Eur J Secur Res (2019) 4:157–174
DOI 10.1007/s41125-017-0021-9

ORIGINAL ARTICLE

The Conceptual and Scientific Demarcation of Security in Contrast to Safety

S. H. Jore[1]

Received: 28 June 2017 / Accepted: 16 October 2017 / Published online: 7 November 2017

Abstract Increased focus on protection from terrorism, espionage, cybersecurity and other malicious crimes has led to increased academic interest in the topic of security, especially in risk and safety studies. This article aims to investigate the conceptual and scientific demarcation of security in contrast to safety, and discuss the status of security as an independent science. Security is a multifaceted concept and academic definitions often distinguish security from safety in terms of intentionality. However, intentionality also plays a part in safety research thus this is not a sufficient parameter for distinguishing the two fields. The dichotomy of non-malicious versus malicious is suggested as a means for differentiation. A new definition of security that incorporates elements associated with the current security research field is proposed. Security can be defined as *the perceived or actual ability to prepare for, adapt to, withstand, and recover from dangers and crises caused by people's deliberate, intentional, and malicious acts such as terrorism, sabotage, organized crime, or hacking*. The conclusion is that before security can be established as an independent discipline, it is necessary to determine what concepts and theories are related to the field, what levels of and objects in society should be included, in addition to the interrelationships and interdependencies with other disciplines.

Keywords Security · Security science · Definition · Demarcation

✉ S. H. Jore
sissel.h.jore@uis.no

[1] University of Stavanger, Postboks, 8600, FORUS, 4036 Stavanger, Norway

1 Introduction

During the last couple of years, European countries have witnessed an increase in terrorist attacks stemming from Islamic terrorism, and the prospect of similar attacks to occur in the future seems alarmingly likely (Hegghammer 2016). The threat of terrorism, espionage, cyber-attacks and organized crimes have become ubiquitous features of European societies, and consequently the demand for research on how to mitigate and protect society from intentional and malicious threats is stronger than ever. Consequently, security, meaning protection from intentional and malicious harm, is on the rise as a pressing research topic.

In safety and risk studies, security has become a hot topic. Several authors have recognized similarities between security and safety research (Brewer 1993; Courtois and Leveson 1996). Others have explored the proposition that security and safety are a duality, and that much could be gained by one domain adopting the knowledge, theories, and methodologies of the other (Aven 2007; Brewer 1993; Kriaa et al. 2015; Piè-Cambacédès and Bouissou 2013). Other scholars have argued that security has specific characteristics that need to be further explored. Along with this latter argument, several scholars have claimed that security should be developed as an independent science, detached from safety science (Jore 2017; Smith and Brooks 2012).

This article aims to investigate the conceptual and scientific demarcation of security in contrast to safety. First, the meaning of security is investigated. Second, the similarities and differences between security and safety are outlined in the light of the demarcation between security and safety studies. The shortcomings of current definitions of security are examined before a new definition of security and security risk management is proposed. Finally, we discuss the status of the security field as an independent science. As such, this article is a conceptual article where the aim is to contribute to conceptual and theoretical development in the safety and security fields.

2 What is Security?

Although security has become an omnipresent aspect of modern societies, the concept of security in itself has drawn surprisingly little scholarly attention compared to similar concepts such as risk and safety. In everyday use, the word invokes the association of safety and the absence of threats, promising some measures of assurance and certainty of being free from harm (Jarvis and Holland 2014). Consequently, the concept of security implies the feeling of being safe and secure, the lack of threats, and the management of future risks. However, the concept of security does not only evoke such positive connotations as being safe and free from danger. Inherent in the concept is also the association of objects such as guns, security technologies and even wars—objects not necessarily contributing to making society and the world more secure. This is what Jarvis and Holland (2014) refer to as the paradoxical element of security.

Despite the importance of the concept of security as a central element in research programs, university courses, academic literature, and in practice, there exists no academic consensus definition of security, and there is an ongoing debate on whether such a consensus definition is achievable and desirable. Manunta (1999) has argued that the goal is to achieve a shared conceptual meaning of security. By contrast, other scholars have claimed that security, like most concepts, does not have an agreed meaning because the concept is context-depended; its meaning changes in accordance with changes in perceptions and discourses of threat and dangers.

The concept of security was originally used in philosophy as referring to the security of the individual human. After the Second World War, the definition changed to designate the survival of the nation-state often referred to in the bipolar logic of the Cold War. However, the political security landscape after the end of the Cold War with focus on peace, human rights, and the robustness of society itself, allowed for an extension and broadening of the security concept. During this period, new conceptualizations of security emerged such as societal security, human security, international security, and homeland security (Baldwin 1997; Rothschild 1995). The present meaning of security has become broader and covers more sectors in society than previously (Brooks 2010). Currently, security is perceived as a shared responsibility covering different levels and sectors in society (Aly 2013; Jore 2012). This is in stark contrast to a few decades ago, when security was predominantly perceived as the responsibility of the police and army. Along with the broadening of the meaning of security, in addition to more focus on society itself as an object of security, security is no longer exclusively connected to the nation-state. Given the diverse meanings of security, it is not obvious to whom and to what the concept of security refers. Today, security is associated with many levels and dimensions. Several scholars have demonstrated that security takes numerous forms and have tried to outline its dimensions; (Collins 2016; Smith and Brooks 2012; Zedner 2009) (Table 1).

