Forecasting Unknown-Unknowns by Boosting the Risk Radar within the Risk Intelligent Organisation

Abstract

This theoretical perspective paper interprets *(un)known-(un)known* risk quadrants as being formed from both abstract and concrete risk knowledge. It shows that these quadrants are useful for categorising risk forecasting challenges against the levels of abstract and concrete risk knowledge that are typically available, as well as for measuring perceived levels of abstract and concrete risk knowledge available for forecasting in psychometric research. Drawing on cybersecurity risk examples, a case is made for refocusing risk management forecasting efforts towards changing unknown-unknowns into known-knowns. We propose that this be achieved by developing the 'boosted risk radar' as organisational practice, where suitably 'risk intelligent' managers gather 'risk intelligence information', such that the 'risk intelligent organisation' can purposefully co-develop both abstract and concrete risk forecasting knowledge. We also illustrate what this can entail in simple practical terms within organisations.

Key words: risk intelligence, competitive intelligence, military intelligence, risk radar.

1. Introduction

The present paper develops a theory of mature organisational risk management that focuses on risk forecasting knowledge production, where the forecasting infrastructure converts 'unknown-unknown' to 'known-known' risk by being more proactive in exploring the organisational environment than is typically the case in the risk management function. In particular, the paper considers the organisational challenge of producing forecasting knowledge for risk within the organisation's social threat environment.

The authors advocate the development of organisational risk-forecasting infrastructure towards a greater fitness for engaging social threats. Thus, we propose, *firstly*, a novel theoretical approach to the production of forecasting knowledge, with a focus on the conversion of 'unknown-unknowns' into 'known-knowns' through 'known-unknowns' (where forecasting knowledge is more heavily laden with abstract theory), but sometimes instead passing through 'unknown-knowns' (where forecasting knowledge is more heavily laden with facts about risks). *Secondly*, as a more practical corollary, we propose the interrelated high-level guiding constructs of 'risk intelligence' and the 'boosted risk radar'. We also illustrate simple practical changes to risk-related organisational processes and activities which can help in implementing the improvements we propose. Hence, we conclude this preliminary section by outlining the risk management context.

Of particular relevance is the dominant contemporary risk management paradigm which treats enterprise-wide risk management (ERM) (Committee of Sponsoring Organisations of the Treadway Commission, 2017) and strategic agility-oriented resilience (British Standards Institution, 2014) as shaping how cutting-edge advances in risk management maturity are usually conceived. We engage with this paradigm as follows. The theories of ERM and resilience both demonstrate the need for 'corporate nervous systems' to negotiate the corporate risk environment, to use the ecological and biological-adaptive metaphor (Institute of Risk Management, 2011). This metaphor's various meanings have been studied widely from Morgan's (2006) organisation-as-brain and organisation-as-organism perspectives. Furthermore, the corporate nervous system's connective role in linking the corporate brain to the corporate risk environment permits its wide use as a convenient practitioner simplification for multiple overlapping 'open', 'organic' and 'cybernetic' systems theory perspectives within organisation theory (Scott, 2003).

We argue that, in today's increasingly fast-moving, technology-driven and contingent organisational risk environment, risk management needs to be concerned with building corporate nervous systems along which information can flow, not primarily to drive strategy and agility *per se*, but more pressingly to engage social threat. We recognise that a substantial body of literature on managing the unexpected through resilience, as illustrated by high reliability organisation practice (Weick & Sutcliffe, 2001; Weick & Putnam, 2006), is already deeply engaged with the broad challenge of facilitating early threat detection and rapid response. Nonetheless, we regard such literature as being not sufficiently concerned with proactive and targeted organisational efforts to investigate and interact with social threat sources. Take for example cyber-criminals, who use "bulletproof" hosting services provided offshore, in physically hardened facilities, or with geographically distributed nomad servers to evade law enforcement (Bradbury, 2014). Proactive approaches to engaging these social threat sources, which represent a significant departure from the preoccupation of resilience with defending against the unexpected, might include acting, either directly or through the use of hired consultants, security professionals, or even co-opted former cyber-criminals, to gather intelligence directly from the cyber-criminals or their hosting services.

In emphasising highly proactive knowledge-seeking as a foundation for risk forecasting, we conceive of knowledge accumulation as a socially-distributed accomplishment that is grounded in complex everyday organisational practice (Orlikowski, 2002), such that we can theorise increasing levels of particular knowledge accomplishments in terms of the competences that they produce for forecasting (especially complex) risks. Thus, we develop the metaphorical 'risk radar' concept, which we consider underused within its present theoretical positioning at the front end of the resilience process, through a novel focus on what it can mean to ‘boost’ its reach into the organisation’s social threat environment.

Our approach will also emphasise the insufficiency of compliance-driven and internal control focused risk management infrastructure, whose centrepiece is the traditional risk listing process and its attendant risk registers. We will argue that these practices too can benefit from ‘boosted risk radars’; indeed, we argue that the boosted risk radar’s interface with the risk identification stage of the organisation’s risk management process should be of interest to any organisation who is seeking risk management that is better integrated and more capable of urgent response.

Thus, the fundamental aim of this paper is to work within the theoretical template provided by the Rumsfeld’s knowledge categories to explore, both terminologically and in more practical terms, how organisations can dedicate forecasting effort to converting ‘unknown-unknowns’ into ‘known-knowns’. Two objectives are set in order to achieve this aim. Firstly, the paper sets out to develop key concepts for exploring how organisations may proactively detect and defend against particular social threats. Secondly, the paper sets out to explore the implications for the nature and scope of risk management practice, in particular seeking practical ways to co-develop abstract and concrete risk forecasting knowledge. However, before doing this, the next section provides a preliminary theoretical outline, clarifying the nature and limitations of forecasting for social threat. This outline introduces the idea that knowledge production for such threats can follow ‘known-unknown’ and ‘unknown-known’ epistemic pathways *en route* to the epistemic accomplishment of converting social threats to ‘known-known’ status. Our final theoretical preliminary will be to situate our organisational forecasting concerns within the organisational risk management practice contexts of enterprise risk management and resilience.

2. Nature and limitations of forecasting for social threat

We use the term 'social threat' to refer to threats which, for practical forecasting purposes, readily admit the simplified frame of some particular human origin which bears malicious (or at least competitive) ill-will towards some particular exposed organisation. Examples of social threat sources include hackers, cyber-criminals, disgruntled employees, agents of corporate espionage, NGOs or other advocacy groups who are seeking to cause reputational damage, or even business competitors who are seeking to gather competitive intelligence by legal means. We assume that most social threats will arise within the organisation's external environment; however, they might also originate, or extend their influence, within organisations, through practices such as corporate blackmail or bribery.

We limit our concern with social threat to its particular (i.e., individual or entity-specific) as opposed to fundamental (i.e., society-wide) expressions; however, within that narrowed context – to reiterate – we allow for a broad range of criminal(istic), malicious and competitive motivations. This narrowed range of social threat concerns draws on Duckett and Fisher's (2003) contribution to the social psychology literature. They follow insurance industry nomenclature by carefully differentiating particular from fundamental exposures to social threat, and by further differentiating "threatening and dangerous" from "competitive and jungle-like" situations (Duckett & Fisher, 2003; p. 204). They clarify that the psychological experience of exposure to social threat can vary significantly across these four exposure categories.

We discern from this a need for academic work on social threat to carefully specify the nature (or range) of the exposures that are at issue. Furthermore, this research might be construed as inviting the application of a precautionary posture of psychological realism to forecasting theory and practice, emphasising that the mind-dependency problems which threaten to bias the production of forecasting knowledge for social threat are highly complex and challenging. Taking this view, part of the rationale for the present paper is our recognition of the need for theoretical terms and organisational procedures which can help to overcome these problems.

We further theorise that all relevant 'particular' social threats are situated between the two extremes of fundamental and interpersonal social threat. This view aligns directly with our main theoretical concern with the epistemological challenges that face the organisation, in engaging a threat which is 'social' in the sense that it invites lay framing in terms of the *largely unknown*, yet often to some worthwhile extent *discoverable*, human volition that is driving and targeting it. These epistemological challenges are likely to require some balancing of theoretical guesswork and assumptions against facts that are made available through practices such as intelligence gathering.

We further emphasise that the production of forecasting knowledge along these epistemological pathways may need to consider the organisation's reflexive experience of some dynamic and evolving attack–defend relationship with particular social threat sources. Thus, we recommend the use of scenario exercises such as red teaming (Zenko, 2015). The use of role-playing allows the production of forecasting knowledge for reflexive and ongoing adversarial relationships, typically codifying knowledge gained within either new or amended planning protocols. Within red teaming and other organisational knowledge production contexts, we envisage our recommended terminology of 'known-unknowns' and 'unknown-knowns' as serving to address mind dependency problems by enabling reflection on the possible imbalances in knowledge production between theory and data.

We also contend that both aleatory and epistemic uncertainties matter for theorising an organisation's exposure to social threat. Der Kiureghian and Ditlevsen (2009) evaluate the conventional distinction between the two, which regards only epistemic uncertainty as reducible (e.g. through intelligence gathering) or as offering practical value, but which also considers it as somewhat misleading. However, they regard aleatory uncertainty as reducible too, especially over the longer term, by acting to modify exposure. Social threat, as we theorise it, will inevitably present at least some aleatory uncertainty because of the contingencies involved. Consider for example uncertainty over *whether*, *when*, *where*, *how* or *why* a cyber-criminal will act. Part of the epistemological challenge here arises from the fact that human volition is inherently capricious and often volatile. Furthermore, its embeddedness within situations that align it to perception, resource and opportunity may also be highly fluid and complex. Thus, a related forecasting issue is the need for some estimate of whether there is likely to be sufficient epistemic uncertainty present to merit a proactive investigation of the social threat source. Such may well be needed, for example, where there is uncertainty over whether, and by what means, an advocacy group has resolved to pursue a campaign against a particular organisation, or where there is uncertainty about criminal harnessing of a new technology.

