energy; Information, Communication Technologies (ICT); Water; Food; Health; Financial; Public & legal order and safety; Civil*

administration; Transport; Chemical and nuclear industry; and Space and research. As mentioned earlier, the ICT sector is protected within the c**ritical information infrastructure protection (CIIP)**.

As expressed in Rinaldi *et al*. (2001), infrastructures are interdependent with their environment; these authors defined the **infrastructure environment** as the framework in which goals and objectives as well as value systems are set, operations are modeled and analyzed, and decisions taken. Kröger and Zio (2011) considered the following aspects that could characterize critical infrastructure environment: economic, business, public policy, legal/regulatory/strategic, technical, security, health, safety, social, political, and/or speed of development/change.

Critical infrastructures do not exist in isolation of one another, they are crucially characterized by their interdependencies (e.g., Bouchon, 2006; Rinaldi *et al*., 2001). Rinaldi *et al*. defined **dependency** as a unidirectional relationship between two infrastructures when the state of one of them influences or is correlated to the state of the other; it is the case between the electric power and telecommunication infrastructures, the former being supported by the latter for, among others, the SCADA systems. Rinaldi *et al*. defined **interdependency** as a bidirectional relationship, each one depending on the other, and **interdependencies** as multiple connections among infrastructures (Figure 1).

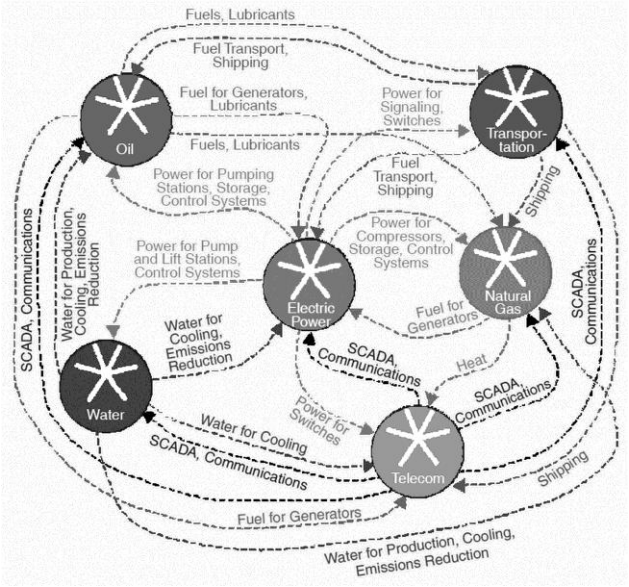

Figure 1. Rinaldi et al.'s examples of infrastructure interdependencies (Rinaldi et al., 2001, p. 15)

The complexity of interdependencies networks illustrated in Figure 1 as well as the diversity of critical infrastructure sectors described in EC (2005) show how a

failure in one infrastructure could easily affect other infrastructures and worsen the extent and nature of damage and potential consequences on health, safety, security, economic and/or social well-being. Protection of critical infrastructures requires for that matter to understand and predict cascading failures as well as their cascading impacts (e.g., Chopra and Khanna, 2015; Stergiopoulos *et al*., 2016)

Moreover, the type of interdependencies, which is another dimension that characterizes critical infrastructures, must also be considered in risk assessment in interdependent infrastructures (e.g., Haimes *et al*., 2008). Interdependencies are categorized into four classes (see Kröger and Zio, 2011; Rinaldi *et al*., 2001): **physical interdependency** when linkages rely on each other's materiel outputs (e.g., a pipeline network providing gas to fuel a gas-fired power station while the electricity generated is used to power compressors and controls the gas supply network, Kröger and Zio); **cyber (or informational) interdependency** when linkages rely on each/other's informational outputs (e.g., a telecommunications infrastructure supporting SCADA or other control systems for energy or water delivery systems, CREDC, 2016); **geographic (or spatial) interdependency** when linkages are spatial proximity (e.g., a natural gas pipeline located in the right-of-way corridor of a high-kVA transmission line, CREDC, op. cite); and **logical interdependency** when linkages are neither physical nor informational nor spatial (e.g., the California electricity crisis due to interdependencies between electric power supply and financial infrastructures, Rinaldi *et al*.).

Critical infrastructure protection requires to identify and classify threats, capabilities, risks, and vulnerabilities; it includes the definition of risk events in terms of their probability of occurrence, impact, and relationship to other risk areas or processes (EC, 2005). **Risk** describes (future) negative, undesirable consequences and the associated uncertainty (Zio, 2016). According to Aven (2011), risk associated with an event can be formulated as uncertainty about and severity of the consequences of the event, uncertainty referring to the lack of knowledge of whether the event will occur or not and how severe would be the consequences. Although risk analysis is at the heart of critical infrastructure protection, it is out of the scope of the present paper. Readers who are interested in risk analysis in complex systems such as critical infrastructures can consult, for example, Aven (2011); Bach *et al*. (2013); Haimes *et al*. (2008); Santos *et al*. (2014); Zio (2009). The concept of risk is tightly related to vulnerability, but they should not be confused. **Vulnerability** is defined by the Society for Risk Analysis (SRA)[7] as both a qualitative property and a quantitative metric. With regard to critical infrastructures, the definition of vulnerability that is often adopted refers to a property of infrastructures or of their systems: vulnerability can be seen as a degree of losses and damages due to the impact of hazards, a degree of exposure to hazards, or a degree of resilience (Kröger and Zio, 2011).

To recap, critical infrastructures are socio-technical networks whose disruption or destruction of their physical or cyber-physical components due to natural disasters, extreme weather conditions, industrial accidents, deliberate attacks, human

7. www.sra.org

errors, etc. would have serious impact on health, safety, security, economic or social well-being. Their protection is therefore a matter of political concern. For instance, the European Commission has published several Communications dealing with critical infrastructure protection (e.g., EC, 2005; EC, 2013). The protection of the sector of information and communication technologies (ICT), being particularly sensitive because of the dependencies of other sectors on ICT, has led to the emergence of working groups across the world on critical information infrastructure protection (e.g., CSS, 2008; ENISA, 2016; NISC, 2007; NIST, 2014; OECD, 2015), especially regarding political strategies to strengthen the security and resilience of critical information infrastructures. As for France, the *Agence Nationale de Sécurité des Systèmes d'Information* (ANSSI)[8] is dedicated to the security and defense of information systems "and contributes to that of critical operators".

Before describing briefly some works on information system security carried out within the framework on critical infrastructure protection, the next chapter gives basic definitions of concepts related to trust.

3. Concepts and definitions around trust

In human and social sciences, the psychological **functionality of trust** would be to reduce perceived uncertainty and, therefore, perceived risk in complex decision-making situations (e.g., Luhmann, 2000; Numan, 1998). The mechanism that underlies trust would be a mental reduction of the field of possibles so that a decision can be taken without considering the outcome of each possible alternative (Lewis and Weigert, 1985; Thuderoz, 2003). That point of view on trust functionality is particularly appropriate for critical infrastructures in which uncertainty is present at any layer because of, among others, the impossibility to have holistic knowledge of them. Indeed, emergent properties and behaviors in such systems of systems could not be inferred from the knowledge of single systems, nor even of single components of each system (see, for instance, Luzeaux, 2010).