Table 1 The dimensions of security (based on Collins 2016; Smith and Brooks 2012 and Zedner 2009)

Level	Associated security concept	Key features of security
Individual	Human security	The individual, human rights
Objects, buildings and public spaces	Object security, onsite security	Asset protection, protection of public places
Organization	Organizational security, private security	Security risk management, security culture
Critical infrastructure	Critical infrastructure security	System vulnerability, cascading effects
Society	Societal security, public security, homeland security	Ability to prepare for and deal with crisis, feeling of safety and trust
State	National security	Protection of borders, survival of the state
International	International security	International organizations‘ efforts to achieve stability and peace

As the table illustrates, security is multi-dimensional in nature and diverse in practice. When scholars in risk and safety science point to "security" as a scientific field, they most often refer to the levels of objects, buildings and public spaces, organizations, critical infrastructure, and society. When other levels are referred to, they often mean compound concepts such as human security or national security. However, security studies are also a sub-discipline within other disciplines. Within criminology, crime prevention has been a central research topic for many years and within international relations the focus has shifted from national security related issues to more focus on risk management, human security, and societal security (Jarvis and Holland 2014; Petersen 2012; Zedner 2009). This multidimensionality of security means that it is impossible to agree upon a consensus definition to apply to all levels and dimensions of security. Consequently, the definition of security will depend on the historical and political context of the utilization of the concept of security.

3 The Demarcation of Safety vs Security

Numerous assumptions exist about the nature and relation between the concepts of security and safety in ordinary language and in academia. Boholm et al. (2015) compared the use and meaning of security and safety and found that the terms frequently have similar meanings, and are thus often treated as synonyms. However, regardless of the common features of security and safety, the concepts also have separate meanings and applications, and most of their specific connotations are not shared. Furthermore, security and safety are connected with different protective means (safety with instruments and security with actors) and sectors: safety is linked with traffic and transportation, workplace conditions, food quality, and regulation, while security is associated with international relations, information technology, and the economy. The multiple meanings of the terms make them difficult to define in an integrated and simple way, and academic definitions often focus on one of several aspects of the terms.

Several scholars have proposed that it is meaningful to distinguish between security and safety to separate the fields of risk and crisis management. According to these scholars, protection from terrorism and other intentional crimes is denoted as security, while safety implies protection from unintentional acts (Boholm 2012, 2016; Boholm et al. 2015; Jore and Egeli 2015; Piè-Cambacédès and Chaudet 2010; Reniers and Audenaert 2014; Reniers et al. 2011). These scholars claim that the difference between security and safety lies in whether the incident is inflicted intentionally or not; safety risks are characterized by being accidental e.g., industrial accidents and security is intentional or deliberate, as with terrorism or deliberate sabotage (George 2008; Johnson 2008; Randall 2008; Reniers and Audenaert 2014). Security and safety are thus different in the nature of the incidents. This differentiation between security and safety is meaningful to many scholars and practitioners and is often used to describe two different approaches to handling risks. Multiple authors describe this demarcation of intentionality (Reniers and Amyotte 2012):

Safety

- Protection against human and technical failure (Holtrop and Kretz 2008).
- Harm to people caused by arbitrary or non-intentional events (Hessami 2004).
- Natural disasters, human error or system, or process errors (Elias et al. 2008).

Security

- Protection against deliberate acts of people (Holtrop and Kretz 2008).
- Loss caused by intentional acts of people (Hessami 2004).
- Intentional human action errors (Elias et al. 2008).

The same distinction of intentionality is also found in the SRA glossary (2015) and in the SEMA referential framework (Piè-Cambacédès and Chaudet 2010).

All these definitions focus on defining security and safety in terms of intentionality. At a superficial level, these definitions can be beneficial for distinguishing the fields from each other. However, these definitions do not serve as a means of defining the scope of security research. To define a research scope exclusively from antagonism to another research field is not sufficient to describe what security science should contain. Furthermore, is intentionality really a good indicator for how the fields should be distinguished from each other?

4 The Demarcation Between Security and Safety is not Exclusively on Intentionality

The difference in intentionality between security and safety is not necessarily as rigid as the definitions suggest. These definitions are based on a presumption that intentionality does not play a role in safety research, and this is not necessarily the case.

The leading theories in safety science are built on the notion that accidents do not "just happen". The underlying idea of this research is that accidents can be prevented by doing risk analysis, building a safety culture, or organizational resilience. In other words, to describe safety as pertaining only to "arbitrary or non-intentional events" is not in line with the current theoretical perspectives in safety research. The literature on organizational safety has for several decades acknowledged that accidents are neither arbitrary nor random, but rather a result of lack of focus of safety planning. According to these theories, human intent can play a role in causing accidents, and organizations should subsequently design robust measures that can cover what used to be referred to as ""human error" (Perrow 2011a, b; Reason 1990, 1997; Weick and Sutcliffe 2011; Woods et al. 2012).

Several of these theories are based on the presupposition that accidents often are caused by deliberate and intentional individual actions. Reason (1997), for example, claims that organizational accidents often depend upon two kinds of failure: the failure of actions to go as intended and the failure of intended actions to achieve their desired consequences. Additionally, he adds a category of intentional actions named violations; these are situations in which humans intend not to follow safety

procedures. Reason distinguishes between three types of violations. First, exceptional violations are singular violations occurring in a particular set of circumstances. Second, routine violations are often habitual, forming an established part of an individual's behavioral repertoire: humans, for example, take shortcuts because most safety procedures involve some kind of burden for the worker. Third, reckless violations are when an individual deliberately breaks a safety procedure, but the intent to harm others is not present. This could, for example, be not wearing a helmet or safety jacket. Reason states that other categories of violation, such as sabotage, also exist. This means that in contrast to what the definitions of security and safety suggest, human intent plays a role in both security and safety (Lilleby and Egeli 2014). In both security and safety a violator could be present, but in the case of security the violator has a malicious intent and deliberately aims to cause harm. Accordingly, it is not sufficient to claim that safety is unintentional and that security is intentional; it is the malicious intent that separates safety from security. As a result, the demarcation between security and safety should be drawn in terms of the dichotomy of non-malicious versus malicious intent, not between intentional and unintentional.