3. (Un)known-(un)knowns

3.1 The four quadrants

Here we explain the origins of, and interpret the meaning and value of, the four *(un)known-(un)known* risk quadrants. In February 2002, US Secretary of Defense Donald Rumsfeld gave a media briefing which has been referenced widely within a range of areas of the academic literature for the terms that it used to categorise the military threats posed by Iraqi President Saddam Hussein’s regime. Rumsfeld offered three categories: things we know we know (known-knowns), things we know we do not know (known-unknowns), and things we do not know we do not know (unknown-unknowns) (CNN, 2016).

To link this idea to the relevant academic literature, it appears in the first instance that the idea of knowledge as a competence-oriented social accomplishment (Orlikowski, 2002) is at issue. A longstanding body of academic literature that deals with this idea emphasises that knowledge is social and cultural (Nicolini, Gherardi, & Yanow, 2016) as well as dialogical (Tsoukas, 2009) in character. Accordingly, we might view its level as slowly increasing within organisations for particular risks; perhaps especially for complex risks whose causal understanding is highly multifactorial. Furthermore, we may differentiate such knowledge from the 'information' it stems from. It is often maintained that, although information and knowledge are always about something (for our purpose, some forecasted risk), knowledge gathers and discerns patterns within information, and can therefore be understood as contributing texture and sharpness to forecasts of complex risks. Insofar as such knowledge has had its mettle tested by risk experience, we can then begin to call it accumulated 'wisdom' (Rowley, 2007), and can theorise about and measure the value it creates (Smith & Raspin, 2011). The work by Smith and Raspin (2011) on organisational knowledge production illustrates how the marketing literature in particular has developed a strong focus on knowledge development (Jaworski & Kohli, 1993) through its concern with the cultivation of marketing intelligence and the creation of measurable value from any marketing ‘insights’ found. Such a practice is rooted in part in resource-based theories of the firm (Barney, 1991); however, as we explain later, it also deeply reflects how businesses have learned from Rumsfeld’s domain: military intelligence.

Recognising that speculation on hostile weapons capability was clearly Rumsfeld’s focus in his 2002 briefing, it is plain that both of the knowledge components of his *(un)known-(un)known* were intended to take some risk as their object. It also seems reasonably certain that they were intended to denote separate categories of knowledge that could be synthesised somehow in order to improve the overall risk knowledge. However, Rumsfeld was pilloried widely because the precise meaning of each knowledge component, and its relationship to the other, remained unexplained.

First, we consider two simple theoretical frameworks for their explanatory power. The first contends that, while one of the two knowledge components always consists of some possible risk scenario that requires discussion and invites further questions, the other will comprise answers to these questions. These answers will either uphold and further inform or quell the concerns which have been expressed. Thus, calling a risk a ‘known-known’ would describe a knowledge accomplishment where a risk issue has been discussed thoroughly, questions have been raised, and further investigative effort has yielded satisfactory answers that clarify the risk. However, the problem which arises is that it is impossible to have answers for questions which have not been asked, and therefore only one of ‘known-unknowns’ and ‘unknown-knowns’ can exist, depending on which of these is used to designate the impossible permutation.

Secondly, though, some might regard the first knowledge component as estimating the uncertainty of the second. Hence, for example, a known-unknown might express a knowledge of high uncertainty regarding the destructiveness, readiness or precise nature of a weapon. However, this begs the question of how the first knowledge component could ever be an unknown. Yet again, therefore, the explanatory theory cannot span all four (un)known-(un)known quadrants.

A third, and more complex, possibility, holds that, while one of the two knowledge components comprises forecasting knowledge that pertains directly to some risk, the other adds the stamp of some knowledge enhancement. What makes this more complex is that such an enhancement might be achieved through further critical reflection on the evidence base, method, theoretical frame, or even psychological bias, that was used to produce the initial risk forecasting knowledge. Notably, this theory relies on time ordering: one of the two knowledge components always takes the other as its object for critical metacognition. However, the theory can be adjusted to make allowance for causal interplay between the two components. This happens when Rumsfeld's *(un)known-(un)knowns* are used to express the extent to which secondary layers of governance or lines of defence are brought to bear in some organisational process of risk forecasting knowledge development.

Notably, adjusting this explanatory theory to pertain to governance interaction rather than simply to time-ordering enables it to escape the flaw of the first two explanatory theories (i.e., limited coverage of the four quadrants). This is because it admits the possibility that risk forecasting knowledge development can be 'pushed' in various directions between governance players and other interested parties, for various reasons, including those of socio-technical risk manipulation. Hence, for example, a known-unknown might comprise geopolitical-agenda-driven and evidence-poor theoretical speculation about a weapons threat that is intended to serve as a 'false flag' pretext for initiating long-planned military aggression. However, perspective will then inevitably complicate how we apply Rumsfeld's categories. In cases where relevant evidential knowledge exists but is withheld from the public for security reasons, the risk would be a known-known for those with appropriate security clearances and either a known-unknown or an unknown-unknown from the public standpoint, depending on the level of public trust. From the more technical standpoint of weapons inspectors who lack privileged access to high level information and maintain a sceptical orientation towards geopolitically-driven and media-driven risk narratives, the same risk might be categorised best as an unknown-known – at least in cases where their professionalism leads them to attach the most salience to the information they themselves have gathered. Thus, one advantage of this explanatory theory is that it facilitates reflection on these issues of perspective. However, perhaps its biggest disadvantage is that it allows some risks to be categorised as unknown-unknowns even when distrusted sources widely consider them to exist.

When looking more closely at how the explanatory theory above might juxtapose evidence with theoretical speculation, Pawson, Wong, and Owen's (2011) study of how Rumsfeld's terms can inform realist theories of policy development is of interest. They call attention to the need for a 'steady conversion of unknowns to knowns' for both the theory-based and evidence-based knowledge components. They point out that this entails not only cultivating an evidence base for scrutinising policy arrangements, but also appreciating the complex nature of both theoretical speculation and evidence. We might value Rumsfeld's categories as facilitating the psychological realist agenda that we touched upon earlier: that of slowly and incrementally overcoming the problems of human frailty by the conversion of unknown-unknowns into known-knowns, through a critical interest in exploring the (sometimes imbalanced) interactions between the two knowledge components at issue.

Logan (2009) offers a philosophy of science interpretation of Rumsfeld's categories, which provides an excellent reason for valuing the first knowledge component (comprising theory) for its often benign and constructive influence upon the second (comprising evidence). He points out that scientific hypothesis testing in ideal situations is for 'known-unknowns'; that is, the theoretical knowledge comprising the hypothesis is known but the empirical findings are not, at least prior to the experiment. In cases where the findings lie out in the range of possibilities permitted by the theory, though, Logan (2009) argues that the thing under study should be regarded as an '*unknown-unknown*'. This helps us to appreciate that forecasting knowledge production in organisations might continually generate new 'unknown-unknowns' to serve as new focal points for forecasting efforts.

One final enhancement to our interpretation of Rumsfeld's terms is offered by celebrity cultural critic Slavoj Zizek, whose critical commentary sought to rectify Rumsfeld's neglect of the 'unknown-known' quadrant (Zizekian Studies, 2015). Zizek's argument was that the second knowledge component could comprise a motivating ideology that was associated with a particular risk belief. Writing from a psychoanalytic perspective that emphasised unconscious motivation, his point was that it is possible to be motivated by an ideological worldview while lacking a critical metacognitive awareness of how their resulting agency relates reflexively to the ideology's influence as a societal force. Hence, for an unknown-known, the 'known' would be a subjective risk belief (e.g. in a weapon of mass destruction capable of rapid deployment) and the 'unknown' would pertain to lack of critical reflection upon the role of ideology in driving the ascendency of that belief within the risk imagination. Of course, Zizek had in mind Rumsfeld's supposed role as an agent of neoconservative ideology, undergirding the United States hegemony in the Middle East.

We contend that the best way of capturing the value offered by the explanatory theories above is as follows. Firstly, we reaffirm that both knowledge components can be viewed as referring to varying levels of socially-distributed risk forecasting knowledge within organisations, and able to be improved through a critical awareness of how their interplay bears upon the overall production of risk forecasting knowledge. Secondly, we suggest that the psychology literature dealing with the use of 'abstract' and 'concrete' mindsets for structuring and developing knowledge holds the key to how we can differentiate these knowledge components for practitioners' use. Vallacher and Wegner (1985) contrast the more abstract and purpose-oriented 'why' of actions with the more process-oriented and concrete 'how' of actions to differentiate the separate emphases of these mindsets. For our present purposes, this can translate directly into a contrast between the abstract theoretical risk context, comprising risk imagination, perception and sense-making, and the concrete-sequential thought process required for a causal understanding of any risk. Of course, this is a problematic distinction, arguably juxtaposing the mind of the artist with the mind of the engineer; however, it perhaps also recognises the need for both within risk forecasting practice. Crutch, Connell, and Warrington (2009) illustrate the complexity of this subject matter at the semantic level by studying how abstract and concrete words relate to separate representational frameworks. They maintain that abstract words interrelate primarily through varying forms of mental association. This can produce useful simplifying and sometimes-metaphorical understandings of complex reality. In contrast, concrete words interrelate more taxonomically to produce a meaningful and ordered understanding of what is observed.