Besides the concept of **interpersonal trust** between two or more people including **organizational trust** (e.g., Deutsch; 1958; Kramer, 1999; Schoorman *et al*., 2007), researchers also consider **systemic trust**, i.e., toward impersonal structures such as institutions (e.g., Luhmann, 2000) and **trust in technologies** (e.g., Lee and See, 2004; McKnight *et al*., 2011). But what is trust? Based on the taxonomy of Barber (1983), Muir (1987, 1994) defined trust as being composed of expectations: expectation of persistence of the natural and moral social orders, expectation of competence, and expectation of responsibility. According to that and also according to the above-mentioned functionality, trust is operationally defined in this paper as a state of **expectations** resulting from a mental reduction of the field of possibles. This definition is not mutually exclusive with the idea of willingness to be vulnerable which constitutes the definitions adopted by most researchers (see the reviews of definitions in McKnight and Chervany, 2001; Schoorman *et al*., 2007). The definition is, besides, consistent with the concept of distrust as confident

8. http://www.ssi.gouv.fr/en/mission/audiences-and-activities/

negative expectations and trust as confident positive expectations (Lewicki *et al.*, 1998).

As shown in Figure 2, trust can be considered in the form of a three-part relationship in which the **trustor** expects the **trusted** or **trustee** (i.e., the **object of trust**) to behave in a certain manner (e.g., Hardin, 2002).

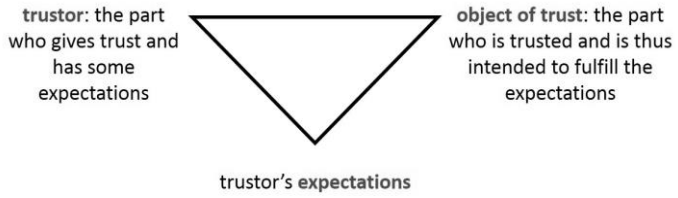

Figure 2. Basic concept of trust as a three-part relationship between trustors, trustees, and expectations.

This three-part pattern, initially considered for interpersonal relationship, is in fact implicitly underpinning the studies on trust related to other objects than people. For example, Figure 3 shows possible trustors, trustees and trustors' expectations around the information system of an organization.

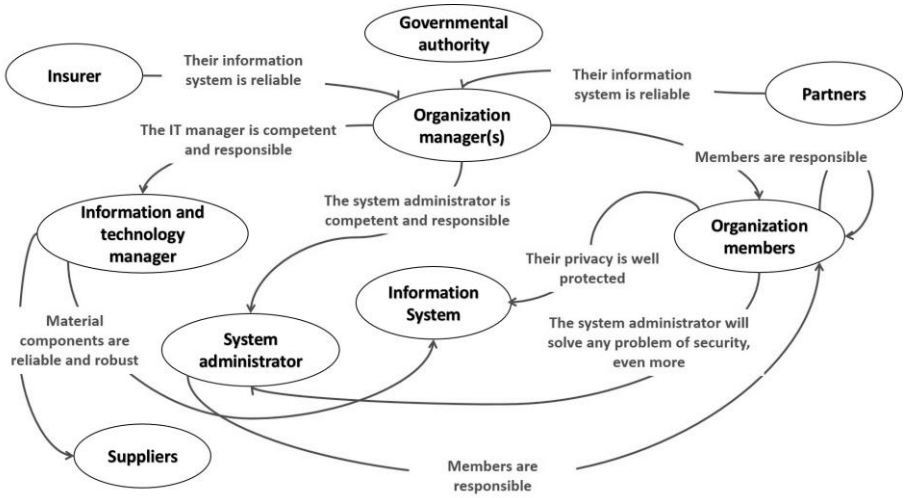

Figure 3. Examples of trusts around information systems. Trustors and trustees are circled, the direction of arrows point out the object of trust (i.e., the trusted), and the texts over the arrows are examples of trustors' expectations.

Of course, with regard to an organization's information system, objects of trust as well as trustors and their expectations are not restricted to those illustrated in Figure 4. Above all, the interrelationships between the different forms of trust are likely more developed and more complex in case of dependency or interdependency with one or more critical infrastructure(s). It is therefore obvious that trusts are mutually interdependent in critical infrastructures in the sense that trustors' expectations rely on the achievement of other expectations from others trustors.

The main difficulty in inferring what could be the content of expectations is due to the necessity to distinguish trustors' expectations and **trust dimensions** (also named antecedents in the literature) although they may overlap. For instance, system administrators may expect that users of information systems would be responsible with regard to cybersecurity; a dimension of this interpersonal trust could be the users' awareness of security issues: the more the administrators perceive that users are aware, the more likely they would trust them and extend access rights. According to Castelfranchi and Falcone (2000), "the quantitative dimensions of trust are based on the quantitative dimensions of its cognitive constituents" (p. 7). These constituents, or "mental ingredients" are the beliefs and evaluations on which trust is based, and explain the content of expectations. In other words, trust dimensions are the core of trust's dynamics. Indeed, the strength of expectations and, therefore, the level of trust as well vary depending on external factors related to the object of trust as well as on personal, social, and cultural characteristics related to the trustor; (e.g., Hancock *et al*., 2011; Hoff and Bashir, 2014; Mayer *et al*., 1995; McKnight and Chervany, 2001). Examples of dimensions related to the trustors are: disposition to trust; optimism bias; faith in humanity or in social order; subjective norms (e.g., Dzindolet *et al*., 2003; Li *et al*., 2008; McKnight and Chervany, 2006). Examples related to human trustees are: benevolence, integrity, morality, credibility, motives, abilities, expertise (Mayer *et al*., 1985; McKnight and Chervany, 2001); dimensions of trust within teams and/or organizations are: trust climate, organizational culture, culture of trust (Karsenty, 2015; Uslaner, 2012). Examples related to the technologies as trustees are: dependability, reliability, predictability, failures rates, false alarms, transparency, safety, performance (e.g., Hancock *et al*., 2011; Hasselbring and Reussner, 2006; Li *et al*., 2008; Schaefer et al., 2016).

Two aspects characterize **trust dynamics**: how it is built and how it evolves. In the absence of direct experience with the trusted, **a priori trust** or **initial trust** is built based on information from third parties, reputation, first impressions, or documents, and depends on personal characteristics such as the disposition to trust (e.g. McKnight and Chervany, 2006). Once interactions between trustors and trustees are established, **good reasons-based trust** is built from facts, relying on trustors' trial and error experience, understanding of the trustees' characteristics, predictability and limits, etc. (e.g., Lewicki and Bunker, 1996; Muir, 1994; Numan, 1998). Trust and distrust are alive, they increase or decrease depending on how expectations are met (or unmet as, for example, in trust violation in interpersonal relationships). Trust and distrust also evolve locally based on situational factors: they may be inappropriate in some situations. The concept of **trust calibration** (Muir, 1994) illustrates this need to adjust trust, and thus expectations, to the

context. For example, in the field of automation, in the case of choice between manual and automated control, human operators should distrust automation in contexts in which they know that automation cannot perform well; and they should trust automation when their own performance might be worse than that of automation. In a general way, appropriate distrust favors protective attitudes and behaviors against potential harmful actions (e.g., Lewicki *et al*., 1998).