Figure 1 illustrates the demarcation between security and safety. Sabotage and terrorism will be examples of security incidents, whereas other violations with no malicious intent to harm others will be examples of safety incidents. While some safety incidents also could be considered crimes, all security incidents fall under the classification of criminal activity.

Another question related to the content of the scientific field of security is what constitutes a security threat. The concept of threat has multiple meanings, but threats can be described as a perceived possibility of harm or a possible perpetrator's intention to cause harm (Meloy and Hoffmann 2013). Central in the definition of threats are a possible perpetrator's intent. Intent lies in the motivation or desire to cause harm and expected outcomes. A threat also depends on a perpetrator's capabilities in terms of resources and knowledge (Smith and Brooks 2012). The demarcation of malicious versus non-malicious intent of the violator helps to outline the range of perpetrators that fall under the category of security. From this division between security and safety, perpetrators with malicious intent of causing harm such as a hacker or a terrorist will be a security threat, while a worker abusing drugs or violate a safety procedure, and thus is engaged in a criminal activity that can cause a major accident will be a safety threat. Consequently, the field of security covers various types of criminal activities: *opportunistic crimes*

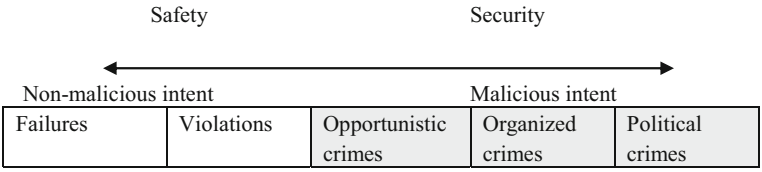

Fig. 1 Demarcation between security and safety (based on Lilleby and Egeli 2014 and Jore 2017)

e.g., thieves, *organized crimes* e.g., sabotage, kidnapping, espionage or an insider leaking sensitive information and *political crimes* such as terrorist attacks.

From this perspective, possible security threats will cover several criminal activities, for example:

- Theft
- Vandalism
- Organized crimes
- Sabotage
- Kidnapping
- Hackers
- Terrorism
- Espionage
- Security political crises

What these threats have in common is that they are all forms of criminal activity. These perpetrators can range from individuals operating alone, such as lone-wolf terrorists or individual hackers, to organized groups, such as kidnappers and terrorists, to those operating on a state level (e.g., information warfare or espionage). This implies that although the concept of security is often applied in reference to terrorism and other major crimes, the concept also covers more ""ordinary crimes" such as theft and vandalism. Accordingly, threats to security constitutes a wide range of perpetrators stemming from multiple sources and levels.

5 How is Security Different from Safety?

In the current threat landscape, there is an expectation that organizations and authorities have a responsibility for security and safety. However, from a mitigation perspective, these risks are fundamentally different in nature.

Safety risks are associated with an organization's production and profit. Productions of goods and services are always connected with some kind of risk, and these are risks the organization is willing to take to produce its desired outcome and to gain profit. The sources of these risks are generally well-known, and the organization can use reliable historical data in the risk management process. Since organizations have knowledge concerning the risks, they usually also know how these risks can be mitigated. The decisions on whether to implement risk-reducing measures are often a result of quantitative probability assessments and cost-benefits assessments. In aviation, for example, safety risks are most often known and connected to the regular characteristics of the system (e.g., engine failure, fatigue and misunderstandings) and are possible to localize due to continuous experimental- and experience-based learning within civil aviation (Pettersen and Bjørnskau 2015)

Conversely, security involves the threats to which organizations are exposed. Security risks are not necessarily directly linked to the production of an organization, and are, therefore, less controllable from an organizational perspective (Petersen 2014). Since security threats are not directly linked to the production of an

organization, organizations do not have the same knowledge regarding possible risk scenarios for security risks as for safety risks. Although all risk assessments are characterized with uncertainties regarding possible scenarios, those related to who, what, how and when an attack might occur are much greater for security risks than for safety risks.

Quantitative methods are historically more widely used in the field of safety than in security, since security threats are by nature more difficult to characterize in quantitative terms. Qualitative methods combined with expert opinions are often preferred for describing and assessing security risks (Aven and Renn 2009; Piè-Cambacédès and Bouissou 2013). The widespread use of qualitative approaches within the security field is also related to the low frequency of most security events, which means there is a lack of relevant historical data on which to build risk assessments. This, however, is not necessarily the case for all security-related risks faced by organizations since the scope of security covers a wide spectrum of activities, from vandalism to terrorism or political security crises. For many security-related risks such as more "ordinary crimes", historical data exist that could be relevant to organizational security risk management.

Since the nature of the threat often is rooted outside the organization, most organizations do not have the means to fully understand and reduce the threat. Most organizations will lack the understanding and the resources to fully undertake threat assessments, and they have to rely on the intelligence services which in most countries publish more general threat assessments than on the individual organizational level. Moreover, organizations will in many cases also lack the means to reduce security threats since it is the state that has the mandate to discover and arrest thieves, terrorists, hackers or other possible perpetrators. This means that when an organization aims to mitigate against a security threat, it will actually have to take into account that these perpetrators are able to search deliberate for the best way to execute their plans, aiming to cause as much damage as possible. For example, an insider will know how to cause as much damage as possible and could deliberately plan for the worst thinking cascading effects. Consequently, certain scenarios that would be labelled as extremely unlikely in the case of safety might actually be relevant in the case of security (Reniers and Audenaert 2014).