Aiming for a more succinct differentiation pertaining more specifically to risk forecasting knowledge, we suggest that a more 'abstract' mindset for risk forecasting knowledge can be understood as expressing theoretical imagination in terms of abstract categories and forms of risk, perhaps also linking abstract occurrences mechanistically (see Elster, 1989) to create narratives for risk events. This theoretical imagination might employ complexity-reducing metaphor or draw heavily on isomorphic learning to explain events as recurrences of previous similar ones. In contrast, a more 'concrete' mindset can be understood as being data-driven and rooted in context-specific description. We can further characterise the abstract mindset in terms of risk imagination strongly influencing risk perception; in contrast, the concrete mindset can be viewed as exerting influence in the reverse direction, with risk perception forming from actual risk experience and related data, thereafter sometimes reshaping the broader abstract context of risk imagination in turn. Accordingly, we theorise the two, in overview, as corresponding to forecasting knowledge shaped principally by explanatory risk imagination and descriptive risk observation, respectively. Notably, this simplifying interpretation requires that the former can include knowledge produced through moral imagination (Werhane, 1999), which might sometimes motivate risk-forecasting effort to take the longer and larger view.

Our resulting 'abstract' and 'concrete' risk forecasting knowledge components give rise to the four quadrants shown in Figure 1.

Figure 1: Four states of risk forecasting knowledge.

Known Knowns *Risk is known both abstractly (in correspondence to events which do or may happen) and as a concrete risk exposure whose portents or impacts can be described using available evidence.*	**Unknown Knowns** *Risk is less well known abstractly, but individual or organisational experience of it nonetheless necessitates its management.*
Known Unknowns *It is understood that a particular type or category of risk deserves attention, yet there is lack of convincing evidence for its presence as a concrete risk exposure for the organisation at a particular time.*	**Unknown Unknowns** *Possible risks which have not been imagined/conceptualised and evidence for whose relevance within some specific organisational context might exist embryonically as scattered information, but not as coherent risk knowledge.*

We further suggest that these four quadrants might be useful for expressing current estimated knowledge levels using psychometric mapping; that is, expert or practitioner estimates could be displayed for expert and concrete knowledge levels in relation to specific forecasting challenges.

We further propose that it is helpful to consider the following four points in order to raise knowledge levels from unknown-unknown to known-known status. Firstly, traditional risk management deals in known-knowns, inasmuch as its subject matter is (often insurable) regularly occurring risk events. These are ideal risk conditions for the ongoing refinement of high levels of abstract and concrete risk forecasting knowledge. Secondly, known-unknown risk events may often be events that are planned for, where planning protocols are created, tested and improved using red-teaming and other forms of scenario exercises. The term is also useful for highlighting challenges in the management of uncertainty should such events occur. For example, the World Health Organisation recently proposed that scientists and public health emergency planners prepare for the ‘known-unknown pathogen’ they call ‘Disease X’ (Nuki & Shaikh, 2018). Their point, in using Rumsfeld’s known-unknown category, is to emphasise the practical necessity of making preparations for a fast-spreading global epidemic which will place managers in knowledge-poor circumstances (e.g., with uncertainty over mode of transmission, spread rate etc.). Thirdly, we can view unknown-known risk forecasting challenges as being characterised at times by the presence of a knowledge of 'what' is happening or might happen, in the absence of any knowledge pertaining to 'why' it is happening or might happen. This seems highly pertinent to behavioural risks within organisations. Following Zizek's theoretical approach, we might look to examples that are characterised by difficulties in understanding behavioural risk, either because plausible psychological explanations are contestable and/or because they invite interpretive bias. Examples might include recklessness within financial institutions, where possible explanations might span psychopathy, sensation-seeking, edgework, controversial psychoanalytically-grounded theories, and a multitude of further alternative theories from behavioural finance and economics. Fourthly, we suggest that it may be possible to become more sensitised to the risk forecasting challenge of converting 'unknown-unknowns' into 'known knowns' by exploring whether known-unknown or unknown-known problems, such as those described above, constitute the most pressing obstacles. Of course, we have already discussed possible reasons for imbalances between abstract and concrete risk knowledge, by touching on issues of socio-technical manipulation, governance power play, and even simply varying perspectives and experiences.

Before setting out our suggestions regarding the ways in which organisations can engage with this conversion challenge, we look more closely at unknown-unknowns. The past decade has presented a never-ending stream of cyber 'black swan' events, affecting governments, businesses, and the general public. Some of the higher profile ones that have affected nation-states include the Stuxnet attack in 2010 (Langner, 2011), the Red October botnet attack in 2012 (Virvilis & Gritzalis, 2013), the Mask malware attack in 2014 (Kaspersky, 2014), and the recent WannaCry ransomware attack in 2017 (Sahi, 2017). Very recently, there have also been many targeted data breaches affecting large organisations, such as Uber (2017), Equifax (2017), and Deloitte (2017). Looking ahead to the future, we can expect the scale, severity and complexity of targeted cyber 'black swan' events to continue to increase. This makes it plain that risk forecasting needs to engage more proactively with what we are calling particular and targeted social threat, taking 'unknown-unknowns' as an appropriate starting point for forecasting knowledge production.

3.2 Application of the theoretical template: objectives and literature context

In applying the theoretical template, we meet the first objective of this paper (to develop key concepts for exploring how organisations may proactively detect and defend against particular social threats) through a critical discussion of our new 'boosted risk radar' concept, which is essentially a high-level abstract metaphor. Conversely, we meet the second objective (exploring the implications for the nature and scope of risk management practice, and in particular seeking practical ways to co-develop abstract and concrete risk forecasting knowledge) through a critical discussion of our proposed multi-layered 'risk intelligence' concept, which engages on more practical levels with how organisational risk management can pivot towards forecasting for unknown-unknowns and related knowledge conversion concerns.

For our literature context, we draw from earlier work on unconventional and irregular social threats (Marshall, Telofski, Ojiako, & Chipulu, 2012; Chipulu, Ojiako, & Marshall, 2016), including threats arising with market competition (see Ojiako, Johnson, Chipulu, & Marshall, 2010). Based on this literature, we argue that remedies to particular social threats can be modelled on the way in which the military deals with asymmetric or unconventional warfare. This entails considering, for example, that information asymmetries and disparities in ethics and resources can be important when theorising the circumstances of, and relationships between, cyber-criminals or hackers and the organisations they target.

A review of the related literature suggests that the drivers of attack persistence and reconfiguration over time can often include perceived social (Donnelly-Saalfield, 2009; Ifedi & Anyu, 2011), ethical (Schminke, Caldwell, Ambrose, & McMahon, 2014; Chipulu et al., 2016) or service (Grégoire & Fisher, 2008; Grégoire, Tripp, & Legoux, 2009; Fisk et al., 2010; Daunt & Harris, 2012) violations by the targeted firm. We further contend that it is important to understand how organisations which normally compete 'within the rules' are likely to effectively recognise, monitor and manage threat actions that are purposeful, targeted and sometimes episodically repeating, yet hard to predict because the threat sources are often anonymous and prepared to violate laws and other norms. We recognise from the learning-from-the-military literature (Ojiako et al., 2010; Ojiako, Marshall, Luke, & Chipulu, 2012; Marshall et al., 2012) that current risk management capabilities are often underprepared for such threat. Notably, Chen and Miller (1994) suggest that even reputable firms may engage in illegal or unethical threat actions when they deem competitors to be major obstacles to their survival.

Literature dealing with particular social threats exists in both the management and marketing fields (see Chen & Miller, 1994; Grégoire and Fisher, 2008; Grégoire et al., 2009; Zourrig, Chebat, & Toffoli, 2009; Ojiako et al., 2010; Nepomuceno, Rohani, & Grégoire, 2017). In the risk management literature, though, such a concern is arguably eclipsed by a greater concern to develop faster and more integrated responses to all sorts of threats. Accordingly, numerous scholars, such as Power (2004, 2009), Ojiako et al. (2010), Marshall and Ojiako (2013, 2015), Wu, Chen, and Olson et al. (2014), Huang, Wu, and Renn (2016), Leva, Balfe, McAleer, and Rocke (2017), Smyth (2017), Slonim (2018), Marshall, Bashir, Ojiako, and Chipulu (2018), and Marshall, Ojiako, and Chipulu (2019), have all concerned themselves with developing broader and more holistic risk management approaches. Over time, it could be argued that this has led to a blending of the risk-based internal control, enterprise risk management, resilience, crisis management, business continuity and organisational agility concepts which we outlined earlier. We sympathise with this integration agenda and seek to contribute new theory to it. Ambitious risk management approaches of this nature sometimes call on 'risk radar' concepts (Jovanovic, 2012; Jovanovic, Balos, & Yan, 2012; Huang et al., 2016) to denote environmental scanning. Central to this metaphor is the idea that proactive scanning is involved (radar equipment must transmit before it can detect anything). Further possible meanings include the idea that radar can be intelligently pointed and located. We will develop the risk radar metaphor further by conceiving of it as something that can be 'boosted' to generate abstract and concrete forecasting knowledge for particular social threats. Acknowledging that the test for a good organisational metaphor is whether it can inspire collaborative creative thinking within organisations (Biscaro & Comacchio, 2017), we argue that our boosted risk radar metaphor might help guide the risk management profession in the pursuit of its integration agenda.

4. Early warning risk radars

4.1 Location and pointing of the risk radar

When conceptualised in its broadest scope as a risk assessment information gathering and processing system (Jovanovic, 2012; Jovanovic et al., 2012; Jovanović & Baloš, 2013; Huang et al., 2016), the objective of the *'risk radar'* is to facilitate the recognition, monitoring and management of risk. Here, issues of risk radar pointing and ownership become important. Clearly, both the theoretical imagination of the abstract mindset and the concrete mindset's concern of interrogating and being led by data are required for 'pointing' purposes. This is because at times risk imagination might be exercised in order to decide what unlikely threat possibilities merit a detailed forecasting effort; alternatively, 'weak signals' of particular social threats could be the drivers.

This leaves the question of 'location', by which we mean both the risk management process context and the locus of risk ownership, within an organisation. For the broad organisational context, we might try to situate the risk radar within the context of enterprise risk management (ERM) approaches, which align the management of risks to governance structures, strategy and, more recently, performance (Aven & Aven, 2015; Bromiley, McShane, Nair, & Rustambekov, 2015; COSO, 2017). However, the main theoretical offering of this paper to risk management's integration agenda is an exploration of the way in which the risk radar can gather, process and communicate intelligence in order to create a risk-intelligent organisation by feeding into and engaging a broad range of pre-existing organisational processes.