To end this chapter, let us introduce two other concepts around trust. Besides the understanding of human relationships and behaviors for establishing **trustworthy interactions**, for instance, in organizations (Whitener *et al*., 1998), other objectives of research on trust and its dimensions are to design **trustworthy technical systems**, i.e., that would induce appropriate trust for appropriate reliance on those systems (e.g., Lee and See, 2004) and, **trustworthy ICT**, i.e., that would be safe and/or secure. Logically, designing trustworthy interactions, socio-technical systems, or technologies should be based on trust dimensions, making it worthwhile to study these dimensions. Finally, we define **trustworthiness** as a quality, more precisely the degree to which an object could be trusted given the expectations toward it. Here also, the properties of trustworthiness are closely linked to trust dimensions. For instance, in computer science, trustworthiness combines reliability and security (Yasinsac and Irvine, 2013).

To recap, trust is a state of expectations held by trustors toward the object of their trust (the trusted). Dimensions of trust are the factors that make levels of trust varying. These dimensions refer not only to the object of trust, but also to the individual, social, cultural, and contextual characteristics. Finally, what is important in the concept of trust is its dimensions: knowing the factors involved in trust building, maintaining, decline, and recovery allows researchers to design trustworthy relationships, socio-technical systems, or IC technologies as well as to create metrics of trustworthiness for decision-making.

Before describing our view on trust research on information systems security, the following chapter describes some trends in research on critical infrastructure protection involving information systems.

4. Trends in research on critical infrastructure protection involving information systems

The main purpose of scientific works carried out within the framework of the protection of critical infrastructures is to identify, understand, and analyze their vulnerabilities and interdependencies in order to predict, prevent, mitigate, and respond to security threats, cascading failures and their impacts. Research on critical infrastructures involving ICT can be categorized into two groups: on the one hand, research focusing on critical infrastructures that are dependent on or interdependent with information infrastructure or ICT; on the other hand, research aiming to contribute to the protection of critical information infrastructure. As mentioned earlier, the sector of ICT includes the Internet, information systems, industrial control systems such as SCADA and DCS systems, fixed and mobile

communications, satellite communication, radio communication and navigation, and broadcasting. Nevertheless, in this paper we consider only the work involving information systems, and only in terms of their security, but a lot of work is dedicated to other information and communication technologies (see, for example, for SCADA systems in critical infrastructures, Miller and Rowe, 2012 and Ten *et al.*, 2010; for communication networks, Duan *et al*., 2016 and Ericsson, 2010; etc.).

As emphasized by O'Brien and Marakas (2010), value of information systems to the modern organization is unlike any other system ever created (p. 31). That renders them particularly vulnerable (see Bisogni and Cavallini, 2010). The definition of information systems (IS) adopted in this paper is that of both technical and social perspectives, that is to say, an information system is the combination of human and material resources (people, hardware, software, data, networks, etc.) which work together to achieve a common goal by collecting, retrieving, processing, storing, and disseminating data and information (e.g., Arduin *et al*., 2015; Huber *et al*., 2017; O'Brien and Marakas, 2010). It means therefore that any part of information systems may be vulnerable and induce vulnerability to the whole of any IS-based critical infrastructure. The reminder of the chapter presents examples of academic works related to information system security that were carried out to contribute to critical infrastructure protection. These works can be categorized into two groups: theoretical and empirical research.

4.1. Examples of theoretical works

The report by Anderson (1999) summarizes the results of a workshop held in California in August 1999 on research and development initiatives concerning the prevention, detection, and response to insiders' misuse of critical defense information systems. The workshop was carried out within the program to protect America's infrastructures[9]. The report is very rich and instructive, contains useful definitions and, above all, many tracks of research, for instance, developing an insider trust model.

The article by Bialas (2006) explains the similarities and differences between the concepts of information security management and critical information infrastructure protection (CIIP). While information security management concerns one organization and is well defined by standards (see, for example, Pinheiro and Júnior 2016), there are not yet dedicated standards to CIIP although knowledge and guidelines do exist: Bialas cited, among others, Bruce *et al*., 2005, but the reader can also refer to works mentioned earlier (i.e., ENISA, 2016; NISC, 2007; NIST, 2014; OECD, 2015). However, although CIIP covers a larger scale than even the biggest organization, Bialas considered that some tools of information security management could be adapted to CIIP (e.g., the plan-do-check-act scheme), but the best would be to develop new ones that would take dependencies into account: intra-dependencies between the different layers of a critical infrastructure (physical layer, cyber layer,

9. President's Commission on Critical Infrastructure Protection (1997). *Critical foundations. Protecting America's infrastructures*: https://fas.org/sgp/library/pccip.pdf.

organizational layer, and strategic business layer at national or international level) and interdependencies between infrastructures.

The article by Dunn (2005) contains several observations. Among them, firstly, CIIP is mainly handled by engineers, consultants, practitioners and security experts who do not deal with the socio-political dimensions of CIIP. Secondly, critical infrastructure protection (CIP) and CIIP are ill-defined if the aspects of services, role and function for society are not taken into account in the objects of protection. That plus the inherent socio-political and cognitive dimensions of CIP/CIIP make a new problem that requires new analytical techniques and methodologies. Thirdly, the question of policies depends on the country (see CSS, 2008), the emphasis of CIIP may be on rather national security; rather economics; or rather law enforcement: the consequence is that determining appropriate protection efforts, goals, strategies, and instruments will depend on the key actors who are involved (respectively: security establishment, private sector, and law enforcement establishment). The conclusion of Dunn is the same as Bialas's: CIP and CIIP require new holistic approaches, methods, and tools.

4.2. Examples of empirical works

The work of Rieke (2004) presents an approach that carefully analyzes the parts of critical information infrastructure which really need protection. An operational formal model of information systems of government/enterprise and their attackers' behavior is proposed in order to carry out vulnerability analysis of government/enterprise networks. His model includes a model of the network structure and configuration; a model of vulnerabilities; and a model of attacker capabilities and profile (Figure 4). Based on the graph of all possible attack paths, the operational model allows to detect attack in an early phase and/or find out the best protection to block attack paths.

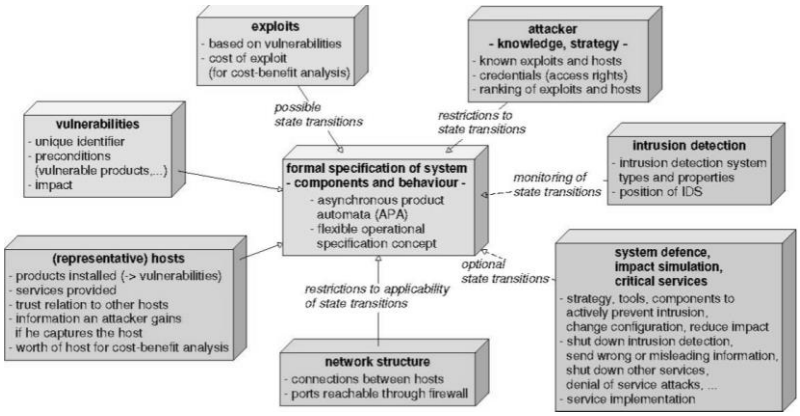

Figure 4. Component of Rieke's model of enterprise network vulnerabilities (in Rieke, 2004, p. 6)

The work of Keeney *et al*. (2005) reports a deep analysis of computer system sabotage perpetrated by organizations' insiders across US critical infrastructures. The findings were utilized by Gonzalez *et al*. (2006) in their empirical work on 'social engineering', a concept defined from the point of view of the hacker: social engineering is "the term that hackers give to acquiring information about computer systems through non-technical means" (Winkler, 1996), in other words, a "manipulation of people" by "psychological forcing" in order to breach the security system. Gonzalez *et al*. proposed to model critical ICT infrastructures and threats, particularly social engineering attacks in order to recognize attack patterns through the modeling of archetypes inspired by chess game.