Additional, some security risks such as terrorism have a symbolic and political dimension. This implies that although an organization might be the scene of an attack, the goal of the perpetrator is not necessarily to harm the company's production but to draw attention to a political cause or gain ransom. The symbolic aspects of security risks such as terrorism also influence which counterterrorism measures are seen as relevant and which assets should be protected. While flight safety is organized to deal with experiences and fears related to technical reliability, human performance, and the organizational robustness of the aviation sector, aviation security is contingent upon being organized to protect against malicious perpetrators as well as the public's fear of their existence (Pettersen and Bjørnskau 2015). This makes the goals and the institutional logics of protection between security and safety very different. The demand for security measures is more often related to public discourses on what might be legitimate terrorist targets than the actual risk-reducing effect of such measures (Jore 2012; Pache and Santos 2010).

Some security events such as terrorism are dramatic and cause major public fear and debates concerning appropriate risk-reducing measures, while other security risks are risks that organizations strive to protect themselves from almost every day, such as hackers or insiders. The risk of hackers, insiders leaking information or espionage are less visible both prior to and after an incident. Since the perpetrators are strategic, they have no interest in revealing their plot before an attack, which means that, unlike many safety risks, early warning signals will not be as easy to detect. Even during or after an attack or crisis, the incident may not in some instances be visible to the organization. If the perpetrator is a spy or a hacker, a successful attack could imply that the organization will not be aware that it has been the target of an attack. This means that while safety rules exist to protect the individual worker or others from avoiding harm, security follows another logic: Perpetrators who fall under the category of security actually have something to gain from breaking the rules. The combination of the perpetrators' gain and often lack of signals to warn about an upcoming incident make security risks difficult to detect. Consequently, mitigation of security risks often implies "to see what nobody else sees", and that static security measures and rules are not sufficient for building a robust security regime. Thus, an organization aiming for achieving security should also focus on perception of threats and security awareness rather than probability assessments. Subsequently, striving for resilience is a more promising trajectory for building organizational security. A resilience approach to security focuses on how a system can adapt, handle and recover from changing conditions and various threats instead of exclusively focusing on estimation of plausible scenarios, probabilities and target hardening (Linkov et al. 2016) (Table 2).

6 Are the Differences Between Security and Safety Addressed in the Academic Field?

The differences between security and safety are reflected by differences in the tools, standards, and risk management in the two domains (Jore and Egeli 2015). In many respects, assessing a security threat is different from assessing a safety risk. In

Table 2 Non-exhaustive list of differences between security and safety (based on Jore 2017)

The nature of the risk	Safety Risk related to production and profit, often well-known risks	Security Strategic humans, dynamic threat, often rooted in causes outside the organization
Type of intent	Non-malicious intent	Intentional, malicious
Historical data	Historical data often exist that are applicable for prediction of future trends	Data sources problematic, historic trends not always good predictors of the future
Types of risk assessment	Quantitative probabilities and frequencies of safety-related risks are often utilized	Qualitative (expert-opinion based) likelihood of security-related risks
Possibility for mitigation	Organization has knowledge about possible risk scenarios and measures	Threats and measures may be symbolic, organizations often lack means

security, the sources of the threats to be assessed are usually not well-known to the analyst and cover an extremely broad range of possible scenarios. In safety, the characteristics of the hazards are more accessible and the number of scenarios to be considered may also be restricted, but the hazard is still regarded as significant (Kriaa et al. 2015). Although there are several international and national standards, guidelines and recommendations in textbooks and the scientific literature on how to conduct security risk assessment a literature review concluded that there does not exist a consensus on what is the best practice of conduction security risk analysis and different security risk concepts and management tools vary across countries and sectors (Maal et al. 2017). Furthermore, in safety science there are currently ongoing debates in both academia and in the practical community about whether there is a need for a specific risk concept for security that can capture the special features of security risk, or whether perspectives dominating the safety field are adaptable to the security field (Amundrud et al. 2017; Jore and Egeli 2015).

There are several academics and practitioners who claim that security and safety are distinct issues and should not be merged. However, the two disciplines are also closely related and share many commonalties; and the tools from one domain have often been adapted to the other (Piè-Cambacédès and Bouissou 2013). However, the theoretical statuses of the two fields are very different. While risk management, resilience and culture-building have been important elements in safety research for several decades, only in recent times have security scholars focused on these topics.

The literature dealing with safety perspectives is extensive and is part of a long research tradition. Several leading perspectives exist, but some of the most widely referenced theories in the field are Normal Accident Theory, the Theory of High Reliability Organizations, and Resilience Engineering (Hopkins 2014). All these theories were originally developed within the safety field, and although some scholars utilized these theoretical perspectives in the security field (Auerswald et al. 2006; Perrow 2011a; Pettersen and Bjørnskau 2015: Thoma et al. 2016), there is a paucity of literature that actually discusses whether these theoretical perspectives are transferable. Hardly any studies exist that test the effectiveness of these theories in a security context or that apply them to a security case for the purpose of theory testing or development. Hence, it has not been clearly established whether these theories and their concepts can be transferred to a security context.