According to Ansoff (1975, p. 22), organisations can respond to threats either reactively or proactively. Reactivity implies the development of competencies for quick and efficient crisis management. Proactivity implies scanning and then actively interrogating whatever is found to be of interest (Hambrick, 1981; Elenkov, 1997; Crant, 2000; Parker, Bindl, & Strauss, 2010). Our paper can be viewed as extending the advocacy of such proactivity at the interface between risk management and competitive intelligence functions, employing the term 'risk intelligence' partly to refer to their fusion. This creates a difficult risk radar ownership issue. While a strong case could be made that risk radars are best championed and owned by the risk management function, the reality is likely to be more complex. First and foremost, risk radar use will arguably be benefited by systematic organisational-wide learning in order to support the development and alignment of internal competencies. It could be argued that such an effort is best undergirded by a risk philosophy that promotes the ethical and cultural imperatives of widespread proactive risk management participation (Thompson, 1986; Valverde, 1991; Althaus, 2005; Campbell, 2006; Schiller & Prpich, 2014), which might result in the spontaneous coordinated participation of various organisational functions (Braunscheidel & Suresh, 2009), including competitive intelligence. Furthermore, some baseline level of participation by many or even all organisational functions may be appropriate under such conditions (see Balogun, Gleadle, Hailey, & Willmott, 2005; Hoyt & Liebenberg, 2011). Our key point here is that, without such a boundary spanning spontaneous co-ordination, the result may be a risk radar coverage that merely reflects pre-existing organisational biases, such as a risk manager's preoccupation with insurable risk or a CFO's preoccupation with financial risk. A related possibility is that the resulting risk intelligence may not be communicated in a timely and coordinated manner, and, if not aggregated sufficiently for upward communication, the consequence may be information overload in the higher echelons (Foss & Rodgers, 2011).

Conceptualising the risk radar as a means of early warning invites further reflection on two key points. Firstly, risk management integration entails not only *internal* integration, drawing together a range of risk management activities, but also further *external* (perhaps hybridised) integration with various other management and governance processes within organisations (Lidskog & Sjödin, 2016). The broad integration challenge here is largely one of information and knowledge management (Hoyt & Liebenberg, 2011), which is re-envisioned in the context of our study to accommodate the risk radar metaphor as its basic sensory apparatus. However, some conceptual awkwardness arises from the notion of a risk radar that is designed to receive and relay *risk information*, while also performing a broader information gathering and processing role. The important thing is that the use of the risk radar allows proactive risk identification to develop forecasting knowledge with the appropriate urgency (Huurne & Gutteling, 2008), while ensuring that all gathered information is circulated throughout relevant organisational lattices with the speed and confidentiality it requires. Some studies (e.g. Thompson & Bloom, 2000; Lin, Rivera, Abrahamsson, & Tehler, 2017) have suggested that risk managers prefer risk information to be formatted differently for use within varying operational and strategic decision contexts, and for stakeholder circulation, and Árvai (2014) argues that such a practice supports integrated risk management more than it threatens it. Accordingly, we caution against any use of unnecessarily restrictive terminology or formatting which might have the effect of communicating risk information too narrowly and preventing its meaningful understanding as applicable knowledge (Huurne & Gutteling, 2008; Árvai, 2014; Lin et al., 2017).

4.2 Information gathering from a risk perspective

It follows that the risk radar needs to look far beyond what the lens of 'risk' renders visible and formats for use within risk management processes. Accordingly, we view it as a metaphor for coordinated attentiveness to all aspects of the organisational environment that might matter to organisations, with proactivity in response to particular social threats serving as a blueprint for enhanced proactivity within the more general organisational scanning activity. One particularly important reason why risk radars should avoid the narrow use of risk terminology is simply that a rich causal understanding of a complex social reality is possible only through an agile use of language (Sitkin & Pablo, 1992; Power, Scheytt, Soin, & Sahlin, 2009; Aven & Aven, 2015). This point may be developed further by returning to our earlier observation that knowledge production in organisations is likely to benefit from the use of Rumsfeld's categories. We argue that this is because they invite critical reflection on the balance that is struck between the abstract-mechanistic and concrete-sequential knowledge which are required for engaging complex social reality. Hence, we advocate the use of Rumsfeld's categories as appropriate high-level terminology for the guidance of risk radar use.

4.3 Generating marketing insights

Our suggestion above that risk radars may serve a more diverse range of organisational purposes deserves some further elaboration. One possibility is that the risk radar's proactive intelligence-gathering techniques could be used not just for engaging particular social threats, but also for generating informational sources of competitive advantage that can be classed as consumer or other marketing insights. Smith and Raspin (2011) discuss organisational processes of knowledge development for the production of consumer insight along these lines. A highly relevant source for opening out the risk radar concept further, their work emphasises the need for elaborately designed scanning systems. Built into such systems are mechanisms which allow for not only the allocation of monitoring tasks to managers with diverse competencies, but also the alignment of such competencies with the changing complexity and volatility levels in competitive environments. More specifically, Smith and Raspin characterise the rare moments of insight that scanning should aspire to create, in terms of four basic 'VRIO' criteria. These criteria are that insights should: (i) offer 'value' for organisations, (ii) be 'rare', in the sense that competitors are unlikely to find them, (iii) not be 'imitable', meaning that competitors should lack the capabilities to either find them or act upon them, and (iv) be aligned to 'organisational capabilities'.

We could even define the term 'risk insight' using these same criteria. Taking this view, the best-practice suggestion arises that perhaps risk assessment processes would benefit from a routine consideration of whether the risks under their purview might be handled differently when they were recognised as offering risk insight value. Routine quantitative scoring for the insight value of identified risks might even help to transform the value of risk registers as decision-making tools (the importance of which role has been emphasised in the literature; see Ackermann, Eden, Williams, & Howick, 2007). This suggestion recognises that strategic decision-makers are more likely to value risk information which is communicated in ways that are consistent, unambiguous and easily understandable (Månsson, Abrahamsson, & Tehler, in press). However, it also raises the problematic question of whether risk management practice in general, and risk radar use in particular, can and should be transparent. At the very least, this section allows us to reaffirm that risk radars need to feed 'multilingual' and often confidential communication and dialogue within organisations (see Ackermann et al., 2007).

4.4 'Boosting' the risk radar

Using the example of how organisations today are challenged to engage more proactively with cyber criminals who are operating through bulletproof hosting facilities, we have already touched very briefly upon the question of how risk radar use may entail information gathering close to primary threat sources. We mentioned various possible courses of action, such as co-opting former cyber-criminals and employing intelligence professionals to infiltrate criminal enterprises and their hosting services. Such a closeness might also be achieved through simple forms of direct (remote-electronic and interpersonal) engagement and interaction, such as building trust and being invited by hacker communities to participate in private online conversations (e.g. on private Discord servers). However, the basic principles of trust-building, co-optation and the like can be generalised to many different kinds of particular social threat. Accordingly, we propose a concept of *'booster infrastructure'* for risk radars, centring on competency for intense proactive engagement and interaction with particular social threat sources who might harbour malice or competitive ill-will towards the organisation. This raises various issues of skills, resources, law and ethics, under the 'booster infrastructure' heading we propose. We might even theorise that such an infrastructure is the key missing link within risk management thinking today. However, we must reiterate strongly that any such enhanced risk management function would need to relax any semantic grip that its favoured risk discourses, documentation and related visual representations might have imposed hitherto on organisational information flows, either deliberately or unwittingly. This should make it better able to elicit enthusiastic participation in the organisationally-distributed co-development of risk forecasting knowledge. In particular, it could be argued that the risk management ownership of booster infrastructure should resist any temptation to process information through the conceptual straitjacket that Ackermann et al. (2007) associated with risk register use. A viable alternative may involve the use of 'action point registers' that triage incoming information towards where it can be assembled most productively as forecasting knowledge (or business insight) with whatever urgency and confidentiality may be deemed appropriate.

4.5 An opportunity for the risk profession?

Critics of the proposal above may claim that the active investigation of primary sources of risk information is best left to the fuzzy area of overlap between the competitive intelligence, business intelligence and marketing intelligence functions, which already have well-established competency in this area (Freeman, 1999; Wright & Calof, 2006; Calof & Wright, 2008; Smith & Lindsay, 2012). Nonetheless, we suggest that risk management can take a leading and coordinating role, linking these functions with the rest of the organisation through a guiding theoretical concern with the cross-functional co-development of risk forecasting knowledge. As is articulated in the literature exploring the relationship between professions and institutional change (Daudigeos, 2013; Muzio, Brock, & Suddaby, 2013), professions make use of their expertise and legitimacy to initiate institutional pressures which advance their own interests, sometimes through the development of new guides, standards and associated job descriptions which raise their status within organisations relative to other professions. This has occurred recently with the rise of the 'Chief Risk Officer' role, which focuses on ensuring that enterprise risk management is taken seriously as a strategy influencer at the top management table (Aabo, Fraser, & Simkins, 2005; Harrison & Phillips, 2014; Pernell, Jung, & Dobbin, 2017; Karanja & Rosso, 2017). Correspondingly, we envisage risk management ownership of a 'booster infrastructure' for risk radar as potentially constituting an opportunity to advance the risk profession within an organisation, in addition to that provided by the rise of ERM.

5. ERM context for boosted risk radars

Considering further the above issue of cross-functional leadership and coordination, it can be argued (see Aabo et al., 2005; Harrison & Phillips, 2014; Pernell et al., 2017; Karanja & Rosso, 2017) that the risk profession *already* strongly aspires to subsume various other – sometimes competing – organisational functions in order to serve its master concept of a single, overarching, early warning risk radar for organisations. Such empire-building efforts by risk management mean that the organisational groundwork for our boosted risk radar proposal is already well established in many organisations. From the perspective of 'boundary maintenance', which explores how professions take shape and gain influence (Montgomery & Oliver, 2007, p. 665), the risk profession is concerned fundamentally with promoting cross-functional information flows, leading to knowledge development, because without these, both ERM practice and resilience are impossible.