The work of Leszczyna *et al*. (2011) proposes an approach to the security assessment of the information systems of critical infrastructures, based on the simulation of attacks with MAISim (Mobile Agent Malware Simulator) that can simulate well-known malware as well as generic behaviors (e.g., file sharing propagation) and non-existent configurations. The steps of the approach are the following: analysis of the ICT system of the critical infrastructure; reconstruction of the evaluated information system in a computer security laboratory; identification of use scenarios from a prior analysis of the utilization of the system by its users as well as from operational procedures, security policies, etc.; experiments; and analysis of results. What is interesting is that these results are employed to build a tool that help users to decide on the trustworthiness of the system. The tool named 'trust case' is graphic-based document. The approach had been applied to the verification of the security of industrial controls systems and power plants. For more details on MAISim, see Leszczyna *et al*. (2010).

The work of Bisogni and Cavallini (2010) presents the Vulnerability of Information Systems (VIS) model dedicated to the assessment of the economic sectors that are most vulnerable to critical information system breakdowns. The model is based on the simulation of information systems (IS) like in Leszczyna *et al*. (2011). More precisely, the VIS model simulates IS disruptions and assesses their socio-economic impact on the affected sectors. It also ranks sectors according to the vulnerability to IS disruptions.

To conclude this presentation of works on information system security under the perspective of critical infrastructure protection, it must be emphasized that it was not the objective to carry out an exhaustive review of research on information system security within the framework of critical infrastructure protection (CIP) and critical information infrastructure protection (CIIP). The presented empirical works address an important aspect of CIP in general which is the identification of vulnerabilities, here, seen as the degree of exposure to cyber-threats. However, apart from the VIS model in Bisogni and Cavallini (2010), most of proposed solutions remain within the perimeter of two-agent interactions (system - user or attacker or both). That confirms that Bialas (2006) and Dunn (2005) were right: CIP and CIIP require new holistic approaches and methods. Moreover, we failed at distinguishing CIP and CIIP in the literature that we reviewed. Therefore, it may be that, at least with regard to research on the security of information systems (IS), the French designation of

"*systèmes d'information d'importance vitale*" (see SGDSN, 2016[10]) would be a relevant operational definition regarding the protection of IS-based critical infrastructures.

It may also be, as noticed by Dunn (2005), that new mindsets are necessary. Indeed, only new approaches could consider a holistic perspective of vulnerabilities in the whole of critical infrastructures. The next chapter presents our view of a CIP-based approach to trust research with regard to the security of information systems that are vital for the society.

5. A human and social science view of research on trust and information system security under the perspective of critical infrastructure protection

This chapter presents our view of the research that should be applied to information system security under the perspective of critical infrastructure protection, with a particular focus on trust. Firstly, we adopt the French terminology of vital information systems to mean clearly information systems that are vital to the society, that is to say, which disruption or destruction would have a significant impact on vital societal functions, health, safety, security, economic or social well-being. This definition reproduces the definition of critical infrastructures, which allows us to remain in the context of critical infrastructure protection (CIP). Secondly, our view hinges on transdisciplinarity. We first explain why, and then we concretize this view through examples of future work.

As previously mentioned, the main objectives of research on trust are, firstly, to understand the role of trust in individual and social decisions and behaviors and, secondly to design trustworthy relationships, socio-technical systems, and technologies such as ICT. Research on decisions and behaviors involves not only disciplines of human and social sciences such as psychology, sociology, organizational science, economics, politics, etc. but also cognitive engineering. Human and social sciences are mainly interested in interpersonal trust, systemic trust, and trust in technology while cognitive engineering is interested in trust in technology. As for ICT, the design of trustworthy ICT has even led to the discipline of trustworthy computing (see Yasinsac and Irvine, 2013). The concept of trust is considered in that field through properties of trustworthiness (e.g., reliability and security) which respond to standards and trust requirements. All those kinds of trust can be addressed at all levels of critical infrastructures that are made up of man-made systems as well as of people, organizations, and institutions.

However, in view of those many disciplines working mostly separately, it is more than likely that the understandings of trust do not necessarily overlap. For instance, dimensions of trust in information systems viewed by software developers are not the same as those of trust viewed by end-users and yet their trusts (i.e., their expectations) are not necessarily independent each other. It is a simplistic example, but at the scale of vital information systems, the interdependence of trust

10. https://www.ssi.gouv.fr/uploads/2016/06/communique_presse-cybersecurite-des-oiv.pdf

expectations of various actors may lead to a lack of mutual comprehension. The lack of mutual comprehension due to a lack of trust may be disastrous in situations of crisis management (Karsenty, 2015). For this author, trust management should be carried out prior to the occurrence of the crisis.

With regard to the security of information systems that are vital to the society, trust research should be considered from a non-disciplinary perspective, more precisely **research should be transdisciplinary**. It should not be surprising since it is the only way to produce new methodologies and tools as it was emphasized as necessary for critical infrastructure protection by Bialas (2006) and Dunn (2005). Indeed, while disciplinary research remains within the boundaries of disciplinary fields, non-disciplinary research combines elements from various disciplines in order to answer practical questions and to solve practical problems; "the interaction may range from communication and comparison of ideas, and the exchange of data, methods and procedures, to the mutual integration of organizing concepts, theories, methodology, and epistemological principles" (Van den Besselaar and Heimeriks, 2001, p. 706). Rosenfield (1992) distinguished three levels among non-disciplinary research. Multidisciplinarity is the first level: researchers work in parallel or sequentially from disciplinary specific base to address common problems. Interdisciplinarity is the second one: researchers work jointly but still from disciplinary-specific basis to address common problems. Finally, in transdisciplinarity, researchers work jointly using shared conceptual framework drawing together disciplinary-specific theories, concepts, and approaches to address common problems. More precisely, at the level of transdisciplinarity, researchers, stakeholders, and practitioners aim at **joint problem solving based on a common view** built from the integration of various disciplinary scientific knowledge as well as experience of stakeholders and practitioners (Gibbons and Nowotny, 2001; Pohl *et al*., 2008; Rosenfield, 1992).

That transdisciplinary perspective is closed to that hybrid one proposed by Le Coze (2011) for industrial safety assessment. Le Coze considers that articulating not only technological and human factors, but also organizational factors (because socio-technical systems have organizational properties) around a framework model (*modèle cadre*) is the best way to apprehend the complexity of industrial safety.