Most of the literature within the field of security either borrows perspectives from safety science that utilizes normative theories describing how to achieve security without building on research or studies that have tested these theories. There are multiple causes for this; first, security historically has not been an area of organizational responsibility. Second, organizations that have a tradition for dealing with security risks have been mainly the military and the police—organizations that have a tradition for classification and, in general, have not been open to research or critical perspectives. Third, while safety science has been a broad research field covering multiple disciplines and levels, this has not until recently been the case for the security field, which has been mainly a subject in criminology or international relations, and these disciplines have thus focused more on the state perspective than the organizational perspective. However, security science also borrows theories, concepts and perspectives from the discipline of criminology. These perspectives

take into account crime prevention and the strategic rational actors behind the threats. However, given that the scope of security nowadays covers cooperate security and an increased amount of sectors in society than previously, these perspectives are not necessarily adjusted to fit the organizational security perspectives (Pease and Farrell 2014).

7 Similarities Between Security and Safety

Although there are several differences between security and safety, the two fields share many characteristics. In both fields, the concept of risk is now used extensively in assessing and managing threats. Although there are debates as to whether security risk management should adopt a different methodology than in safety risk management (Jore and Egeli 2015), risk analysis methodology in both fields is often based on similar phases involving analyzing threats, vulnerabilities, potential consequences, the likelihood of occurrence, and ranking risks (Piè-Cambacédès and Bouissou 2013; Young and Leveson 2014).

Theoretical perspectives and risk analysis methodology developed within the area of safety are also used within the area of security (Kriaa et al. 2015). Although it has been much more common to transfer safety perspectives to security than vice versa, there are also tools and perspectives developed within the field of security that have been transferred to safety such as the defense-in-depth approach, initially deployed in military circles and then in nuclear safety (Piè-Cambacédès and Bouissou 2013). Several recent articles address risk analysis from a cross-fertilization perspective, looking at similarities, differences, and interdependencies between the risk concept and the risk analysis methodology employed in security and safety risk management. This means that despite the differences between security and safety, some authors claim that the perspectives developed in each field can be applicable to the other (Amundrud et al. 2017; Kriaa et al. 2015; Piè-Cambacédès and Bouissou 2013).

All major organizational accidents in both security and safety contexts involve technical, organizational, and operational (human) elements. This means that both within the areas of security and safety, humans play an important role in detection, mitigation, and emergency management. Despite the differences in the nature of the threats in security and safety, the consequences can often be similar (e.g., as in a fire). Consequently, for many emergencies the same security measures can reduce both security and safety threats (e.g., a fire extinguisher), although this is not always the case. Some measures have different effects on security and safety. For example, labeling chemical substances is a beneficial security measure, but can become a threat in itself in the hands of a security perpetrator (Reniers et al. 2011). This means that from an organizational perspective, it is necessary to see security and safety in relation to each other, so that security measures do not threaten safety or vice versa.

8 The Need for a New Definition of Security

As described so far in this article, security has developed as a discipline overlapping with, but independent, from safety. Given the special characteristics of security, in addition to a lack of theoretical perspectives, there is a need to define the scope of security research. Differences between security and safety extend beyond only the intentional aspect of the fields. All the definitions of security mentioned so far in this article have exclusively defined security in contrast to safety—meaning that none of those definitions focus on what security is, only what it is not. Consequently, none of the definitions explicitly attempt to establish what security is. For a body of knowledge aspiring to become an independent science, a definition entirely based on how security differs from safety is insufficient. There is a need to define the content of security in itself, and although the concept of security is a diverse and multidimensional concept in the academic field, those in favor of a security science claim that it is possible to define security as long as it is considered from a contextual perspective (Smith and Brooks 2012). This means that it is possible to propose a definition of security that covers the current comprehension of security.

Definitions of security exists that focus on other aspects than exclusively defining security in contrast to safety. These definitions focus more on the content of what security is, examining certain aspects of what is included in the general current notion of security. Security is now understood as both a state and a process, which often can reduce risk and protect or build resilience against possible threat scenarios. In Presidential Policy Directive 21 (PPD-21), for example, security is understood as something created actively to reduce risk. Security is defined as "*Reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters*" (Department of Homeland Security, 2016).

This definition proposes that security is a risk-reducing process conducted by means of physical protection. The academic literature that deals with how organizations can create security often builds on perspectives from safety science, and this literature incorporates risk management and resilience as important factors in the responsibilities of organizations and authorities responsible for security (Smith and Brooks 2012; Sheffi 2005; Talbot and Jakeman 2011). This implies that security is something done actively in all phases of a crisis, and accordingly, security also means to prepare for, adapt to, withstand, and recover from dangers and crises. Security risk management includes assessing and reducing the likelihood and consequences of possible attacks by applying various types of risk-reducing measures. Such measures include critical infrastructure protection and building organizational and societal resilience (Brooks and Corkill 2014; Talbot and Jakeman 2011). The Department of Homeland Security (2016) delineates what constitutes security by giving a list of measures for how to create security:

- Badge entry to doors
- Use antivirus software
- Erect fencing around buildings
- Lock computer screens

All these measures serve as some form of physical protection. What these measures have in common is that they are static, and do not take into account the strategic and calculated nature of security threats when the perpetrator can adjust plans to avoid security measures. The current literature describes security measures as much more than physical protection or target hardening (Reniers et al. 2011; Talbot and Jakeman 2011) defining security as a myriad of possible measures ranging from security awareness programs and building a security culture to surveillance and screening employees. This means recent perspectives on security also include multiple types of measures such as building security risk management, resilience, security awareness, and a security-oriented culture.