5.1 Resilience context

The above point can be extended as follows. A related consideration that favours the advancement of the risk management profession through further development of the risk radar is that the risk radar is already accepted widely as a foundational principle of organisational resilience. The well-known *'Roads to Resilience'* report (Franken, Goffin, Szwejczewski, & Kutsch, 2014) recognises five such principles (the five Rs) as follows: (i) risk radar should anticipate problems before they escalate, (ii) resources and assets should be diversified, (iii) relationships and networks should allow risk information to flow, (iv) rapid responses should be initiated before crises or disasters happen, and (v) review and adaptation should occur *ex post*.

However, we might ask how far these relationships and networks should extend. Should the human alertness and proactivity that constitute the risk radar be limited by the boundaries of the organisation? It could be argued that any confidential information that it gathers is best handled within the organisation. Nonetheless, the risk profession's growing attention to third party risk and partnership risk (PWC, 2013) is also an important consideration. We live in an *'age of access'* (Rifkin, 2001) that is characterised by complex supply chains and fluidity in co-working and partnering between organisations. Many new opportunities for malice towards organisations target the interfaces between organisations (Korsgaard, Brower, & Lester, 2015), arguably because this is where blind spots in risk radars are often found. We posit that this places an especially high premium on robust people skills, where a specific concern with stakeholder relationship maintenance is combined with a more general willingness to go out into the social world, in order to operate fit-for-purpose risk radars today. Consider for example that internet 4.0 technologies, while promising to revolutionise supply chains through industrial automation, also create new opportunities for hackers and cyber-criminals to infiltrate previously closed-off production facilities through newly created cyber-physical systems, big data analytics and cloud computing access points (Gilchrist, 2016, pp. 179-193). Given that tampering with machine-to-machine communication has a considerable potential to cause hard-to-detect damage, it is in the interests of exposed supply chain partners not only to co-ordinate their efforts to monitor for intrusions, but also to liaise closely with Information Technology (IT) security software developers. However, our previously stated suggestions for engaging sources of social threat also apply. There may be further opportunities to liaise with or co-opt individuals who are active in groups of hackers or cyber-criminals who have begun to focus their expertise in this area, or indeed with those who provide their web hosting facilities.

5.2 Challenges

There remain important further grounds for resisting the central proposal of this paper, some of which relate to the sheer complexity of any risk radar operating beyond the boundaries of particular organisations. Schoemaker, Day, and Snyder (2013) associate the production of knowledge through the use of 'strategic radars' (by networked firms in particular) with the problem of managing the resulting data avalanches. However, a much more fundamental and indeed obvious problem is that we can expect particular social threat sources to strongly resist the disclosure of any usable information concerning threats which they themselves pose, and hence, they may take strong measures to prevent or dissimulate any such disclosures. On the one hand, then, the information-gathering challenges that arise under these circumstances bolster our argument for the critical juxtaposition of abstract and concrete risk knowledge as a means of contextualising any information gleaned. However, we still need to acknowledge that the closer an early warning risk radar gets to the source of a social threat, the more practical and ethical challenges it is likely to encounter. Hence, there may be points of diminishing returns and increasing legal and reputational risk from greater resource expenditures on the boosting of risk radars.

To gain a better understanding of such risk, we could consider the sociological and psychological perspectives of 'organisational edgework' (Lyng, 2005; Zinn, in press). This involves viewing information-gathering encounters that push towards the 'edges' of appropriate behaviour as experiences that are characterised by intoxicating exhilaration, anxiety, relief, reward etc. Because such experiences are their own rewards, we can expect risk radar use to lead to at least some transgressive edgework. Thus, the question that arises is whether the negative legal-financial and reputational-financial impacts that arise from either real or perceived transgression might sometimes outweigh the anticipated benefits from information gained. The more that a risk radar is 'boosted' as we propose, the more serious these issues of risk-adjusted returns are likely to become. As we emphasise later on, professionalism in the application of relevant ethics codes can help to address this problem. We will argue that this can be facilitated through the participation of the competitive intelligence profession in the riskier and more controversial aspects of risk radar use.

6. Risk intelligence: three meanings

Having outlined some key organisational challenges and obstacles that are linked to our boosted risk radar proposal, we now look more closely at its forecasting knowledge development concerns, with reference to what we consider important facilitating terminology and related practices. In proposing three possible meanings of 'risk intelligence' that we think combine to provide the necessary terminological foundation for the development of boosted risk radars, we are able to look at the challenges and obstacles on a more practical organisational level and to recommend practical improvements within organisations.

6.1 Meaning 1: Risk intelligence is managing risk intelligently

Our view of 'risk intelligence' in the present section will be concerned with the combined intellectual, ethical and psychological wherewithal for gathering and developing risk forecasting knowledge for social threats.

Evan’s (2012) theory of risk intelligence (RQ) concerns simple estimates (a subject that is removed substantially from forecasting for complex risks). While described generally as “a special kind of intelligence for thinking about risk and uncertainty” (p. 288), its more precise measurement focus is on a resistance to false certainty when estimating probabilities for the correctness of truth claims. Similarly, several scholars focus narrowly on measurable aptitudes for thinking in rational (Stanovich, 2009a) or flexible (Mellers et al., 2015) ways about decisions under uncertainty. It is acknowledged widely (Frey and Detterman, 2004; Stanovich, 2009b; Stanovich & West, 2009) that such scientific approaches to measuring various forms of intelligence can sacrifice valuable bandwidth in their quest for measurability. Correspondingly, we suggest that risk intelligence is more likely to become a useful psychological concept for risk practitioners when used openly and flexibly; furthermore, it is most likely to be used effectively when practitioners are encouraged to focus its range of psychological meanings on what matters most for them, capturing these meanings for organisational learning purposes.

It could be argued that the human challenge of operating the boosted risk radar lends itself to the following broad psychological view of risk intelligence. Introducing some parallels with the RQ construct, we can consider how risk radars will benefit from a high IQ in particular ways. Consider for example the importance of the cognitive problem-solving skills that are fundamental to IQ, such as such as pattern recognition (Gottfredson, 1997). A high competency in this particular skill can often be vital to the flexible balancing of concrete risk knowledge and abstract explanatory and historical contextual knowledge, both for the purpose of initially becoming attuned to social threats and for the ongoing refinement of related forecasting knowledge (pertaining for example to changes in the intentions, plans or capabilities underlying such threats). We could also expand our scope to consider the emotional intelligence quotient (EQ) (Mayer et al., 2004).

The contributions of a high EQ to risk intelligence might include the insights that it can bring to problems such as a selective inattention to concrete risk information, which does not fit with affect-laden organisational narratives. It might even offer protective or curative benefits for problems of organisational paranoia (Kramer, 2008), which are bound to shape and weight prevailing risk forecasts for social threats at times. Turning to the cultural intelligence quotient (CQ) (Brislin, Worthley, & Macnab, 2006), we might also consider whether the risk profession's rapidly growing interest in cultural contexts is likely to advantage or disadvantage accurate risk forecasting. Such intelligence may prove important for appreciating why subtleties of the cultural context (e.g. ambiguities in legal and ethical rectitude within hacker communities that distance themselves from cyber-criminals) can matter both when theorising and when actively engaging with social threats to organisations. Thus, it may be useful to view risk intelligence as a composite of all of the above psychological quotients drawn together to enhance forecasting knowledge production, not least by addressing the mind dependency problems associated with an exposure to social threats that we touched upon earlier.

6.1.1 Ethical risk intelligence practice

Although 'EQ' is reserved for 'emotional intelligence' within the research literature, 'ethical intelligence' may perhaps be a more pressing practical concern in the use of our proposed risk radar. In particular, it could be argued that what matters most is a practical understanding of the ethical (and hence, legal and reputational) *do*s and *don't*s of engaging with various primary or near-primary social threat sources in order to elicit concrete risk information and gain contextual understanding. Conveniently, though, highly practical guidance on ethical codes for risk intelligence can be derived from the codes of conduct developed by the competitive intelligence profession. Here, the practical challenges that arise with our boosted risk radar concept start to become very clear. The approach taken by the Strategic and Competitive Intelligence Professionals (SCIP) is to offer a succinct high-level code of conduct (SCIP, 1997). Some foundational ethical principles are discernible. Their guidance emphasises the importance of honesty within contexts of social interaction, the need for compliance with all laws, and the need to avoid or declare conflicts of interest. It also incorporates more specific ethical imperatives, covering adherence to company policies and guidelines, and accurate disclosure of all relevant information when communicating with information sources. Thus, the effect of the code is to accentuate the profession's specialisation in legitimate intelligence-gathering that is capable of staving off reputationally-damaging suggestions of deceit and subterfuge. We conclude that organisations should clarify the ethical and psychological risk intelligence that they need for risk radar use, bearing in mind the need to act in accordance with appropriate codes of practice, and indeed to develop these as storehouses for the ethical and behavioural insights gained through risk radar use.

6.2 Meanings 2 and 3: Risk intelligence processes and risk intelligent organisations

Throughout the discussion that follows, we selectively juxtapose some basic properties of the traditional risk management process with various similar organisational processes and related activities that are pertinent to the gathering and processing of intelligence. Our aim will be to highlight opportunities for the consolidation of similar and overlapping processes. This will enable us to outline a consolidated risk intelligence process, and thus, to offer an outline vision of the risk intelligent organisation.