Getting back to trust research within the protection of critical infrastructures in general and of vital information systems in particular, concretely, an important step is to unify knowledge and experience of trust issues in critical infrastructure protection. That does not exclude to create new knowledge, but it should encompass human, technology, and society dimensions by crossing disciplines from human and social sciences (psychology, sociology, economics, etc.) to engineering and computer sciences. Organizational sciences might be the link between these soft and hard sciences because, as it is emphasized in Boy (2013) and Le Coze (2011), organization is at the heart of the functioning of socio-technical systems.

The techniques of ontology (e.g., Gruber, 1995), ontology alignment (e.g., Shvaiko and Euzénat, 2008), and ontology modularization (e.g., d'Aquin, 2012) are perfect tools for creating transdisciplinary knowledge bases composed of

heterogeneous information from various domains and that would be understandable by and sharable among all actors of critical infrastructure protection. Examples of competency questions (Ushold & Gruninger, 1996) that could guide ontologies building from a transdisciplinary view of critical infrastructure protection may be: How to characterize vulnerabilities in terms of their potential societal impacts (for instance, economic, health, and environmental costs)? What are the invariant characteristics of information systems that are vital to the society? How to identify vulnerabilities that could be due to inappropriate trust and distrust? How to identify interdependencies between trust expectations at people, technologies, organizational, and institutional levels which, if not fulfilled, could lead to vulnerabilities to a whole infrastructure?

Another important step is to work on meta-trustworthiness metrics of vital information systems, that is to say, metrics that would measure the degree to which these systems would be trustworthy, not only from a computer science viewpoint, but also from human and social sciences angle; and not only from the per se perspective, but also in view of the interdependencies between those systems and critical infrastructures of other sectors. The mathematical concept of trust reputation used in the domain of computer science (e.g. Alcaraz and Zeadally, 2015) could serve as a basis for research on such new metrics of meta-trustworthiness. These metrics would help managers, stakeholders, and institutions to prevent, mitigate, or respond to security threats due to lack of trustworthiness of the global vital information system including people.

Those two examples of works that could be carried out through a transdisciplinary protection of vital information systems are a small sample of what could be done. An agenda of research has first to be defined, of course, with a prior transdisciplinary dialogue between researchers, practitioners, experts, stakeholders, and governmental institutions.

6. Conclusion

This paper addresses issues of trust research related to the security of vital information systems (VIS). We propose to use the framework of critical infrastructure protection to deal with the complexity of such systems and avoid analyzing trust from only a two-agent interaction perspective, which could not be relevant given the society issues of the security of those systems. Indeed, the very definition of critical infrastructures involves vital services, that is to say, disruption or destruction of those infrastructures due to natural disasters, extreme weather conditions, industrial accidents, deliberate attacks, etc. would have a significant impact on vital societal functions, health, safety, security, economic or social well-being.

Until now, research in the framework of critical infrastructure protection is mainly carried out in engineering and computing sciences. Given the society issues, it is astonishing that the disciplines of human and social sciences are almost absent

from the research on that topic. And yet, to speak only about trust, they have a solid background of knowledge and savoir-faire.

Research on trust is fundamental to understand its role in individual and social behaviors and decisions, and to design trustworthy technologies. The former involves disciplines of human and social sciences as well as cognitive engineering. Human and social sciences are interested in interpersonal trust, systemic trust, and trust in technology while cognitive engineering is mainly interested in trust in technology. All these aspects of trust are useful for the protection of VIS. As for the design of trustworthy technologies, research is mainly carried out in the domain of computer science and has even led to the discipline of *trustworthy computing*. The concept of trust is considered in that discipline through properties of trustworthiness which respond to standards and trust requirements, of course, in the language of computer science.

It is not at all sure that researchers of the disciplines mentioned above have the same understanding of trust neither of security. That could be particularly appalling in today's world relying on information and communication technologies and because the worse of cyber-attacks is to come given the deployment of cloud computing and the Internet of Things.

With regard to the protection of VIS, trust research should be considered from a transdisciplinary perspective. It is the only way to produce new knowledge, methodologies and tools necessary for critical infrastructure protection. Researchers, stakeholders, and practitioners will work jointly based on a common view of the physical, functional, and organizational aspects of VIS, which will be built from the integration of various disciplinary knowledge as well as experience of stakeholders and practitioners. The first step would be, therefore, to build transdisciplinary knowledge bases (for instance, with techniques such ontology, ontology matching, and ontology modularization) that would be understandable by all parties. Another step is to work on metrics of meta-trustworthiness of VIS, that is to say, metrics that would measure the degree to which these systems would be trustworthy, not only from a computer science viewpoint, but also from human and social sciences angle; and not only from a per se perspective, but also in view of their interdependencies with critical infrastructures of other sectors.

To conclude, a preliminary working program is proposed:

- Organizing national, European, and/or international workshops gathering together experts in the domain of critical infrastructure protection and vital information systems in order to present safety, security and society issues of critical infrastructures and vital information systems as well as to provide definitions that could constitute a basis for a common background.

- Identifying researchers in each scientific discipline who could work on trust issues of vital information systems, as well practitioners and institutional experts.

- Organizing workshops with these identified actors to: (1) discuss about the conceptual approaches, methods, and tools in each discipline which could be used to

create common conceptual and methodological approaches; and (2) define a short-, medium-, and long-term working agenda.

Acknowledgements:

The author warmly thanks Kathia Oliveira and Pierre-Emmanuel Arduin to have offered her the opportunity to write on the topic of trust in the field of computer science.

She also thanks the three anonymous reviewers for their precious comments and suggestions.

References

Aberer K., Despotovic Z. (2001). Managing trust in a peer-2-peer information system. *Proceedings of the Tenth International Conference on Information and Knowledge Management (CIKM 2001)*. ACM, New York, NY.

D'Aquin M. (2012). Modularizing ontologies. In M. C. Suárez-Figueroa, A. Gómez-Pérez, E. Motta, A. Gangemi. (Eds.), *Ontology engineering in a networked world* (Chapter 10, pp. 213-233). Springer-Verlag Berlin Heidelberg.

Alcaraz C., Zeadally S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructures*, vol. 8, pp. 53-66.

Arduin P.-E., Grundstein M., Rosenthal-Sabroux, C. (2015). *Information and knowledge systems*. ISTE Ltd and Wiley, London.

Aven T. (2011). On some recent definitions and analysis frameworks for risk, vulnerability, and resilience. *Risk Analysis*, vol. 31, n° 4, pp. 515-522.

Bach C., Bouchon S., Fekete A., Birkmann J., Serre D. (2013). Adding value to critical infrastructure research and disaster risk management: The resilience concept. *Surveys and Perspectives Integrating Environment and Society*, vol. 6, n°1.

Barber B. (1983). *The logic and limits of trust*. Rutgers University Press, New Brunswick, NJ.

Bisogni F., Cavallini S. (2010). Assessing the economic loss and social impact of information system breakdowns. In T. Moore, S. Shenoi (Eds.), *Critical infrastructure protection IV. Fourth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, ICCIP 2010* (Chapter 13, pp. 185-198). Springer-Verlag, Berlin Heidelberg.