Given the weaknesses in the current definitions of security, Jore (2017) has proposed a new definition that also incorporates security as a measure to build resilience to malicious attacks. We will further develop this definition so that it also incorporates that security is a perceived state related to fear and dangers:

> Security can be defined as the perceived or actual ability to prepare for, adapt to, withstand, and recover from dangers and crises caused by people's deliberate, intentional, malicious acts, such as terrorism, sabotage, organized crime, or hacking.
> Security risk management includes assessing and reducing the likelihood and consequences of possible attacks by applying various types of risk-reducing measures. For example, by establishing critical infrastructure protection and by building organizational and societal resilience.

Given the proposed definition of security, which in many respects overlaps with the current definition of risk management and resilience perspectives, should security be considered a science in itself, or as a sub-discipline of safety science?

9 Is Security an Independent Science?

Numerous terrorist attacks worldwide, organized crime, espionage and cyber threats to interconnected facets of infrastructure have become challenges that states and organizations are facing. A subsequent focus on protection from such threats have led to a demand for better protective measures. The corollary of this focus of attention can be seen in new security regulations and new security risk-management standards that point out different actors' responsibility to conduct security risk assessments and implement appropriate measures. This massive attention on security has led to the request for security knowledge from multiple actors in society. Security has become a topic of many university courses, textbooks, academic journals, and research programs. However, regardless of the many scholars interested in the topic, few of them would probably call themselves security scholars. This is not because there are no excellent researchers interested in the topic, but because most of them write within their own disciplines and publish in journals other than the few exclusively concerned with security. Within universities, the same tendencies are present; several universities offer courses in security and

related topics, but there are still limited study programs that aim to teach students the main topic of security (Smith and Brooks 2012).

Although security science is not yet established as an independent science, researchers, educators, industries, and governments have for many years worked on defining the body of knowledge upon which security science should be based (ASIS International 2017; Brooks 2010; Smith and Brooks 2012; Hesse and Smith 2001; Kooi and Hinduja 2008; Smith 2001). Although security is an important topic across many disciplines, the status of the security field has not reached a level where it can be defined as a science from a traditional paradigm perspective; there does not exist a clear definition and scope of its body of knowledge, or leading theoretical perspectives and agreed-upon concepts and models concerning security. Security science is diverse, multi-dimensional, and cross-disciplinary, without a defined specified knowledge base or skill structure (Brooks 2010). Nevertheless, security can be defined within its given context, and so can also the science of security. In fact, textbooks in "security science" claim that although "security science" currently cannot be regarded as an academic discipline, security is an emerging science on its way to developing into an independent science, as security is an in-demand field of research and application (Smith and Brooks 2012).

When comparing security science to safety science it is important to bear in mind that the same criticism that has been made of security as a science can also be made of safety as a science. Although safety science has a longer history, with many more researchers and practitioners dedicated to the field, scientific diversity is a complicated issue for safety science as well. Among the many different scientific communities interested in the topic of safety, there seems to be little central coordination of what is a very heterogeneous intellectual production. The hegemony of an encompassing paradigm of safety science would be unlikely to cover the multifaceted nature of the topic (Le Coze et al. 2014).

This heterogeneity is also necessary for understanding a phenomenon as complex and multidimensional as security, which should not be understood from only one perspective or theoretical approach. Such a phenomenon should, therefore, embrace multidisciplinary research. The object of security can be researched from a positivist as well as constructivist approach, and the study of security should thus include the objective, subjective, and symbolic nature of security across multiple dimensions and levels of society (Manunta 1999; Smith and Brooks 2012). This research should also include risk perception and the paradoxical elements of security.

The heterogeneity of security threats also needs to be explored. It is not obvious that the same risk management methodologies and theoretical perspectives are applicable to different security threats such as terrorism, espionage, the insider threat and hacking. These threats are different in nature, and this diversity mandates a variety of theoretical perspectives.

The scholars arguing for an independent security science advocate an interdisciplinary approach covering different dimensions and aspects of security. They claim that to understand a complex phenomenon such as security, building blocks from other sciences should be critically examined. It is in the intersection of other disciplines that security science diverges from safety science. Criminology and international relations will be natural crossing points for the study of security, which

is not necessarily the case for safety science. After all, the study of security deals with how to mitigate and protect society from criminal acts, so theoretical perspectives from safety science will not be sufficient for a holistic security management. However, this does not mean that there are no interesting theoretical perspectives that can be transferred from safety to the security field, but it is important that such theories are not just uncritically imported or transferred. Security science needs to be acknowledged for its own characteristic and challengers. Cross-fertilizations between security and other disciplines are thus crucial, but given the immature status of security sciences today, the science of security should be developed as a distinct discipline recognized for its distinct characteristics.

10 Conclusions

This article has discussed the conceptual and scientific demarcation of security in contrast to safety. Security is a multifaceted concept whose meaning has changed in accordance with discourses of threats and dangers. Scholars in risk and safety science have proposed that it is meaningful to distinguish between security and safety in terms of intentionality to separate the fields of handling risks and crises. However, since intentionality also plays a part in safety research, this is not a good parameter for separating the fields. The demarcation between security and safety should be based on the malicious intent of the perpetrator, since this indicator aims to highlight the specific characteristics of the field of security, in addition to specifying possible threats to security. Given the shortcomings of the current definitions, we have proposed a new definition of security that incorporates elements associated with security as a research field today:

> Security can be defined as the perceived or actual ability to prepare for, adapt to, withstand, and recover from dangers and crises caused by people's deliberate, intentional, and malicious acts such as terrorism, sabotage, organized crime, or hacking.
> Security risk management includes assessing and reducing the likelihood and consequences of possible attacks with various types of risk-reducing measures, for example, through critical infrastructure protection and by building organizational and societal resilience.