6.2.1 Learning from competitive, marketing and military intelligence processes

Maguire, Ojiako, and Robson (2009) and Ojiako et al. (2010, 2012) contend that a competency to exploit novel situations has often eluded organisations. Furthermore, studies dealing with how businesses can learn from the military (Darling, Parry, & Moore, 2005; Ojiako et al., 2010; Roche & Blaine, 2015) have suggested that organisations, especially those that are competing, in dynamic environments, with irregular social threats from competitors, regulators, advocacy organisations, criminals, cyber-hackers and the like, can learn a lot from military approaches to combating irregular military threats. Seeking to contribute to the traditions of this literature, we advocate building the risk radar by hybridising the traditional risk management process with conceptually-similar marketing intelligence, competitive and military intelligence processes. There is no doubt from the organisational intelligence literature (e.g. Dishman & Calof, 2008; Calof & Wright, 2008; McMullen, Shepherd, & Patzelt, 2009) that various organisational intelligence processes can offer a range of information-gathering and knowledge-development enhancements. We will argue that organisational efforts to harness these competencies under the rubric of a general ‘risk intelligence’ process might be best to proceed from a constructively simple theoretical emphasis on the challenge of boosting risk forecasting knowledge production for urgent and far-reaching engagement with ‘irregular’ social threats, paralleling the irregular threats that the military has learned to engage.

6.2.2 Adopting the terminology of military intelligence processes

Our emphasis on ‘gathering’ or ‘collecting’ information, which is key to competitive, marketing, business and other forms of intelligence practice within organisations (Taplin, 1989), has deep roots in decades of military intelligence theory and practice (Roche & Blaine, 2015). Military intelligence involves intelligence gathering, which may sometimes require personal bravery and sacrifice, in strong contrast to the risk management concept of risk identification, the sedentary connotations of which are (we think regrettably) consistent with much contemporary desk-based risk identification practice. An obvious yet curiously under-recognised benefit of adopting the military intelligence 'gathering' and 'collecting' metaphors is that they invite far more proactive and energetic views regarding the ways in which organisations can develop their attentiveness to social threats.

A corresponding practical opportunity for hybridisation is as follows. Whereas the ISO 31000 risk management process (ISO, 2009) begins with an *'establishing the context'* stage prior to its *'risk identification'* stage, US Military Joint Publication 2-0 (Department of Defense, 2013) moves through parallel '*planning'* and *'direction'* stages, followed by *'collection'*. This document captures some of the logic of ISO 31000's first two stages in its view of *'planning'* and *'direction'* as being concerned with the specification of the information that is necessary for the successful achievement of specified military objectives, so that specified *'collection'* activities can take place at the next stage. However, in the military intelligence process, stage two intelligence '*collection'* conjoins logically with stage one *'direction'*, but such a directed elicitation of active information gathering effort will not necessarily take place in the equivalent risk management process.

Perhaps, then, the ISO 310000 '*establishing the context'* stage can be improved through further provisions for the establishment of contextual *uncertainties*, the purpose of which is to focus intelligence-gathering activities explicitly at stage two. In terms of our primary guiding metaphor, the aim of such new provisions might also be construed as 'pointing the risk radar in a particular direction'. We might also take into account here our further layer of theoretical concern in focusing the risk intelligence effort on the conversion of unknown-unknowns, through a further metaphorical conceptualisation of this enhanced and hybridised practice as serving to point the risk radar towards where the 'black swans' (i.e., unknown-unknowns) are most likely to fly in from. Arguably, then, what makes this high-level metaphorical view particularly valuable is that it relates directly to what might often be the practical necessity of establishing stage one specifications of contextual uncertainty, which prime stage two information gathering to be attuned to wholly novel social threats. Remembering that our risk intelligence goal is the co-development of abstract and concrete risk knowledge, it is also worth mentioning that there is no reason why such priming could not specify stage two information-gathering challenges in terms of demands placed on both abstract theoretical imagination and requirements for concrete risk information.

6.2.3 Learning from military intelligence practice

Risk analysis typically focuses on the estimation of probabilities and consequences for risks, so that risk evaluation can then consider each risk's significance with reference to pre-established criteria such as risk appetite or tolerance (Aven, 2012, 2018). The parallel practice within the military is to ensure the reliability and credibility of the collected intelligence through a process of filtering and weighting (Corkill, 2008; Wheaton, 2009). Such a practice is espoused for example in the joint warfare publication on intelligence support that was published by the UK Ministry of Defence (2003).

If we are to re-envision risk management as a practice that is to be invigorated through active intelligence gathering, we might regard simple reliability ratings for sources, and simple credibility ratings for the information or knowledge these sources provide, as providing a highly practical means of enhancing consolidated risk intelligence processes that are dedicated to risk forecasting knowledge production. Notably, credibility judgments about risk forecasts must be differentiated from the probability judgments that they help shape. Inquiries regarding credibility in part question the appropriateness of some abstract theoretical framework, which assembles information as knowledge, perhaps in a simple 'story' form. Thus, a risk intelligence process requirement to judge credibility, inspired by military intelligence practice, can help to sensitise those involved in risk forecasting knowledge production to the need to differentiate between abstract and concrete risk knowledge in order to apply an appropriate critical scrutiny to a risk forecast.

To reiterate our concerns regarding learning from the military, gaining an understanding of the ways in which military commanders have dealt with the dynamics of an ever-changing combat environment may include learning from relatively modern ‘asymmetric’ or ‘unconventional’ military approaches in response to combat experiences with irregular adversaries (see Kilcullen, 2010; Nagl, 2010; Ministry of Defence, 2010). Such learning invites the following practices. Small, agile and highly cross-trained special risk intelligence teams or task forces (similar to military special operators), bolstered by competitive intelligence capability, may create sufficient organisational capacity to allow risk forecasting knowledge development to be grounded in what Ojiako et al. (2010) call ‘distributed intelligence’. This term refers to intelligence built from the lowest level of the organisation through a widespread representation of its various functions in the special teams. This enables team members to contribute a sufficiently broad and overlapping range of knowledge and experience pertaining to how particular social threats might impact organisations. In military circles, every special operator is considered to be mandated to gather intelligence. Similarly, in organisations, every employee might be seen as a proactive gatherer of intelligence who can interact with the special teams. This suggestion is intended to gel with the commonplace ERM philosophy which emphasises universal responsibility for initiating risk communications throughout the corporate nervous system (Institute of Risk Management, 2011).

Organisations can also develop risk forecasting knowledge through risk simulations structured in accordance with military *‘red teaming’* practice (Zenko, 2015). This entails realistic role-play rehearsals of attacks upon organisations, in order to enrich forecasts, identify security vulnerabilities and improve planning protocols. Dedicated ‘red teams’ can also offer decision support. The well-known UK Ministry of Defence (2013) guidance explaining how is of interest in part for its surprising use of business terminology. It defines red teaming as "the independent application of a range of structures, creative and critical thinking techniques to assist the end user make a better informed decision to produce a more robust product" (p. 4). Lauder (2009) observes that *'red teaming'* in this sense usually entails the voicing of contrarian positions in order to inculcate more open-minded group decision-making, either in scenario exercises or in real life decision-making contexts. We might develop its potential contribution to risk forecasting practice further by noting that it creates opportunities for the application of critical scrutiny to the co-production of abstract and concrete forecasting knowledge. Furthermore, red teaming practice creates opportunities for former cyber-criminals and hackers to be co-opted as defenders of organisations.

7. Conclusion

The paper has advocated for the enhancement of risk forecasting practice under the combined influence of the multi-layered terminology and theory. Our theories pertaining to (1) the critical application of Rumsfeld's knowledge quadrants for the co-development of abstract and concrete forecasting knowledge, (2) the boosted risk radar, and (3) risk intelligence considered in the three interrelated aspects we propose, all offer novelty. By relating these theories both to one another and to highly practical proposals for enhancing organisational risk forecasting, we ensure the novelty of our contribution to the risk management and forecasting literatures, particularly in relation to the challenges created by irregular social threats in general and cybersecurity threats in particular.

Thus, we have provided the initial terminological and conceptual groundwork for theory development and for improvements to organisational forecasting practice. Further research on risk forecasting as critical knowledge production focused on Rumsfeld's binary knowledge ontology and its four quadrants, is called for. Psychometric research may assist if it can supply measurement tools showing that practitioners can estimate separate levels of abstract and concrete forecasting knowledge. If it can also be proven that this knowledge ontology is helpful for critical scrutiny purposes, this would strengthen the case for improving risk management as we advocate.

References

Aabo, T., Fraser, J., & Simkins, B. (2005). The rise and evolution of the chief risk officer: enterprise risk management at Hydro One. *Journal of Applied Corporate Finance*, *17*(3), 62-75.

Ackermann, F., Eden, C., Williams, T., & Howick, S. (2007). Systemic risk assessment: a case study. *Journal of the Operational Research Society*, *58*(1), 39-51.

Althaus, C. (2005). A disciplinary perspective on the epistemological status of risk. *Risk Analysis*, *25*(3), 567-588.

Ansoff, H. (1975). Managing strategic surprise by response to weak signals. *California Management Review*, *18*(2), 21-33.

Árvai, J. (2014). The end of risk communication as we know it. *Journal of Risk Research*, *17*(10), 1245-1249.

Aven, T. (2012). Foundational issues in risk assessment and risk management. *Risk Analysis*, *32*(10), 1647-1656.

Aven, T. (2018). An emerging new risk analysis science: foundations and implications. *Risk Analysis*, *38*(5), 876-888.

Aven, E., & Aven, T. (2015). On the need for rethinking current practice that highlights goal achievement risk in an enterprise context. *Risk Analysis*, *35*(9), 1706-1716.

Balogun, J., Gleadle, P., Hailey, V., & Willmott, H. (2005). Managing change across boundaries: boundary-shaking practices. *British Journal of Management*, *16*(4), 261-278.

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, *17*(1), 99-120.

Biscaro, C., & Comacchio, A. (2017). Knowledge creation across worldviews: how metaphors impact and orient group creativity. *Organization Science*, 29 (1), 58-79.

Bradbury, D. (2014). Testing the defences of bulletproof hosting companies. *Network Security*, *2014*(6), 8-12.