Bouchon S. (2006). *The vulnerability of interdependent critical infrastructures systems: Epistemological and conceptual state of the art*. European Commission, Brussels. Institute for the Protection and Security of the Citizen, Ispra, Italy.

Bouwmans I., Weijnen M. P. C., Gheorge A. (2006). Infrastructures at risk. In A.V. Gheorge, M. Masera, M. Weijnen, De L. Vries (Eds.), *Critical infrastructures at risk. Securing the European electric power system* (Chapter 2, pp. 19-36). Springer, Netherlands.

Boy G. A. (2013). Dealing with the unexpected in our complex socio-technical world. In *Proceedings of the 12th IFAC Symposium on Analysis, Design, and Evaluation of Human-Machine Systems*, vol. 46, n°15, pp. 402-409.

Bruce R., Dynes S., Brechbuhl H., Brown B., Goetz E., Verhoest P., Luiijf E. Helmus S. (2005). *TNO Report 33680. International policy framework for protecting critical information infrastructure: A discussion paper outlining key policy issues* (at Tuck School of Business, Dartmouth College, Hanover, NH). TNO Information and Communication Technologies, Delft, Netherlands. Electronic document, accessed 01/12/2016: http://www.ists.dartmouth.edu/library/158.pdf.

Carter L., Bélanger, F. (2005). The utilization of e- government services: citizen trust, innovation and acceptance factors. *Information Systems Journal*, vol. 15, n°1, pp. 5-25.

Castelfranchi C., Falcone R. (2000). Trust is much more than subjective probability: Mental components and sources of trust. *Proceedings of the 33rd Hawaii International Conference on System Sciences*. IEEE, Piscataway, NJ.

Chopra S., Khanna V. (2015). Interconnectedness and interdependencies of critical infrastructures in the US economy: Implications for resilience. *Physica A: Statistical Mechanics and its Applications*, vol. 436, pp. 865-877.

CREDC (2016). *Report of Discussions from Breakout Sessions of the 2016 Annual Industrial Workshop of the Cyber Resilient Energy Delivery Consortium*. Electronic document, accessed 28/11/2016: https://cred-c.org/files/2016/09/CREDC-IW2016_Breakout-Discussion-Report_FINAL.pdf.

CSS (2008). *International CIIP Handbook 2008/2009. An inventory of 25 national and 7 international critical information infrastructure protection policies*. Center for Security Studies, ETH, Zurich.

Deutsch M. (1958). Trust and suspicion. *The Journal of Conflict Resolution*, vol. 2, n°4, pp. 265-279.

Dietz G., Den Hartog, D. N. (2006). Measuring trust inside organizations. *Personnel Review*, vol., 35, n°5, pp. 557-588.

Disterer G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, vol. 4, n°2, pp. 92-100.

Dzindolet M.T., Peterson S.A., Pomranky R.A., Pierce L.G. Beck H.P. (2003). The role of automation trust in automation reliance. *International Journal of Human-Computer Studies*, vol. 58, n°6, pp. 697-718.

Duan S., Lee S., Chinthavali S. (2016). Reliable communication models in interdependent critical infrastructure networks. *Proceedings of 2016 Resilience Week (RWS)*. IEEE, Piscataway, NJ.

Dunn M. (2005). The socio-political dimensions of critical information infrastructure protection (CIIP). *International Journal of Critical Infrastructures*, vol. 1, n° 2/3, pp. 258-268.

EC (2005). *COM(2005) 576 final: Green Paper on a European Programme for Critical Infrastructure Protection*. European Commission, Brussels.

EC (2006). C*OM(2006) 786 final: European Programme for Critical Infrastructure Protection EPCIP*. European Commission, Brussels.

EC (2008). *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*. European Commission, Brussels.

EC (2013). *SWE(2013) 318 final: Commission staff working document on a new approach to the European programme for critical infrastructure protection making European critical infrastructures more secure*. European Commission, Brussels.

ENISA (2016). *Stocktaking, analysis and recommendations on the protection of CIIs*. European Union Agency for Network and Information Security, Heraklion, Greece.

Ericsson G. N. (2010). Cyber security and power system communication—Essential parts of a smart grid infrastructure. *IEEE Transactions on Power Delivery*, vol. 25, n°3, pp. 1501-1507.

Eusgeld I., Nan C., Dietz S. (2011). System-of-systems approach for critical infrastructures. *Reliability Engineering and System Safety*, vol. 96, n°6, pp. 679-686.

Firesmith D. G. (2003). *Common concepts underlying safety, security, and survivability engineering*. Technical Report CMU/SEI-2003-TN-033, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, December 2003.

Fogel J, Nehmad E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, vol. 25, n°1, pp. 153-60.

Fulmer C. A., Gelfand, M. J. (2015). Trust after violations: Are collectivists more or less forgiving? *Journal of Trust Research*, vol. 5, n°2, pp. 109-131.

Galland J.-P. (2010). Critique de la notion d'infrastructure critique. *Flux*, vol. 3, n° 81, pp 6-18.

Geoffroy C., Rigaud E., Guarnieri F. (2017). Resilience activation in extreme situations: A literature review. In L. Walls, M. Revie, T. Bedford (Eds.), *Risk, Reliability and Safety: Innovating Theory and Practice. Proceedings of ESREL 2016* (pp.2231-2237). CRC Press, Taylor & Francis Group, London.

Gibbons M., Nowotny H. (2001). The potential of transdisciplinarity. In J. Thompson Klein *et al*. (Eds), *Transdisciplinarity: Joint problem solving among science, technology, and society. An Effective Way for Managing Complexity* (pp. 67-80). Birkhäuser Verlag GmbH, Basel, Switzerland.

Gonzalez J.J., Sarriegi J. M., Gurrutxaga A. (2006). A framework for conceptualizing social engineering attacks. In J. Lopez (Ed.), Critical information infrastructures security. *Proceedings of the First International Workshop in Critical Information Infrastructures Security CRITIS 2006* (pp. 79-90). Springer-Verlag Berlin Heidelberg.

Gruber T. R. (1995). Toward principles for the design of ontologies used for knowledge sharing. *International Journal of Human-Computer Studies*, vol. 43, n°5-6, pp. 907-928.

Grimsman D., Chetty V., Woodburry N., Vaziripour E., Roy S., Zappala D., Warnick S. (2016). A case study of a systematic attack design method for critical infrastructure cyber-physical systems. *Proceedings of 2016 American Control Conference (ACC 2016)*. Boston, MA.

Haimes Y.Y. (2009). On the definition of resilience in systems. *Risk Analysis*, vol. 29, n°4, pp. 498-501.

Haimes Y., Santos J., Crowther K., Henry M., Lian C., Yan Z. (2008). Risk analysis in interdependent infrastructures. In E. Goetz, S. Shenoi (Eds.), *Critical Infrastructure*

Protection. ICCIP 2007. IFIP International Federation for Information Processing, vol. 253 (pp. 297-310). Springer, Boston, MA.

Hämmerli B. M. (2005). C(I)IP task description and a proposal for a substitute of national C(I)IP policies. *Proceedings of the First IEEE International Workshop on Critical Infrastructure Protection (IWCIP'05)*. IEEE, Piscataway, NJ.