Although they are distinct scientific fields, safety and security share many commonalities, and there is a practical need for an integrated approach between security and safety that cannot be overlooked. In practical security risk management, the same perspectives and risk analysis methodologies seem to be shared across the security and safety fields. Additionally, research funders such as the European Union are requesting multi-hazard management and science. Nevertheless, there are certain characteristics of the security field that are different from the safety field and need to be further explored. Furthermore, the theoretical perspectives and risk analysis tools available to organizations are not based on

the same research traditions in the two disciplines. Security and safety have developed as two distinct disciplines for many years, led by partitioned communities developing their own tools and methodologies, but there are also many theories and perspectives both disciplines share. At the moment, the best trajectory might be to continue to look for cross-fertilization between security and safety and to further develop both disciplines. Extending the development of both fields might eventually lead to a more integrated approach in the future.

However, the distinct characteristics of security currently are not fully addressed in the theories and methodologies available, and there is a need for critical examination of theories and risk-analysis tools that are transferred from one discipline to the other. The field of security is characterized by attributes that have not been fully researched and that need to be examined in more detail. The current body of knowledge in the security field is to a large extent very fragmented and segmented. With only a few exceptions, few attempts have been made to describe the foundation of security science. To establish security as an independent discipline, it is necessary to determine what concepts and theories are related to the field. What levels of and objects in society should such a field include, and what are the interrelationships and interdependencies with other disciplines? Ultimately, a structure of security knowledge may be formed that supports security as an independent science.

References

Aly A (2013) The policy response to home-grown terrorism: reconceptualising prevent and resilience as collective resistance. J Polic Intell Count Terror 8(1):2–18

Amundrud Ø, Aven T, Flage R (2017) How the definition of security risk can be made compatible with safety definitions. Proc Inst Mech Eng Part O 231(3):286–294

ASIS International 2017: https://www.asisonline.org/search/pages/All-Search-Results.aspx?k=security%20science

Auerswald PE, Branscomb LM, La Porte TM, Michel-Kerjan EO (2006) Seeds of disaster, roots of response: how private action can reduce public vulnerability. Cambridge University Press, Cambridge

Aven T (2007) A unified framework for risk and vulnerability analysis covering both safety and security. Reliab Eng Syst Saf 92(6):745–754

Aven T, Renn O (2009) The role of quantitative risk assessments for characterizing risk and uncertainty and delineating appropriate risk management options, with special emphasis on terrorism risk. Risk Anal 29(4):587–600

Baldwin DA (1997) The concept of security. Rev Int Stud 23(01):5–26

Boholm M (2012) The semantic distinction between "risk" and "danger": a linguistic analysis. Risk Anal 32(2):281–293

Boholm M (2016) Risk, language and discourse. Doctoral dissertation, KTH Royal Institute of Technology

Boholm M, Möller N, Hansson SO (2015) The concepts of risk, safety, and security: applications in everyday language. Risk Anal 36:320–338

Brewer DF (1993) Applying security techniques to achieving safety. In: Redmill F, Anderson T (eds) Directions in safety-critical systems. Springer, London, pp 246–256
Brooks DJ (2010) What is security: definition through knowledge categorization. Secur J 23(3):225–239
Brooks DJ, Corkill J (2014) Corporate security and the stratum of security management. In: Walby K, Lippert RK (eds) Corporate security in the 21st century. Springer, London, pp 216–234
Collins A (2016) Contemporary security studies. Oxford University Press, Oxford
Courtois P-J, Leveson NG (1996) Safeware: system safety and computers. JSTOR 84:612–614
Department of Homeland Security, (2016), https://www.dhs.gov/what-security-and-resilience)
Elias I, van Gullik A, Muyselaar A, van Veen J (2008) Crisis in de vitale infrastructuur. Rapport Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Nederland
George R (2008) Critical infrastructure protection. Int J Crit Infrastruct Prot 1:4–5
Hegghammer T (2016) The future of jihadism in Europe: a pessimistic view. Perspectives on Terrorism 10(6). Available at http://www.terrorismanalysts.com/pt/index.php/pot/article/view/566. Accessed 21 Dec 2016
Hessami A (2004) A systems framework for safety and security: the holistic paradigm. Syst Eng 7(2):99–112
Hesse L, Smith CL (2001) Core curriculum in security science. In: H. Armstrong (ed) Proceedings of the 5th Australian Security Research Symposium. Perth, Western Australia: School of Computing and Information Science, Edith Cowan University, pp 87–104
Holtrop D, Kretz D (2008) Research Security and Safety: An Inventory of Policy, Legislation and Regulations. Research Report 141223/EA8/043/000603/sfo. Arcadis, The Netherlands (in Dutch)
Hopkins A (2014) Issues in safety science. Saf Sci 67:6–14
Jarvis L, Holland J (2014) Security: a critical introduction. Palgrave Macmillan, Basingstoke
Johnson CW (2008) Using evacuation simulations for contingency planning to enhance the security and safety of the 2012 Olympic venues. Saf Sci 46(2):302–322. doi:10.1016/j.ssci.2007.05.008
Jore SH (2012) Counterterrorism as Risk Management Strategies. PhD thesis no 178, Faculty of Science and Technology, University of Stavanger, Norway
Jore SH (2017) Safety and security—Is there a need for an integrated approach? In: Walls L, Revie M, Bedford T (eds) Risk, reliability and safety: innovation theory and practice. Taylor and Francis Group, CRC Press, London, pp 852–859
Jore SH, Egeli A (2015) Risk management methodology for protecting against malicious acts? Are probabilities adequate means for describing terrorism and other security risks? In: Podofillini L, Sudret B, Stojadinovic B, Zio E, Kröger W (eds) Safety and reliability of complex engineered systems. CRC Press, London, pp 807–815
Kooi B, Hinduja S (2008) Teaching security courses experientially. J Crim Justice Educ 19(2):290–307
Kriaa S, Pietre-Cambacedes L, Bouissou M, Halgand Y (2015) A survey of approaches combining safety and security for industrial control systems. Reliab Eng Syst Saf 139:156–178
Le Coze JC, Pettersen K, Reiman T (2014) The foundations of safety science. Saf Sci 67:1–5
Lilleby J, Egeli A (2014) Achieving common ground for safety and security risk analyses using Human Reliability Assessment. Bridging the gap between safety and security risk analysis using Human Factors. NEON-conference Stavanger, Norway
Linkov I, Trump BD, Fox-Lent C (2016) Resilience: Approaches to Risk Analysis and Governance, In: An edited collection of authored pieces comparing, contrasting, and integrating risk and resilience with an emphasis on ways to measure resilience, p. 6/Available at: > .file:///C:/Users/ibslab/AppData/Local/Microsoft/Windows/Temporary%20Internet%20Files/Content.IE5/KEN67U7S/Resilience%20Book.pdf
Maal M, Busmundrud O, Endregard M (2017) Methodology for security risk assessments–Is there a best practice? In: Walls L, Revie M, Bedford T (eds) Risk, reliability and safety: innovation theory and practice. Taylor and Francis Group, London, pp 860–866
Manunta G (1999) What is security? Secur J 12(3):57–66
Meloy JR, Hoffmann J (2013) International handbook of threat assessment. Oxford University Press, Oxford
Pache AC, Santos F (2010) When worlds collide: the internal dynamics of organizational responses to conflicting institutional demands. Acad Manag Rev 35(3):455–476
Pease K, Farrell G (2014) What have criminologists done for us lately? In: Gill M (ed) The handbook of security. Palgrave Macmillan, Basingstoke, pp 65–88
Perrow C (2011a) The next catastrophe: reducing our vulnerabilities to natural, industrial, and terrorist disasters. Princeton University Press, Princeton