Braunscheidel, M., & Suresh, N. (2009). The organisational antecedents of a firm's supply chain agility for risk mitigation and response. *Journal of Operations Management*, *27*(2), 119-140.

Brislin, R., Worthley, R., & Macnab, B. (2006). Cultural intelligence: understanding behaviours that serve people's goals. *Group and Organisation Management*, *31*(1), 40-55.

British Standards Institution (2014). *BS 65000 guidance on organisational resilience*. Available at: http://www.standardsuk.com/, accessed 25/03/18.

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: review, critique, and research directions. *Long Range Planning*, *48*(4), 265-276.

Calof, J., & Wright, S. (2008). Competitive intelligence: a practitioner, academic and inter-disciplinary perspective. *European Journal of Marketing*, *42*(7/8), 717-730.

Campbell, S. (2006). Risk and the subjectivity of preference. *Journal of Risk Research*, *9*(3), 225-242.

Chen, M., & Miller, D. (1994). Competitive attack, retaliation and performance: an expectancy-valence framework. *Strategic Management Journal*, *15*(2), 85-102.

Chipulu, M., Ojiako, U., & Marshall, A. (2016). Consumer action in response to ethical violations by service operations firms: the impact of heterogeneity. *Society and Business Review*, *11*(1), 24-45.

CNN (2016). *RUMSFELD / KNOWNS.* [online video] Available at: https://www.youtube.com/watch?v=REWeBzGuzCc, accessed 02/04/18.

Corkill, J. (2008). Evaluation a critical point on the path to intelligence. *Journal of the Australian Institute of Professional Intelligence Officers*, *16*(1), 3-11.

Committee of Sponsoring Organisations of the Treadway Commission (COSO) (2017). *Enterprise risk management: integrating with strategy and performance.* http://www.standardsuk.com, accessed 28/03/18.

Crant, J. (2000). Proactive behaviour in organisations. *Journal of Management*, *26*(3), 435-462.

Crutch, S., Connell, S., & Warrington, E. (2009). The different representational frameworks underpinning abstract and concrete knowledge: evidence from odd-one-out judgements. *Quarterly Journal of Experimental Psychology*, *62*(7) 1377-1390.

Darling, M., Parry, C., & Moore, J. (2005). Learning in the thick of it. *Harvard Business Review*, *83*(7), 84-93.

Daudigeos, T. (2013). In their profession's service: how staff professionals exert influence in their organisation. *Journal of Management Studies*, *50*(5), 722-749.

Daunt, K., & Harris, L. (2012). Exploring the forms of dysfunctional customer behaviour: A study of differences in servicescape and customer disaffection with service. *Journal of Marketing Management*, *28*(1-2), 129-153.

Department of Defense. (2013). *JP 2-0: joint intelligence.* http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf, accessed 26/12/17.

Der Kiureghian, A., & Ditlevsen, A. (2009). Aleatory or epistemic? Does it matter? *Structural Safety*, *31*(2), 105-112.

Dishman, P., & Calof, J. (2008). Competitive intelligence: a multiphasic precedent to marketing strategy. *European Journal of Marketing*, *42*(7/8), 766-785.

Donnelly-Saalfield, J. (2009). Irreparable harms: how the devastating effects of oil extraction in Nigeria have not been remedied by Nigerian courts, the African Commission, or US courts. *Hastings West-Northwest Journal of Environmental Law and Policy*, *15*, 371-420.

Duckett, J., & Fisher, K. (2003). The impact of social threat on worldview and ideological attitudes. *Political Psychology*, *24*(1), 199-222.

Elenkov, D. (1997). Strategic uncertainty and environmental scanning: The case for institutional influences on scanning behaviour. *Strategic Management Journal*, *18*(4), 287-302.

Elster, J. (1989). *Nuts and bolts for the social sciences*. Cambridge University Press.

Evans, D. (2012). *Risk intelligence: how to live with uncertainty*. New York: Free Press.

Fisk, R., Grove, S., Harris, L., Keeffe, D., Daunt, K., Russell-Bennett, R., & Wirtz, J. (2010). Customers behaving badly: a state of the art review, research agenda and implications for practitioners. *Journal of Services Marketing*, *24*(6), 417-429.

Foss, K., & Rodgers, W. (2011). Enhancing information usefulness by line managers' involvement in cross-unit activities. *Organisation Studies*, 32(5), 683-703.

Franken, A., Goffin, K., Szwejczewski, M., & Kutsch, E. (2014). *Roads to resilience: building dynamic approaches to risk*. Cranfield Management School.

Freeman, O. (1999). Competitor intelligence: information or intelligence? *Business Information Review*, *16*(2), 71-77.

Frey, M., & Detterman, D. (2004). Scholastic assessment or g? The relationship between the scholastic assessment test and general cognitive ability. *Psychological Science*, *15*(6), 373-378.

Gilchrist, A. (2016). *Industry 4.0: the industrial internet of things.* Apress: Berkeley, CA.

Gottfredson, L. (1997). Mainstream science on intelligence (editorial). *Intelligence*, *24*, 13–23.

Grégoire, Y., & Fisher, R. (2008). Customer betrayal and retaliation: when your best customers become your worst enemies. *Journal of the Academy of Marketing Science*, *36*(2), 247-261.

Grégoire, Y., Tripp, T., & Legoux, R. (2009). When customer love turns into lasting hate: The effects of relationship strength and time on customer revenge and avoidance. *Journal of Marketing*, *73*(6), 18-32.

Hambrick, D. (1981). Specialization of environmental scanning activities among upper level executives. *Journal of Management Studies*, *18*(3), 299-320.

Harrison, G., & Phillips, R. (2014). Subjective beliefs and statistical forecasts of financial risks: the chief risk officer project. In T.J. Andersen (ed.), *Contemporary challenges in risk management*. Palgrave Macmillan, London.

Hoyt, R., & Liebenberg, A. (2011). The value of enterprise risk management. *Journal of Risk and Insurance*, *78*(4), 795-822.

Huang, C., Wu, T., & Renn, O. (2016). A risk radar driven by internet of intelligences serving for emergency management in community. *Environmental Research*, *148*, 550-559.

Huurne, E., & Gutteling, J. (2008). Information needs and risk perception as predictors of risk information seeking. *Journal of Risk Research*, *11*(7), 847-862.

Ifedi, J., & Anyu, J. (2011). "Blood oil," ethnicity, and conflict in the Niger delta region of Nigeria. *Mediterranean Quarterly*, *22*(1), 74-92.

Institute of Risk Management (2011). *Risk appetite and tolerance: a guidance paper from the Institute of Risk Management*. Institute of Risk Management.

ISO (2009). *ISO 31000: Risk management – principles and guidelines*. Geneva: International Standards Organisation.

Jaworski, B., & Kohli, A. (1993). Market orientation: antecedents and consequences. *Journal of Marketing*, *57*, 53-70.

Jovanovic, A. (2012). *From iNTeg-Risk to European Emerging Risk Radar (E2R2), managing early warnings – what and how to look for?* Book of Abstracts of the 4th iNTeg-Risk Conference, 2012 (p. 46).

Jovanovic, A., Balos, D., & Yan, L. (2012). The European emerging risk radar initiative–a chance for China? *Procedia Engineering*, *43*, 489-493.

Jovanović, A., & Baloš, D. (2013). iNTeg-Risk project: concept and first results. *Journal of Risk Research*, *16*(3-4), 275-291.

Karanja, E., & Rosso, M. (2017). The chief risk officer: a study of roles and responsibilities. *Risk Management*, *19*(2), 103-130.

Kaspersky (2014). *Unveiling "Careto" – the masked APT.* Kaspersky Lab, https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf, accessed 11/03/18.

Kilcullen, D. (2010). *Counterinsurgency*. London: Hurst.

Korsgaard, M., Brower, H., & Lester, S. (2015). It isn't always mutual: A critical review of dyadic trust. *Journal of Management*, *41*(1), 47-70.

Kramer, R. (2008). Organizational paranoia: origins and dysfunctional consequences of exaggerated distrust and suspicion in the workplace. In C. Wankel (ed.), *21st Century Handbook of Organizations: a reference handbook* (pp. 231-238). Los Angeles: Sage Publications.

Langner, R. (2011). Stuxnet: dissecting a cyberwarfare weapon. *IEEE Security and Privacy*, *9*(3), 49-51.

Lauder, M. (2009). Red dawn: the emergence of a red teaming capability in the Canadian forces. *Canadian Army Journal*, *12*(2), 25-36.

Leva, M., Balfe, N., McAleer, B., & Rocke, M. (2017). Risk registers: structuring data collection to develop risk intelligence. *Safety Science*, *100*(Part B), 143-156.

Lidskog, R., & Sjödin, D. (2016). Risk governance through professional expertise. Forestry consultants' handling of uncertainties after a storm disaster. *Journal of Risk Research*, *19*(10), 1275-1290.

Lin, L., Rivera, C., Abrahamsson, M., & Tehler, H. (2017). Communicating risk in disaster risk management systems – experimental evidence of the perceived usefulness of risk descriptions. *Journal of Risk Research*, *20*(12), 1534-1553.

Logan, D. (2009). Known knowns, known unknowns, unknown unknowns and the propagation of scientific enquiry. *Journal of Experimental Botany*, *60*(3) 712–714.

Lyng, S. (ed.) (2005). *Edgework. The sociology of risk-taking*. New York: Routledge.

Maguire, S., Ojiako, U., & Robson, I. (2009). The intelligence alchemy and the twenty-first century organisation. *Strategic Change*, *18*(3-4), 125-139.

Månsson, P., Abrahamsson, M., & Tehler, H. (in press). Aggregated risk: an experimental study on combining different ways of presenting risk information. *Journal of Risk Research*, in press.

Marshall, A., Bashir, H., Ojiako, U., & Chipulu, M. (2018). A Machiavellian behavioural framing of social conflict risks in supply chains. *Management Research Review*, in press.