Hancock P. A., Billings D. R., Schaefer K. E., Chen J. Y., De Visser E. J., Parasuraman, R. (2011). A meta-analysis of factors affecting trust in human-robot interaction. Human Factors, vol. 53, n°5, pp. 517-527.

Hardin R. (2002). *Trust and trustworthiness*. Russell Sage Foundation, New York, NY.

Hasselbring W., Reussner, R. H. (2006). Toward trustworthy software systems. *IEEE Computer*, vol. 39, n°4, pp. 91-92.

Hoff K. A., Bashir M. (2014). Trust in automation: Integrating empirical evidence on factors that influence trust. *Human Factors*, vol. 57, n°3, pp. 407-434.

Huber M. W., Piercy C. A., Mickeown P.G. (2007). *Information systems: Creating business value*. John Wiley & Sons, Hoboken, NJ.

Karabacak, B. Yildirim S. O., Bayka N. (2016). A vulnerability driven cybersecurity maturity model for measuring national critical infrastructure protection preparedness. *International Journal of Critical Infrastructure Protection*, vol. 15, pp. 47-59.

Karsenty L. (2015). Comment maintenir des relations de confiance et construire du sens face à une crise ? *Le travail humain*, vol. 78, n°2, pp. 141-164.

Keeney M, Kowalski E., Cappelli D., Moore A., Shimeall T., Rogers, S. (2005). *Insider threat study: Computer system sabotage in critical infrastructure sectors*. US Secret Service and CERT Coordination Center/Software Engineering Institute, Pittsburgh, PA. Electronic document, accessed 01/12/2016: https://resources.sei.cmu.edu/asset_files/SpecialReport/2005_003_001_51946.pdf.

Kramer R.M. (1999). Trust and distrust in organizations: emerging perspectives, enduring questions. *Annual Review of Psychology*, vol. 50, n°1, 569-598.

Kröger W., Zio E. (2011). *Vulnerable systems*. Springer-Verlag, London.

Lamsal P (2001). *Understanding Trust and Security*. Department of Computer Science. University of Helsinki, Finland. Electronic document, accessed on 23/11/2016: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.17.7843&rep=rep1&type=pdf.

Le Coze J. C. (2011). *De l'investigation d'accident à l'évaluation de la sécurité industrielle: proposition d'un cadre interdisciplinaire (concepts, méthode, modèle)*. Thèse en Gestion et Management, École Nationale Supérieure des Mines de Paris, Paris.

Lee J. D., See, K. A. (2004). Trust in technology: Designing for appropriate reliance. *Human Factors*, vol. 46, n°1, pp. 50-80.

Leszczyna R., Fovino I. N., Masera M. (2010). Simulating malware with MAISim. *Journal in Computer Virology*, vol. 6, n°1, pp. 66-75.

Leszczyna R., Fovino I. N., Masera M. (2011). Approach to security assessment of critical infrastructures' information systems. *IET Information Security*, vol. 5, n°3, pp. 135-144.

Lewicki R. J., Bunker B. B. (1996). Developing and maintaining trust in work relationships. In R. M. Kramer and T. R. Tyler (Eds.), *Trust in organizations: Frontier of theory and research* (pp. 114-139). Sage Publications, Thousand Oaks, CA.

Lewicki R. J., McAllister D. J., Bies, R. J. (1998). Trust and distrust: New relationships and realities. *Academy of Management Review*, vol. 23, n°3, pp. 438-458.

Lewis J. D., Weigert A. (1985). Trust as a social reality. *Social Forces*, vol. 63, n°4, pp. 967-985.

Lewis J. D., Weigert A. J. (2012). The social dynamics of trust: Theoretical and empirical research, 1985–2012. *Social Forces*, vol. 91, n°1, pp. 25-31.

Li X., Hess, T. J. Valacich J. S. (2008). Why do we trust new technology? A study of initial trust formation with organizational information systems. *The Journal of Strategic Information Systems*, vol. 17, n°1, pp. 39-71.

Luhmann N. (2000). Familiarity, Confidence, Trust: Problems and Alternatives. In D. Gambetta (Ed.), *Trust: Making and Breaking Cooperative Relations* (Chapter 6, pp. 94-107), electronic edition (http://www.sociology.ox.ac.uk/papers/luhmann94-107.pdf). Department of Sociology, University of Oxford, Oxford, U.K.

Luiijf E., Klaver M. (2015). Governing critical ICT: Elements that requires attention. *European Journal of Risk Regulation*, vol. 6, n°2, pp. 263-270.

Luzeaux D. (2010). System of systems. From concept to actual development. In D. Luzeaux and J.-R. Ruault (Eds.) *Systems of Systems* (Chapter 1, pp. 1-88). ISTE Ltd and Wiley, London.

McKnight D. H., Carter M., Thatcher J. B., Clay P. F. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems (TMIS)*, vol. 2, n°2, Article 12.

McKnight, D. H., Chervany, N. L. (2001). Trust and distrust definitions: One bite at a time. In R. Falcone, M. Singh, Y.-H. Tan (Eds.), *Trust in cyber-societies* (pp. 27–54). Springer-Verlag Berlin Heidelberg.

McKnight D. H., Chervany, N. L. (2006). Reflections on an initial trust-building model. In R. Bachmann and A. Zaheer (Eds.) *Handbook of trust research* (Chapter 2, pp. 29-51). Edward Elgar Publishing, Cheltenham, U.K.

Mangin J.-P. L. (2014). The moderating role of risk, security and trust applied to the TAM model in the offer of banking financial services in Canada. *Journal of Internet Banking and Commerce*, vol. 19, n°2, pp.1-21.

Mayer R.C., Davis J.H., Schoorman, F.D. (1995). An integrative model of organizational trust. *Academy of Management Journal*, vol. 20, n°3, pp. 709-734

Misztal B. A. (1996, 2013). *Trust in modern societies: The search for the bases of social order* (2013 e-book version). Polity Press, Cambridge, U.K.

Miller B., Rowe D. (2012). A survey of SCADA and critical infrastructure incidents, *Proceedings of the 13th Annual Conference on Information Technology Education and The 1st Annual Conference on Research in Information Technology (SIGITE/RIIT 2012)*. ACM, New York, NY.

Moteff J., Parfomak P. (2004). *Critical infrastructure and key assets: Definition and identification*. CRS Report for Congress, Congressional Research Service, The Library of

Congress, Washington, DC. Electronic document, accessed 23/11/2016: http://www.dtic.mil/dtic/tr/fulltext/u2/a454016.pdf.

Muir B. M. (1987). Trust between humans and machines, and the design of decision aids. *International Journal of Man-Machine Studies*, vol. 27, n°5-6, pp. 527-539.

Muir B. M. (1994). Trust in automation: Part I. Theoretical issues in the study of trust and human intervention in automated systems. *Ergonomics*, vol. 37, n°11, pp. 1905-1922.

NISC (2007). *Japanese Government's efforts to address information security issues*. National center of Incident readiness and Strategy for Cybersecurity, Tokyo (see http://www.nisc.go.jp/eng/).

NIST (2014). *Framework for improving critical infrastructure cybersecurity*. National Institute of Standards and Technology, Gaithersburg, MD.