Perrow C (2011b) Normal accidents: Living with high-risk technologies. Princeton University Press, Princeton
Petersen KL (2012) Risk analysis—A field within security studies? Eur J Int Relat 18(4):693–717
Petersen KL (2014) The politics of corporate security and the translation of national security. In: Walby K, Lippert RK (eds) Corporate Security in the 21st Century. Palgrave Macmillan, Basingstoke, pp 78–94
Pettersen KA, Bjørnskau T (2015) Organizational contradictions between safety and security—perceived challenges and ways of integrating critical infrastructure protection in civil aviation. Saf Sci 71:167–177
Piè-Cambacédès L, Bouissou M (2013) Cross-fertilization between safety and security engineering. Reliab Eng Syst Saf 110:110–126
Piè-Cambacédès L, Chaudet C (2010) The SEMA referential framework: avoiding ambiguities in the terms "security" nd "safety". Int J Crit Infrastruct Prot 3(2):556–6
Randall A (2008) 21st century security and CPTED. CRS Press, Boca Raton, Florida. http://www.crcpress.com
Reason J (1990) Human error. Cambridge University Press, Cambridge
Reason JT, Reason JT (1997) Managing the risks of organizational accidents. Ashgate, Aldershot
Reniers G, Amyotte P (2012) Prevention in the chemical and process industries: future directions. J Loss Prev Process Ind 25(1):227–231
Reniers GL, Audenaert A (2014) Preparing for major terrorist attacks against chemical clusters: intelligently planning protection measures with domino effects. Process Saf Environ Prot 92(6):583–589
Reniers GL, Cremer K, Buytaert J (2011) Continuously and simultaneously optimizing an organization's safety and security culture and climate: the improvement diamond for excellence achievement and leadership in safety and security (IDEAL SandS) model. J Clean Prod 19(11):1239–1249
Rothschild E (1995) What is security? Daedalus 124:53–98
SRA Glossary (2015). Available from http://www.sra.org/sites/default/files/pdf/SRA-glossary-approved22june2015-x.pdf
Sheffi Y (2005) The resilient enterprise: overcoming vulnerability for competitive advantage. MIT Press Books, Cambridge
Smith CL (2001) Security science: an emerging applied science. J Sci Teachers Assoc West Aust 37(2):8–10
Smith C, Brooks DJ (2012) Security science: the theory and practice of security. Butterworth-Heinemann, Oxford
Talbot J, Jakeman M (2011) Security risk management body of knowledge, vol 69. Wiley, Hoboken
Thoma K, Scharte B, Hiller D, Leismann T (2016) Resilience engineering as part of security research: definitions, concepts and science approaches. Eur J Secur Res 1(1):3–19
Weick KE, Sutcliffe KM (2011) Managing the unexpected: resilient performance in an age of uncertainty, vol 8. Wiley, Hoboken
Woods DD, Leveson N, Hollnagel E (2012) Resilience engineering: concepts and precepts. Ashgate, Aldershot
Young W, Leveson NG (2014) An integrated approach to safety and security based on systems theory. Commun ACM 57(2):31–35
Zedner L (2009) Security: key ideas in criminology series. Routledge, London and New York