Marshall, A., & Ojiako, U. (2013). Managing risk through the veil of ignorance. *Journal of Risk Research*, *16*(10), 1225-1239.

Marshall, A., & Ojiako, U. (2015). A realist philosophical understanding of entrepreneurial risk-taking. *Society and Business Review*, *10*(2), 178-193.

Marshall, A., Ojiako, U., & Chipulu, M. (2019). Risk appetite: a futility, perversity and jeopardy critique of over-optimistic corporate risk taking. *International Journal of Organisational Analysis*, in press.

Marshall, R., Telofski, R., Ojiako, U., & Chipulu, M. (2012). An examination of 'irregular competition' between corporations and NGOs. *Voluntas*, *23*, 371-391.

Mayer, J., Salovey, P., & Caruso, D. (2004). Emotional intelligence: theory, findings, and implications. *Psychological Inquiry*, *15*, 197-215.

McMullen, J., Shepherd, D., & Patzelt, H. (2009). Managerial (in)attention to competitive threats. *Journal of Management Studies*, *46*(2), 157-181.

Mellers, B., Stone, E., Atanasov, P., Rohrbaugh, N., Metz, S., Ungar, L., Bishop, M., et al. (2015). The psychology of intelligence analysis: drivers of prediction accuracy in world politics. *Journal of Experimental Psychology: Applied*, *21*(1), 1-14.

Ministry of Defence (UK) (2003). *Joint warfare publication 2-00: intelligence support to joint operations*. Joint Doctrine and Concepts Centre, Ministry of Defence.

Ministry of Defence (UK) (2010). *Countering insurgency: Army Field Manual, Vol. 1 Pt. 10 (AC71876)*. Ministry of Defence.

Ministry of Defence (UK) (2013). *Red teaming guide, development, concepts and doctrine centre* (2nd ed.). Ministry of Defence.

Montgomery, K., & Oliver, A. (2007). A fresh look at how professions take shape: dual-directed networking dynamics and social boundaries. *Organisation Studies*, *28*(5), 661-687.

Morgan, G. (2006). *Images of organization*. Sage Publications.

Muzio, D., Brock, D., & Suddaby, R. (2013). Professions and institutional change: Towards an institutionalist sociology of the professions. *Journal of Management Studies*, *50*(5), 699-721.

Nagl, J. (2010). Thinking globally, acting locally: counterinsurgency lessons from modern wars. *Journal of Strategic Studies*, *33*(1), 16-59

Nepomuceno, M., Rohani, M., & Grégoire, Y. (2017). Consumer resistance: from anti-consumption to revenge. In *Consumer perception of product risks and benefits* (pp. 345-364). Springer International Publishing.

Nicolini, D., Gherardi, S., & Yanow, D. (2016). Introduction: toward a practice-based view of knowing and learning in organizations. In D. Nicolini, S. Gherardi, & D. Yanow (eds), *Knowing in organizations* (Ch. 1). Routledge.

Nuki, P., & Shaikh, A. (2018). *Scientists put on alert for deadly new pathogen: 'Disease X'*. The Telegraph Online, 10th March 2018 edition, https://www.telegraph.co.uk/news/2018/03/09/world-health-organization-issues-alert-disease-x/, accessed 24/04/18.

Ojiako, U., Johnson, J., Chipulu, M., & Marshall, A. (2010). Unconventional competition – drawing lessons from the military. *Prometheus*, *28*(4), 327-342.

Ojiako, U., Marshall, A., Luke, M., & Chipulu, M. (2012). Managing competition risk: A critical realist philosophical exploration. *Competition and Change*, *16*(2), 130-149.

Orlikowski, W. (2002). Knowing in practice: enacting a collective capability in distributed organizing. *Organization Science*, *13*(3), 249–273.

Parker, S., Bindl, U., & Strauss, K. (2010). Making things happen: A model of proactive motivation. *Journal of Management*, *36*(4), 827-856.

Pawson, R., Wong, G., & Owen, L. (2011). Known knowns, known unknowns, unknown unknowns: the predicament of evidence-based policy. *American Journal of Evaluation*, *32*(4), 518-546.

Pernell, K., Jung, J., & Dobbin, F. (2017). The hazards of expert control: chief risk officers and risky derivatives. *American Sociological Review*, *82*(3), 511-541.

Power, M. (2004). The risk management of everything. *Journal of Risk Finance*, *5*(3), 58-65.

Power, M. (2009). The risk management of nothing. *Accounting, Organisations and Society*, *34*(6), 849-855.

Power, M., Scheytt, T., Soin, K., & Sahlin, K. (2009). Reputational risk as a logic of organising in late modernity. *Organisation Studies*, *30*(2-3), 301-324.

PWC (2013). *TPRM viewpoint: PwC viewpoint on third party risk management*. PricewaterhouseCoopers.

Rifkin, J. (2001). *Age of access: the new culture of hypercapitalism, where all of life is a paid-for experience*. Jeremy P. Tarcher.

Roche, E., & Blaine, M. (2015). The intelligence gap: what the multinational enterprise can learn from government and military intelligence organisations. *Thunderbird International Business Review*, *57*(1), 3-13.

Rowley, J. (2007). The wisdom hierarchy: representations of the DIKW hierarchy. *Journal of Information and Communication Science*, *33*(2), 163-180.

Sahi S. (2017). A study of WannaCry ransomware attack. *International Journal of Engineering Research in Computer Science and Engineering*, *4*(9), 5-7.

Schiller, F., & Prpich, G. (2014). Learning to organise risk management in organisations: what future for enterprise risk management? *Journal of Risk Research*, *17*(8), 999-1017.

Schoemaker, P., Day, G., & Snyder, S. (2013). Integrating organizational networks, weak signals, strategic radars and scenario planning. *Technological Forecasting and Change*, *80*(4), 815-824.

Schminke, M., Caldwell, J., Ambrose, M., & McMahon, S. (2014), Better than ever? Employee reactions to ethical failures in organisations, and the ethical recovery paradox. *Organisational Behaviour and Human Decision Processes*, *123*(2), 206-219.

Scott, W. (2003). *Organizations: rational, natural, and open systems* (5th ed.). Prentice Hall, Upper Saddle River, New Jersey.

SCIP (1997). *Competitive intelligence ethics: navigating the gray zone*. Strategic and Competitive Intelligence Professionals.

Sitkin, S., & Pablo, A. (1992). Reconceptualizing the determinants of risk behaviour. *Academy of Management Review*, *17*(1), 9-38.

Slonim, O. (2018). National intelligence: A tool for political forecasting and the forecasting of rare events. *Technological Forecasting and Social Change*, *128*, 245-251.

Smith, B., & Raspin, P. (2011). *Creating market insight: how firms create value from market understanding*. John Wiley & Sons.

Smith, R., & Lindsay, D. (2012). From information to intelligence management. *Business Information Review*, *29*(2), 121-124.

Smyth, V. (2017). Software vulnerability management: how intelligence helps reduce the risk. *Network Security*, *2017*(3), 10-12.

Stanovich, K. (2009a). *What intelligence tests miss: the psychology of rational thought*. New Haven, CT: Yale University Press.

Stanovich, K. (2009b). Rational and irrational thought: the thinking that IQ tests miss. *Scientific American Mind*, *20*(6), 34-39.

Stanovich, K., & West, R. (2009). What intelligence tests miss. *The Psychologist*, *27*(2), 80-83.

Taplin, W. (1989). Six general principles of intelligence. *International Journal of Intelligence and Counter Intelligence*, *3*(4), 475–491.

Thompson, P. (1986). The philosophical foundations of risk. *The Southern Journal of Philosophy*, *24*(2), 273-286.

Thompson, K., & Bloom, D. (2000). Communication of risk assessment information to risk managers. *Journal of Risk Research*, *3*(4), 333-352.

Tsoukas, H. (2009). A dialogical approach to the creation of new knowledge in organizations. *Organization Science*, *20*(6), 941–957.

Vallacher, R., & Wegner, D. (1985). *A theory of action identification*. Lawrence Erlbaum Associates, Hillsdale NJ.

Valverde, L. (1991). Cognitive status of risk: a response to Thompson. *RISK: Health, Safety and Environment*, *2*(4), 313-339.

Virvilis, N., & Gritzalis, D. (2013). The big four – what we did wrong in advanced persistent threat detection? In *International Conference on Availability, Reliability and Security*, 2-6 September, 2013.

Weick, K., & Sutcliffe, K. (2001). *Managing the unexpected: resilient performance in an age of uncertainty*. John Wiley & Sons.

Weick, K., & Putnam, T. (2006). Organizing for mindfulness: eastern wisdom and western knowledge. *Journal of Management Inquiry*, *15*(3), 275-287.

Werhane, P. (1999). *Moral imagination and management decision-making*. Oxford University Press.

Wheaton, K. (2009). Evaluating intelligence: answering questions asked and not. *International Journal of Intelligence and Counterintelligence*, *22*(4), 614-631.

Wright, S., & Calof, J. (2006). The quest for competitive, business and marketing intelligence: a country comparison of current practices. *European Journal of Marketing*, *40*(5/6), 453-465.

Wu, D., Chen, S., & Olson, D. (2014). Business intelligence in risk management: some recent progresses. *Information Sciences*, *256*, 1-7.

Zenko, M. (2015). *Red team: how to succeed by thinking like the enemy*. Basic Books.

Zinn, J. (in press). The meaning of risk-taking–key concepts and dimensions. *Journal of Risk Research*, in press.

Zizekian Studies. (2015). Slavoj Zizek | Unknown knowns and psychoanalysis [online video]. https://www.youtube.com/watch?v=i1IjkfcwoHs, accessed 02/04/18.

Zourrig, H., Chebat, J., & Toffoli, R. (2009). Consumer revenge behaviour: a cross-cultural perspective. *Journal of Business Research*, *62*(10), 995-1001.