Numan J. H. (1998). *Knowledge-based systems as companions. Trust, human computer interaction and complex systems*. Doctoral thesis, University Library, Groningen, The Netherlands.

O'Brien J. A., Marakas G. M. (2010). *Information management systems*, Tenth Edition, McGraw-Hill/Irwin, New York, NY.

OECD (2015). *Digital security management for economic and social prosperity. OECD recommendation and companion document*. Organization for Economic Co-operation and Development, OECD Publishing, Paris.

Offor P. I. (2013). Managing Risk in Secure System: Antecedents to System Engineers' Trust Assumptions Decisions. *Proceedings of 2013 International Conference on Social Computing (SocialCom)*. IEEE, Piscataway, NJ.

Pinheiro, F. S., Júnior W. R. (2016). Information security and ISO 27001. *Revista de Gestão & Tecnologia*, vol. 3, n°3, pp. 20-28.

Pohl C., Hadorn, G. H. (2008). Methodological challenges of transdisciplinary research. *Natures Sciences Sociétés*, vol. 16, n°2, pp. 111-121.

President's Commission on Critical Infrastructure Protection (1997). *Critical foundations. Protecting America's infrastructures*. Electronic document, accessed 01/12/2016: https://fas.org/sgp/library/pccip.pdf.

Rieke R. (2004). Tool based formal modelling, analysis and visualisation of enterprise network vulnerabilities utilising attack graph exploration. In U. E. Gattiker (Ed.), *EICAR 2004 Conference CD-rom: Best Paper Proceedings*. Electronic document, accessed 01/12/2016: http://sit.sit.fraunhofer.de/smv/publications/download/Eicar-2004.pdf.

Rinaldi S. M., Peerenboom J. P., Kelly T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems*, vol. 1, n° 6, pp. 11-25.

Rosenfield P. L. (1992). The potential of transdisciplinary research for sustaining and extending linkages between the health and social sciences. *Social Science & Medicine*, vol. 35, n°11, pp. 1343-1357.

Ruotsalainen P., Nykänen P., Seppälä A., Blobel B. (2014). Trust-based information system architecture for personal wellness. *Proceedings of MIE2014*. Electronic document, accessed 23/11/2016: http://ebooks.iospress.nl/bookseries/studies-in-health-technology-and-informatics.

Santos J. R., Herrera L. C., Yu K. D. S., Pagsuyoin S. A. T., Tan R. R. (2014). State of the art in risk analysis of workforce criticality influencing disaster preparedness for interdependent systems. *Risk Analysis*, vol. 34, n° 6, pp. 1056-1068.

Schaefer K. E., Chen J. Y., Szalma J. L., Hancock P. A. (2016). A meta-analysis of factors influencing the development of trust in automation: Implications for understanding autonomy in future systems. *Human Factors*, vol. 58, n°3, pp. 377-400.

Schoorman F. D., Mayer R. C., Davis, J. H. (2007). An integrative model of organizational trust: Past, present, and future. *Academy of Management Review*, vol. 32, n°2, pp. 344-354.

Shvaiko P., Euzenat J. (2008) Ten Challenges for Ontology Matching. In: Meersman R., Tari Z. (Eds.), *On the Move to Meaningful Internet Systems: OTM 2008*. Lecture Notes in Computer Science, Vol. 5332 (pp. 1164-1182). Springer-Verlag Berlin Heidelberg.

SGDSN (2016). *Publication des premiers arrêtés sectoriels relatifs à la sécurité des systèmes d'information des opérateurs d'importance vitale*. Communiqué de Presse du 27 juin 2016, Secrétariat Général de la Défense et de la Sécurité Nationale, Paris.

Stergiopoulos G., Kotzanikolaou P., Theocharidou M., Lykou G., Gritzalis D. (2016). Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures. *International Journal of Critical Infrastructure Protection*, vol. 12, pp. 46-60.

Swamynathan G., Zhao B. Y., Almeroth K. C. (2005). Decoupling service and feedback trust in a peer-to-peer reputation system. *Proceedings of Parallel and Distributed Processing and Applications – ISPA 2005 International Workshop on Applications and Economics of Peer-to-Peer Systems (AEPP 2005)*. Springer-Verlag Berlin Heidelberg.

Ten C. W., Manimaran G., Liu C. C. (2010). Cybersecurity for critical infrastructures: Attack and defense modeling. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 40, n°4, pp. 853-865.

Thakur K., Ali M. L., Jiang N., Qiu M. (2016). Impact of cyber-attacks on critical infrastructures. *Proceedings of 2016 IEEE 2nd International Conference on Big Data Security on Cloud*. IEEE, Piscataway, NJ.

Thuderoz C. (2003). Introduction au propos : la confiance en question. In V. Mangematin et C. Thuderoz (Eds.), *Des mondes de confiance. Un concept à l'épreuve de la réalité sociale* (Chapitre 1, pp. 19-30). CNRS Editions, Paris.

Truong N. B., Um T. W., Lee G. M. (2016). A Reputation and knowledge-based trust service platform for trustworthy social Internet of Things. *Proceedings of the 19th Conference on Innovations in Clouds, Internet, and Networks (ICIN 2016)*. IOS Press BV, Amsterdam.

Uschold M., Gruninger M. (1996). Ontologies: Principles, methods and applications. *The Knowledge Engineering Review*, vol. 11, n°2, pp. 93-136.

Uslaner E. M. (2002). *The moral foundations of trust*. Cambridge University Press, Cambridge, U.K.

Van den Besselaar P.A.A, Heimeriks G. (2001). Disciplinary, multidisciplinary, interdisciplinary: Concepts and indicators. *Proceedings of the 8th International Conference on Scientometrics and Informetrics (ISSI 2001)*. UNSW Press, Kensington, Australia.

Warrington T. B., Abgrab N. J., Caldwell H. M. (2000). Building trust to develop competitive advantage in e-business relationships. *Competitiveness Review: An International Business Journal*, vol. 10, n°2, pp. 160-168.

Whitener E. M., Brodt S. E., Korsgaard M. A., Werner J. M. (1998). Managers as initiators of trust: An exchange relationship framework for understanding managerial trustworthy behavior. *Academy of Management Review*, vol. 23, n°3, pp. 513-530.

Yasinsac A., Irvine C. (2013). Help! Is There a Trustworthy-Systems Doctor in the House? *IEEE Security & Privacy*, vol. 1, n°1, pp. 73-77.

Zhou B., Joseph A., Sastry S. (2011). A taxonomy of cyber attacks on SCADA systems. *Proceedings of 2011 IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing*. IEEE, Piscataway, NJ

Zio E. (2009). Reliability Engineering: Old problems and new challenges. *Reliability Engineering and System Safety*, vol. 94, n°2, pp. 125-141.

Zio E. (2016). Critical infrastructures vulnerability and risk analysis. *European Journal for Security Research*, vol. 1, n°2, pp. 97-114.

Zolesio J.-L. (2010). Critical infrastructure protection. In D. Luzeaux and J.-R. Ruault (Eds.) *Systems of Systems* (Chapter 8, pp. 261-290). ISTE Ltd and Wiley, London.

Article reçu le : 19 décembre 2016

Article accepté le : 10 mars 2017